IX Jornadas de Ingeniería Telemática

JITEL 2010

Universidad de Valladolid, del 29 de Septiembre al 1 de Octubre de 2010

Editores:

Yannis Dimitriadis

María Jesús Verdú Pérez

ISBN: 978-84-693-5398-1

Editores: Yannis Dimitriadis, María Jesús Verdú Pérez, Universidad de Valladolid

Entidades colaboradoras:

Patrocinadores:

Presentación

Han pasado muchos años desde la primera edición de las Jornadas de Ingeniería Telemática (JITEL) que se celebraron en Bilbao en 1997. Desde entonces, cada dos años y recientemente cada año, las personas y las instituciones que trabajan en el área de Ingeniería Telemática se reúnen bajo el patrocinio de la Asociación de Telemática (ATEL). Estos lugares de encuentro propician la creación y fortalecimiento de una comunidad activa que debate, comparte y divulga los temas más importantes en el campo de sistemas, redes y servicios telemáticos.

Este año, las IX Jornadas de Ingeniería Telemática (JITEL 2010) se celebran en Valladolid del 29 de septiembre al 1 de octubre de 2010. La edición de JITEL 2010 tiene el privilegio de poder reforzar aún más la comunidad, ya que comparte espacio y tiempo con el mayor evento de Investigación, Desarrollo e Innovación en Telecomunicaciones en España, las XX Jornadas de Telecom I+D que tienen lugar entre el 27 y el 29 de septiembre en el mismo Palacio de Congresos Conde Ansúrez de Valladolid. Actividades compartidas de conferencias, mesas redondas y demostraciones podrán mejorar los lazos entre los diversos actores del sistema de I+D+i en el ámbito de Ingeniería Telemática. Se espera que esta iniciativa se pueda continuar en el futuro con aras de un mayor avance para la sociedad tanto en épocas de crisis como de crecimiento económico y social, de acuerdo con el lema principal de esta edición de Telecom I+D "Compromiso con la Sociedad".

Por otro lado, la innovación educativa cobra un mayor peso dentro de este ámbito ya que está directamente ligada con una mayor capacitación de los futuros profesionales de Ingeniería Telemática. Las I Jornadas de Innovación Educativa en Ingeniería Telemática (JIE) ocupan un espacio propio dentro de este evento, dado el reto de adaptación de los estudios en el nuevo Espacio Europeo de Educación Superior. Así, se espera que educación, investigación, desarrollo, innovación, y transferencia tecnológica den la mano tanto este año como en años posteriores.

Este libro de actas recoge las contribuciones que se presentan en sesiones de presentaciones orales, pósteres, o demostraciones de JITEL 2010. En esta edición se recibieron 70 artículos (además de los 16 artículos correspondientes a JIE 2010) para su publicación. Cada artículo se sometió a un proceso de revisión por parte de por lo menos 3 investigadores, bajo el auspicio del comité de programa que reúne todas las universidades españolas. Se empleó un riguroso proceso de selección que pretendió eliminar discrepancias entre revisores y llegar a un consenso basado en los méritos de originalidad, importancia y adecuación al área de ingeniería telemática. Como resultado de este proceso el comité de programa decidió publicar 48 artículos que se presentan de forma oral, mientras que otros 12 contribuciones se presentan en formato de pósteres. Hay que destacar una calificación adicional de cada artículo en función de su adecuación para los asistentes a Telecom I+D, que dio lugar a 12 artículos con "Sello Telecom I+D" que se presentan el día de solapamiento entre ambos congresos. Estos artículos, como los equivalentes de Telecom I+D con especial interés para los asistentes a JITEL, pretenden integrar reforzar todavía más los dos eventos.

El programa de las jornadas se completa con conferencias invitadas, así como una mesa redonda, demostraciones, casos de éxito y proyectos en el marco de las actividades conjuntas con Telecom I+D.

Tal y como es habitual, se otorgan unos premios que destacan la calidad extraordinaria de algunos artículos, en función de la valoración inicial por parte de los revisores externos, así como de revisores adicionales y de su presentación en el congreso. De forma adicional, los 6 mejores artículos de JITEL y Telecom I+D se publican en un número especial de la revista IEEE America Latina.

Es especialmente importante mencionar el auspicio de la Asociación de Telemática (ATEL) como entidad organizadora de JITEL 2010, como un foro que reúne personas y organismos, universidades, centros de investigación, empresas o fundaciones del área de Ingeniería Telemática. La asamblea anual y la reunión de socios de ATEL tienen lugar también dentro de este espacio de encuentro.

El apoyo de los patrocinadores y colaboradores (el Ministerio de Ciencia e Innovación, la Junta de Castilla y León, la Universidad de Valladolid, Telefónica I+D, y la sección española de IEEE) merece un agradecimiento. Su contribución es fundamental para que estas actividades se puedan llevar a cabo, y especialmente en épocas de recortes económicos.

Lo último, y quizás más importante, se refiere a todas las personas, actores humanos que dedican su energía, entusiasmo y capacidad profesional para llevar a cabo estos eventos. El comité de programa ha realizado una labor científica importante en el proceso de elaboración del programa, mientras que el comité organizador ha estado siempre activo para que las jornadas se lleven a cabo con éxito. Damos gracias al. Dr. Iván M. Jorrín Abellán por su aportación artística y desinteresada en la elaboración de logotipos, carteles y portadas. El agradecimiento a ambos comités es profundo.

Os damos la bienvenida a las IX Jornadas de Ingeniería Telemática (JITEL 2010), a sus actividades científicas, así como a la ciudad de Valladolid que pretende ofrecer una acogida llena de patrimonio histórico, cultural y gastronómico.

Valladolid, septiembre de 2010

Yannis Dimitriadis

María Jesús Verdú Pérez

Co-presidentes del Comité de Programa de JITEL 2010

Comité de Programa

Javier Aracil Rico (Universidad Autónoma de Madrid)
Marcelo Bagnulo Braun (Universidad Carlos III de Madrid)
Víctor M. Carneiro Díaz (Universidade da Coruña)
Guiomar Corral Torruella (Universitat Ramon Llull)
Carlos Delgado Kloos (Universidad Carlos III de Madrid)
Jesús E. Díaz Verdejo (Universidad de Granada)
Yannis Dimitriadis (Co-presidente) (Universidad de Valladolid)
Rafael M. Estepa Alonso (Universidad de Sevilla)
Santiago Felici Castell (Universitat de València)
Julián Fernández Navajas (Universidad de Zaragoza)
Roberto García Fernández (Universidad de Oviedo)
Sebastián García Galán (Universidad de Jaén)
Mercedes Garijo Ayestarán (Univ. Politécnica de Madrid)
Ana Gómez Oliva (Universidad Politécnica de Madrid)
Jesús M. González-Barahona (Universidad Rey Juan Carlos)
Antonio Gómez Skarmeta (Universidad de Murcia)
José Luis González Sánchez (Universidad de Extremadura)
Klaus Hackbart (Universidad de Cantabria)
Xavier Hesselbach Serra (Univ. Politècnica de Catalunya)
Guillermo Ibáñez Fernández (Universidad de Alcalá)
Eduardo Jacob Taquet (Euskal Herriko Unibertsitatea)
Josemaría Malgosa Sanahuja (Univ. Politécnica de Cartagena)
Pilar Manzanares López (Univ. Politécnica de Cartagena)
Jorge Martínez Bauset (Universitat Politècnica de València)
Jesús Martínez Cruz (Universidad de Málaga)
Daniel Morató Osés (Universidad Pública de Navarra)
Miquel Oliver Riera (Universitat Pompeu Fabra)
Magdalena Payeras Capellà (Universitat de les Illes Balears)
Manuel Ramos Cabrer (Universidade de Vigo)
Álvaro Suárez Sarmiento (Univ. de Las Palmas de Gran Canaria)
Juan R. Velasco (Representante de la Asociación de Telemática)
María Jesús Verdú Pérez (Co-presidenta) (Universidad de Valladolid)
José Vizcaíno de Hoyos (Representante de Telecom I+D 2010)

Comité Organizador

Míriam Antón Rodríguez (Universidad de Valladolid)
Juan Ignacio Asensio Pérez (Universidad de Valladolid)
Daniel Boto Giralda (Universidad de Valladolid)
José Fernando Díez Higuera (Universidad de Valladolid)
Yannis Dimitriadis (Co-presidente) (Universidad de Valladolid)
Eusebio Fernández López (Universidad de Valladolid)
Eduardo Gómez Sánchez (Universidad de Valladolid)
David González Ortega (Universidad de Valladolid)
Mario Martínez Zarzuela (Universidad de Valladolid)
Luisa M. Regueras Santos (Universidad de Valladolid)
Manuel Rodríguez Cayetano (Universidad de Valladolid)
José Antonio Sánchez (Universidad de Valladolid)
Federico Simmross Wattenberg (Universidad de Valladolid)
Elena Verdú Pérez (Universidad de Valladolid)
María Jesús Verdú Pérez (Co-presidenta) (Universidad de Valladolid)
Isabel de la Torre Díez (Universidad de Valladolid)

Revisores

Ramon Agüero (Universidad de Cantabria)
Mónica Aguilar (Universitat Politècnica de Catalunya)
Bernardo Alarcos (Universidad de Alcalá)
José M. Alcaraz Calero (Universidad de Murcia)
Jesús Alcober (Universitat Politècnica de Catalunya)
Álvaro Alesanco-Iglesias (Universidad de Zaragoza)
Luis Álvarez Sabucedo (Universidad de Vigo)
Manuel Álvarez-Campana (Universidad Politécnica de Madrid)
Pablo Ameigeiras Gutiérrez (Universidad de Granada)
Mercedes Amor (Universidad de Málaga)
José Manuel Arco (Universidad de Alcalá)
Juan Ignacio Asensio-Pérez (Universidad de Valladolid)
Marcelo Bagnulo Braun (Universidad Carlos III de Madrid)
Jaume Barceló (Universidad Carlos III de Madrid)
Boris Bellalta (Universitat Pompeu Fabra)
Carlos Bernardos Cano (Universidad Carlos III de Madrid)
Miguel L. Bote Lorenzo (Universidad de Valladolid)
Juan Felipe Botero (Universitat Politècnica de Catalunya)
María Victoria Bueno Delgado (Universidad Politécnica de Cartagena)
Sergio Cabrero (Universidad de Oviedo)
Javier Carmona-Murillo (Universidad de Extremadura)
Loren Carrasco (Universitat de les Illes Balears)
Vicente Casares-Giner (Universidad Politecnica de Valencia)
Guiomar Corral Torruella (Universitat Ramon Llull)
David Cortés Polo (Universidad de Extremadura)
Rubén Cuevas Rumín (Universidad Carlos III de Madrid)
Francisco De Toro Negro (Universidad de Granada)
Jesus E. Díaz Verdejo (Universidad de Granada)
Almudena Díaz Zayas (Universidad de Málaga)
José Fernando Díez-Higuera (Universidad de Valladolid)
Yannis Dimitriadis (Universidad de Valladolid)
Mª José Domenech Benlloch (Universidad Politécnica de Valencia)
Esteban Egea López (Universidad Politécnica de Cartagena)
Oscar Esparza (Universitat Politècnica de Catalunya)
Antonio Estepa (Universidad de Sevilla)
Guillem Femenias Nadal (Universitat de les Illes Balears)
Ángel Fernandez (Universidad Politécnica de Madrid)
David Fernández (Universidad Politécnica de Madrid)
Eusebio Fernández (Universidad de Valladolid)
Gregorio Fernández Fernández (Universidad Politécnica de Madrid)
Julián Fernández Navajas (Universidad de Zaragoza)
Javier Fernández-Sanguino Peña (Universidad Rey Juan Carlos)
Josep L. Ferrer Gomila (Universitat de les Illes Balears)
Jorge Fontenla González (Universidad de Vigo)
Vreixo Formoso (Universidade da Coruña)
Ignasi Furió (Universitat de les Illes Balears)

Jaime Galán-Jimenez (Universidad de Extremadura)
Juan José Gálvez García (Universidad de Murcia)
Alberto García (Universidad de Cantabria)
José García (Universidad de Zaragoza)
Marta García (Universidad de Cantabria)
Pedro García (Universidad de Granada)
Roberto García (Universidad de Oviedo)
Sebastián García Galán (Universidad de Jaén)
José Luis García Dorado (Universidad Autónoma de Madrid)
Ana Belén García Hernando (Universidad Politécnica de Madrid)
Alberto García Martínez (Universidad Carlos III de Madrid)
Antonio Javier García Sánchez (Universidad Politécnica de Cartagena)
Felipe García Sánchez (Universidad Politécnica de Cartagena)
Xabiel García Pañeda (Universidad de Oviedo)
Mercedes Garijo Ayestarán (Universidad Politécnica de Madrid)
Alfonso Gazo Cervero (Universidad de Extremadura)
José Manuel Giménez Guzmán (Universidad Politécnica de Valencia)
José Manuel Gimenez Guzman (Universidad de Alcalá)
Félix Gómez Mármol (Universidad de Murcia)
Eduardo Gómez Sánchez (Universidad de Valladolid)
Antonio Gómez Skarmeta (Universidad de Murcia)
Jesús M. González Barahona (Universidad Rey Juan Carlos)
Carlos González Martínez (Universidad Politécnica de Madrid)
Eduardo Grampin (Universidad Carlos III de Madrid)
Juan Carlos Guerri (Universidad Politécnica de Valencia)
Klaus Hackbarth (Universidad de Cantabria)
José Alberto Hernández (Universidad Carlos III de Madrid)
Ángela Hernández Solana (Universidad de Zaragoza)
Xavier Hesselbach Serra (Universitat Politècnica de Catalunya)
Xisca Hinarejos (Universitat de les Illes Balears)
Enrique de la Hoz (Universidad de Alcalá)
Maider Huarte Arrayago (Euskal Herriko Unibertsitatea)
Llorenç Huguet Rotger (Universitat de les Illes Balears)
Carlos A. Iglesias (Universidad Politécnica de Madrid)
José Ángel Irastorza (Universidad de Cantabria)
Mikel Izal (Universidad Pública de Navarra)
David Larrabeiti (Universidad Carlos III de Madrid)
Ana Lobo (Universidad de Oviedo)
Miguel A. López Carmona (Universidad de Alcalá)
Gabriel López Millán (Universidad de Murcia)
Javier López Muñoz (Universidad de Málaga)
Jorge López de Vergara (Universidad Autónoma de Madrid)
Gabriel Maciá Fernández (Universidad de Granada)
Elsa María Macías López (Universidad de Las Palmas de Gran Canaria)
Germán Madinabeitia (Universidad de Sevilla)
Eduardo Magaña (Universidad Pública de Navarra)
José A. Mañas (Universidad Politécnica de Madrid)
Rafael Marín (Universidad de Murcia)
Domingo Marrero Marrero (Universidad de Las Palmas de Gran Canaria)
Iván Marsá Maestre (Universidad de Alcalá)
Israel Martín Escalona (Universitat Politècnica de Catalunya)

Jorge Martínez Bauset (Universidad Politécnica de Valencia)
Jesús Martínez Cruz (Universidad de Málaga)
Eduardo Martínez Gracia (Universidad de Murcia)
Antonio Martínez Mas (Universidad Politécnica de Madrid)
Gregorio Martínez Pérez (Universidad de Murcia)
Felipe Mata (Universidad Autónoma de Madrid)
Jorge Mata (Universitat Politècnica de Catalunya)
Jon Matías (Euskal Herriko Unibertsitatea)
David Melendi (Universidad de Oviedo)
Pedro Merino Gómez (Universidad de Málaga)
David Montoro (Universidad Politécnica de Cartagena)
Daniel Morató (Universidad Pública de Navarra)
Juan Pedro Muñoz Gea (Universidad Politécnica de Cartagena)
Macià Mut Puigserver (Universitat Illes Balears)
Andrés Navarro (Universidad de Alcalá)
Juan Luis Navarro Mesa (Universidad de Las Palmas de Gran Canaria)
Jorge Navarro Ortiz (Universidad de Granada)
López Nores Martín (Universidade de Vigo)
Antonio de la Oliva Delgado (Universidad Carlos III de Madrid)
Miquel Oliver (Universitat Pompeu Fabra)
Jordi Ortiz Murillo (Universidad de Murcia)
Alberto Pan Bermúdez (Universidad de A Coruña)
Iván Pau de la Cruz (Universidad Politécnica de Madrid)
Pablo Pavón Mariño (Universidad Politécnica de Cartagena)
Magdalena Payeras Capellà (Universitat de les Illes Balears)
Andreu Pere Isern-Deyà (Universitat de les Illes Balears)
Fernando Pereñiguez García (Universidad de Murcia)
Rocío Pérez de Prado (Universidad de Jaén)
Pedro José Piñero Escuer (Universidad Politécnica de Cartagena)
Vicent Pla (Universidad Politécnica de Valencia)
Jaume Ramis Bibiloni (Universitat de les Illes Balears)
Javier Ramos (Universidad Autónoma de Madrid)
Manuel Ramos Cabrer (Universidade de Vigo)
Juan José Ramos Muñoz (Universidad de Granada)
Felip Riera (Universitat de les Illes Balears)
David Rincón (Universitat Politècnica de Catalunya)
Casiano Rodríguez (Universidad de La Laguna)
Manuel Rodríguez Cayetano (Universidad de Valladolid)
Laura Rodriguez de Lope-López (Universidad de Cantabria)
Francisco Javier Rodríguez Pérez (Universidad de Extremadura)
Gregorio Rubio Cifuentes (Universidad Politécnica de Madrid)
Pedro M. Ruiz (Universidad de Murcia)
Antonio Ruiz Martínez (Universidad de Murcia)
José Ruiz Mas (Universidad de Zaragoza)
F. Javier Ruiz Piñar (Universidad Politécnica de Madrid)
Alberto Salmerón (Universidad de Málaga)
Alfredo Salvador (Universidad Autónoma de Madrid)
Luis Sánchez (Universidad de Cantabria)
Antonio Javier Sánchez-Esquevillas (Universidad de Valladolid)
Pedro Santiago del Rio (Universidad Autónoma de Madrid)
Roberto Sanz (Universidad de Cantabria)

Federico Simmross-Wattenberg (Universidad de Valladolid)
Juan Bautista Tomás Gabarrón (Universidad Politécnica de Cartagena)
Antonio Urbano Fullana (Universitat de les Illes Balears)
Francisco Valera (Universidad Carlos III de Madrid)
Enrique Vázquez (Universidad Politécnica de Madrid)
Guillermo Vega Gorgojo (Universidad de Valladolid)
Elena Verdú Pérez (Universidad de Valladolid)
María Jesús Verdú Pérez (Universidad de Valladolid)
José R. Vidal Catalá (Universidad Politécnica de Valencia)
Juan Carlos Yelmo (Universidad Politécnica de Madrid)
Johan Zuidweg (Universitat Pompeu Fabra)

Contenido

Artículos

S1A. Artículos con sello de interés para Telecom I+D (I)

S1B. Artículos con sello de interés para Telecom I+D (II)

S2A. ANÁLISIS DE PRESTACIONES Y MODELADO DE REDES TELEMÁTICAS I

S2B. REDES INALÁMBRICAS I

S3A. REDES INALÁMBRICAS II

S4A. ANÁLISIS DE PRESTACIONES Y MODELADO DE REDES TELEMÁTICAS II

S5A. SEGURIDAD

S5B. SOCIEDAD DE LA INFORMACIÓN Y SERVICIOS DOMÉSTICOS

S6A. INFRAESTRUCTURAS Y SERVICIOS DE PRÓXIMA GENERACIÓN

S6B. REDES AD-HOC Y REDES DE SENSORES

Pósteres

Demostraciones

Entornos de verificación de soluciones multi-path BGP

Lisardo Prieto González, José Manuel Camacho Camacho, Francisco Valera Pintor
Ingeniería Telemática,
Universidad Carlos III de Madrid
Avda. de la Universidad, 30, 28911 Leganés (Madrid) España
{lpgonzal, jcamacho, fvalera}@it.uc3m.es

***Resumen*-. Actualmente la utilización simultánea de múltiples caminos en redes de comunicaciones tiene el potencial de generar una serie de importantes beneficios como la mejor utilización de los recursos disponibles o la mayor robustez y protección de las transmisiones. Sin embargo, las soluciones existentes hoy en día para dotar a los routers de un paradigma multi-camino no pasan de ser propuestas aisladas o soluciones concretas intra-dominio. Entre otras cosas, esto se debe a las dificultades de probar y validar las diferentes soluciones como a las dificultades de un posterior despliegue. En este artículo se propone un entorno desarrollado para poder verificar soluciones multi-path inter-dominio (BGP) tanto por la vía de la simulación como por la vía de la implementación real de la solución. Se describirá también cómo se ha validado la propuesta con dos soluciones actualmente en desarrollo, habiéndose detectado así en ellas problemas de convergencia.**

***Palabras Clave*- encaminamiento, multi-path, BGP, simulación, emulación, virtualización, C-BGP, XORP.**

I. INTRODUCCIÓN

Las técnicas de encaminamiento multi-camino (en adelante *multi-path routing*) ponen a disposición de los routers diferentes alternativas para alcanzar un destino concreto que pueden ser usadas de forma concurrente ateniéndose a ciertas restricciones (como que las rutas estén libres de bucles por ejemplo). Esto es posible gracias a la instalación en la tabla de encaminamiento de un router de diferentes 'siguientes saltos' hacia el mismo destino para que los utilice todos simultáneamente.

El encaminamiento multi-path tiene una serie de ventajas potenciales muy notables debido a las cuales está recibiendo cada vez más atención. Por ejemplo ([1], [2]):

- Incremento efectivo de la capacidad de la red al permitir que el tráfico se envíe por un mayor número de enlaces.
- Respuesta más rápida a cambios en la red, puesto que ya se han explorado y puesto en funcionamiento diferentes caminos.
- Ingeniería de tráfico escalable, ampliando las posibilidades a la hora de poder configurar los caminos utilizados para optimizar retardos.
- Mejoras en la seguridad, proporcionando protección por ejemplo frente a ataques de denegación de servicio o de inspección de paquetes.

Actualmente existen diferentes soluciones desplegadas en Internet, pero prácticamente todas en el dominio de un único proveedor (intra-dominio) y basadas en protocolos IGP, como el encaminamiento multi-topología de OSPF [3] o el balanceo de carga propuesto por EIGRP [4] o M-PATH [5].

En el caso de entornos inter-dominio, el despliegue de soluciones es mucho menor y aunque es cierto que existen alternativas que proporcionan una mayor variedad de caminos, son en general soluciones muy específicas (habilitar múltiples enlaces entre proveedores, soluciones con encaminamiento basado en fuente, etc. Ver [1]).

No obstante, el creciente interés por las ventajas que ofrecen las alternativas multi-path ha llevado a multitud de propuestas que persiguen dotar de dicha versatilidad al protocolo BGP (ver prospectiva en [1] y [2]).

El proyecto Trilogy (*ICT-2007-216372, Architecting The Future Internet*, [6]) tiene como principal objetivo el desarrollo de nuevas soluciones para la arquitectura de control de Internet (a nivel de routing, control de congestión, etc.). En este proyecto se está prestando una atención especial a diferentes soluciones multi-path, como la propuesta en la capa de transporte, mTCP [7] o diferentes extensiones para multi-path BGP (LP-BGP [8] y MpASS [1]).

Uno de los principales problemas encontrados en el desarrollo de soluciones multi-path BGP es la dificultad para validar dichas propuestas y sobre todo para compararlas con otras alternativas en contextos reales, tanto a nivel de tamaño de la red como a nivel de relaciones reales entre proveedores. En general cada propuesta utiliza un mecanismo diferente de validación (teórico, desarrollo de un software específico para la situación, etc.) y eso evidentemente complica considerablemente la comparación entre ellos o con cualquier otro mecanismo que se pueda proponer.

En este artículo se propone un entorno de verificación de soluciones multi-path BGP, con un doble desarrollo basado en simulación y en emulación real que ha permitido por ejemplo probar las dos soluciones que se han planteado en Trilogy (LP-BGP y MpASS) y detectar problemas de convergencia en dichas soluciones. El artículo describe el trabajo realizado para tratar de objetivar la comparativa entre soluciones multi-path de tal forma que sea sencillo evaluar

diferentes alternativas contrastándolas entre ellas. El entorno es fácilmente extensible y adaptable a las diversas soluciones que se quieran comparar.

El resto del artículo está organizado como sigue. En la sección II se detallan las diferentes alternativas consideradas antes de proceder al desarrollo de extensiones para dos de ellas: C-BGP y XORP. En las secciones III y IV se explican las extensiones desarrolladas y en la sección V se comenta cómo se han utilizado para validar las propuestas de multi-path BGP que se están trabajando en el proyecto Trilogy. Por último, en la sección VI se presentan las principales conclusiones y una serie de líneas de trabajo futuro.

II. ESTADO DEL ARTE

Actualmente se ha observado que las diferentes soluciones que se han propuesto para proporcionar una alternativa multi-path a BGP son validadas o bien únicamente de forma teórica o bien en base a desarrollos específicos para la propuesta en cuestión que impide la comparación entre las diversas alternativas.

Para desarrollar un entorno flexible que permita evaluar diferentes facetas de las soluciones que se estén considerando, se optó por un lado por utilizar técnicas de simulación, que permitiesen valorar de forma sencilla los resultados obtenidos tras la convergencia (ver sección V) sin tener en cuenta los efectos más complejos derivados de la evolución temporal del protocolo. El objetivo de este entorno es poder integrar de forma sencilla las propuestas que se quieran comparar, admitiendo incluso configurar cada router con una variante multi-path distinta.

De forma complementaria se ha habilitado también una implementación real para permitir lo mismo que la opción de la simulación para poder examinar el detalle de la evolución del protocolo. Por último, se ha recurrido también a técnicas de virtualización con el doble objetivo de simplificar por un lado los experimentos de laboratorio evitando la configuración de equipos físicos y por otro aumentando el tamaño de la red que se puede utilizar en la validación.

En esta sección se describen las diferentes herramientas que se han considerado como alternativas a las opciones finalmente utilizadas.

A. Simulación

Puesto que el objetivo de este enfoque es el de ampliar las funcionalidades de simuladores existentes para darles soporte multi-path, se evaluaron dos de los principales simuladores de código abierto con soporte para BGP: C-BGP [9] y NS-2/BGP++ [10].

C-BGP está especializado en simular el proceso de decisión de BGP basándose en la configuración de cada router, las rutas externas de BGP recibidas y la topología de la red.

El objetivo del simulador es ser usado como una herramienta de investigación para experimentar con procesos de decisión modificados y atributos adicionales de encaminamiento en BGP. También puede ser utilizado por el administrador de un ISP para evaluar el posible impacto de cambios lógicos y topológicos de las tablas de rutas calculadas en sus routers físicos. Los cambios topológicos incluyen caídas de enlaces y de routers. Los fallos lógicos contemplan modificaciones en la configuración de los routers, tales como las políticas de entrada y salida de tráfico o los pesos de los enlaces IGP. Gracias a su eficiencia, C-BGP puede ser utilizado en topologías muy grandes, del mismo tamaño en orden de magnitud que Internet.

Está programado en C y principalmente es utilizado y probado en máquinas con GNU/Linux y MacOS. También se puede utilizar en otras plataformas como FreeBSD, Solaris y Windows.

Por otro lado, BGP++ es una implementación en C++ de BGP para los simuladores de red NS-2 [11] y GTNetS [12]. BGP++ es una modificación del paquete software Zebra BGPd [13] para trabajar con los simuladores citados. BGP++ intenta mantener la mayor parte de la funcionalidad de Zebra BGPd mientras que incorpora dichas características en un potente entorno de simulación. La ventaja de este enfoque es que ahorra esfuerzo de desarrollo ya que los algoritmos no son reescritos y ya han sido validados.

Una característica muy útil de BGP++ es que mantiene la sintaxis de configuración que se utiliza en Zebra BGPd para configurar los routers.

Al igual que en el caso de C-BGP, BGP++ principalmente se utiliza en entornos Linux, pero puede ser compilado para Windows utilizando Cygwin.

Ambas alternativas se han comparado de cara a seleccionar la más adecuada para los objetivos propuestos.

En lo concerniente al tiempo necesario para obtener los resultados de la simulación, en escenarios idénticos las simulaciones tienen una duración menor en C-BGP. Además, el consumo de memoria de C-BGP es significativamente menor. Sin embargo, cabe destacar que el simulador de red C-BGP no permite simular aspectos relacionados con la dinámica de BGP, ya que el modelo de encaminamiento que emplea no simula el envío de mensajes BGP sobre conexiones TCP. Tampoco contempla el establecimiento de sesión ni temporizadores [14], al contrario que BGP++, el cual corre sobre un simulador a nivel de paquetes como es NS-2 y sí los contempla

En una primera revisión del código fuente de ambos se apreció que podría resultar mucho más sencillo modificar C-BGP que BGP++, entre otros motivos porque el último es dependiente del simulador NS-2 (el cual debe ser modificado para su instalación) y además de modificar el protocolo implementado en BGP++, habría que modificar los vínculos con NS-2. Se observó también que C-BGP implementa una serie de métodos para JNI (*Java Native Interface*), esto es, permite que aplicaciones desarrolladas en lenguaje Java puedan utilizar las funcionalidades proporcionadas por el simulador aun estando escritas en diferente lenguaje de programación.

Con respecto a la escalabilidad, C-BGP es capaz de simular topologías del tamaño de Internet con hardware limitado [15], mientras que con NS-2/BGP++ se requiere un entorno con múltiples máquinas trabajando en paralelo de forma distribuida, esto es, requiere un mayor número de recursos para obtener resultados de convergencia.

En conclusión, el entorno de simulación elegido sobre el que realizar las diferentes modificaciones para dar soporte multi-path fue C-BGP, principalmente debido a su eficiencia y bajo consumo de recursos.

B. Emulación real

La utilización de herramientas como C-BGP es realmente útil para obtener resultados preliminares sobre la convergencia y las tablas de rutas generadas por el protocolo bajo análisis con relativa rapidez. Sin embargo tal y como se apuntó en la sección anterior C-BGP prescinde de los aspectos relacionados con la dinámica del protocolo como por ejemplo el orden de ocurrencia de eventos.

Aunque otros simuladores (como NS-2/BGP++) permiten el estudio de la dinámica de los protocolos, para completar el entorno de simulación se ha preferido optar por la implementación real que permita incluso el despliegue de las soluciones en equipos reales.

En esta sección se tratarán dos implementaciones *open source* del protocolo BGP. El objetivo es analizar las posibilidades de modificar software BGP añadiendo soporte multi-path para su posterior utilización sobre un *testbed* real (o virtualizado). En concreto se presentarán en esta sección los paquetes de software para routing Zebra [13] y XORP [16].

1. GNU Zebra – routing software

El paquete de routing Zebra contiene una estructura modular que permite lanzar varios procesos de routing simultáneamente. En otras palabras, Zebra permite ejecutar diferentes protocolos de routing en la misma máquina de manera independiente. Además de las ventajas que esto proporciona a los administradores de la red a la hora de actualizar y configurar el router, puede ser muy interesante de cara a analizar la interacción de las soluciones multi-path BGP con otro protocolos, como por ejemplo los de routing intra-dominio (RIP, OSPF, etc.), sin necesidad de instalar software adicional.

Zebra está disponible para Linux y la mayoría de plataformas BSD. También es posible disponer de Zebra en sistemas Linux embebidos como OpenWRT [20]. Los protocolos soportados por Zebra para IPv4son los siguientes: RIPv1, RIPv2, RIPng, OSPF, IGMP y BGP4+.

La eficiencia en la implementación de Zebra es una de sus principales ventajas, el consumo de RAM del proceso de BGP de Zebra está entorno a 20Mb. Entre las limitaciones que encontramos para su utilización en nuestros experimentos con multi-path BGP están la escasa documentación para desarrolladores con la que cuenta el proyecto y el uso del plano de *forwarding* del *kernel* del sistema operativo, lo que en caso de querer mantener dos o más entradas por prefijo en la tabla de rutas nos forzaría a parchear el kernel del sistema operativo.

2. XORP

El proyecto de routing XORP es probablemente el paquete software más modular, flexible y completo para crear un router existente a día de hoy. Tanto es así que ha sido adoptado por fabricantes de routers de bajo coste como Vyatta [18] como solución software para sus productos.

Además de la modularidad de su diseño y su disponibilidad para los sistemas operativos más populares (Linux, BSD, Mac OSX y Windows Server 2003), cuenta con una extensa documentación para desarrolladores y una API abierta la cual puede facilitar la implementación de una solución de routing multi-path.

XORP soporta los siguientes protocolos de routing: RIPv1, RIPv2, RIPng, OSPF, IGMP, BGP, MLD, PIM-SM y MIBs para SNMP.

Otra de las ventajas de XORP es su integración con CLICK (router software modular) [19] lo que permite el diseño de un plano de *forwarding* para soporte de múltiples entradas por prefijo más sencillo sin necesidad de modificar el *kernel* directamente. Además de cara a contar con más interfaces de red, XORP soporta la creación de routers distribuidos, esto es, un equipo ejecuta los procesos de routing (OSPF, BGP, etc.) y el resultado de los mismos es instalado en las tablas de rutas de equipos diferentes (tal y como se muestra en la Figura 1) gracias a un módulo especial llamado el *forwarding engine abstraction* (FEA) [17].

Entre las desventajas de XORP se encuentra su falta de eficiencia en términos de consumo de memoria. A diferencia de Zebra que utilizaba entorno a 20Mb, XORP consume unos 100Mb (a lo que hay que añadir el tamaño de la RIB que dependerá de la topología y los prefijos anunciados). Finalmente, XORP fue elegido para implementar las soluciones multi-path debido a su modularidad y por ser fácilmente extensible.

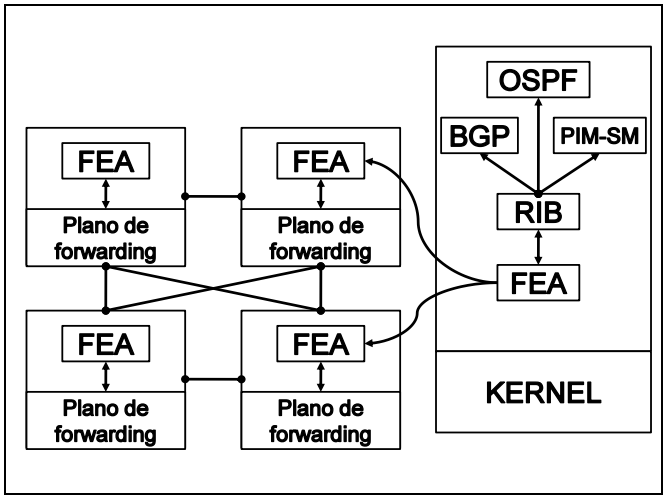


Figura 1. Plano de *forwarding* distribuido en varios equipos.

C. **Virtualización**

En el apartado anterior presentamos implementaciones de BGP fácilmente extensibles a un escenario multi-path. Si se pretenden utilizar estas implementaciones para la verificación de dichas extensiones multi-path va a resultar imprescindible el despliegue de una maqueta de red (*testbed*).

A la hora de verificar los protocolos sobre topologías de cierto tamaño, la necesidad de un número elevado de equipos puede suponer una limitación tanto en términos de coste económico como en términos de la complejidad de su instalación y monitorización. Afortunadamente este problema también se da en los servidores de aplicaciones de Internet, lo que ha dado lugar a la proliferación de herramientas de virtualización que permiten la configuración y emulación de múltiples máquinas (virtuales) sobre un mismo equipo (físico).

Los principales requisitos que se buscan en una solución de virtualización son: (1) eficiencia y baja sobrecarga de CPU, (2) soporte para virtualizar redes, (3) máximo número de interfaces de red por cada máquina virtual, (4) posibilidad de utilizar imágenes de máquinas virtuales con OpenWRT+Zebra [20] y GNU/Linux+XORP. El uso de dichas imágenes puede facilitar la migración de las modificaciones multi-path de BGP a routers físicos reales como los Linksys WRT54G [21] y los ya citados routers Vyatta.

III. MC-BGP

Para dotar al simulador de red C-BGP de soporte multi-path es necesario realizar una serie de cambios en su arquitectura. Dichos cambios comprenden tanto las estructuras de datos internas que definen los routers BGP como las funciones empleadas para mostrar información y ejecutar el proceso de selección de rutas.

Además de dotar al simulador de soporte multi-path, se han añadido funcionalidades extra, modificando la gramática de comandos empleada por el mismo. Dichas funcionalidades resultan muy útiles a la hora de obtener resultados necesarios en las métricas para la evaluación de las modificaciones sobre BGP. Las funcionalidades añadidas son:

- Mostrar y asignar el tipo de protocolo multi-path a emplear por un determinado router BGP, permitiendo que cada router utilice incluso un protocolo diferente. Esto permite por ejemplo validar el impacto de la introducción de la solución únicamente en una parte de la red (en el núcleo por ejemplo) o la compatibilidad entre soluciones.
- Mostrar la *FIB* (*Forwarding Information Base*) almacenada por un determinado router BGP para poder analizar el detalle de la evolución del protocolo.
- Mostrar el número de bucles detectados al ejecutar el protocolo multi-path en un determinado router BGP para evaluar la convergencia.
- Mostrar y asignar el máximo nivel de agregación de rutas en un determinado router BGP.
- Mostrar el número de mensajes enviado entre los distintos routers hasta que converge. Esto será posteriormente considerado como una métrica más de comparación (ver sección V).

A. Soporte multi-path

El simulador de red C-BGP está compuesto por tres capas principales: planificador, simulación IP y simulación BGP [9]. La capa del planificador es la parte central del simulador. Contiene la secuencia de eventos pendientes que representan los mensajes a ser enviados hacia determinados nodos de la red. El planificador mete en una cola los nuevos eventos cuando un nodo envía un mensaje a otro. Esos mensajes son posteriormente extraídos de la cola y enviados al nodo correspondiente.

El primer componente de la capa de simulación es una representación de la capa IP de la topología de red modelada. Esto es básicamente una estructura de datos que mantiene un grafo de nodos y enlaces. El segundo componente es un modelo estático IGP. Este modelo es responsable de calcular las rutas intra-dominio para cada dominio IGP, basándose en el conocimiento de la topología al completo. Las rutas intra-dominio se almacenan en una tabla de rutas junto con las rutas estáticas (configuradas manualmente). Por último, el tercer componente de la capa de simulación IP es el modelo de router IP el cual es responsable de enviar mensajes a la capa BGP si el mensaje tiene destino local o de reenviar el mensaje a otro nodo si el mensaje debe ser entregado a un destino remoto.

Finalmente, la capa de simulación BGP también contiene una serie de componentes. El primer componente es la configuración de la capa BGP. Esto incluye el grafo de las sesiones BGP al igual que la configuración de los distintos routers BGP en la red modelada. El segundo componente de la capa de simulación BGP es el modelo de routing BGP. Este modelo contiene el proceso de decisión y los filtros de routing. El modelo de routing BGP depende de una serie de tablas de rutas las cuales contienen las rutas BGP conocidas por cada router BGP y las mejores rutas seleccionadas por cada uno de ellos.

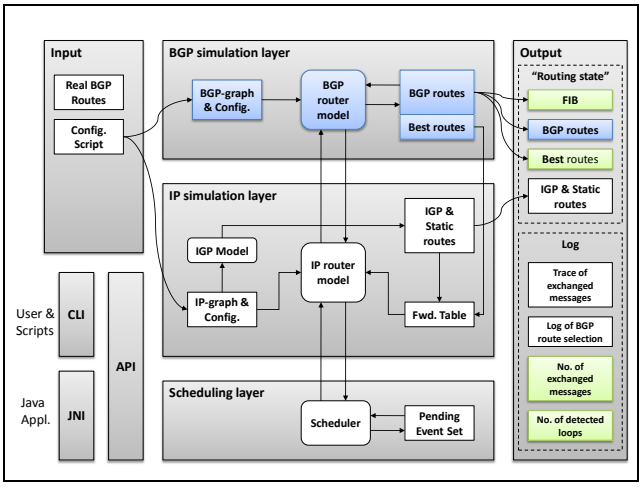


Figura 2. Arquitectura mC-BGP

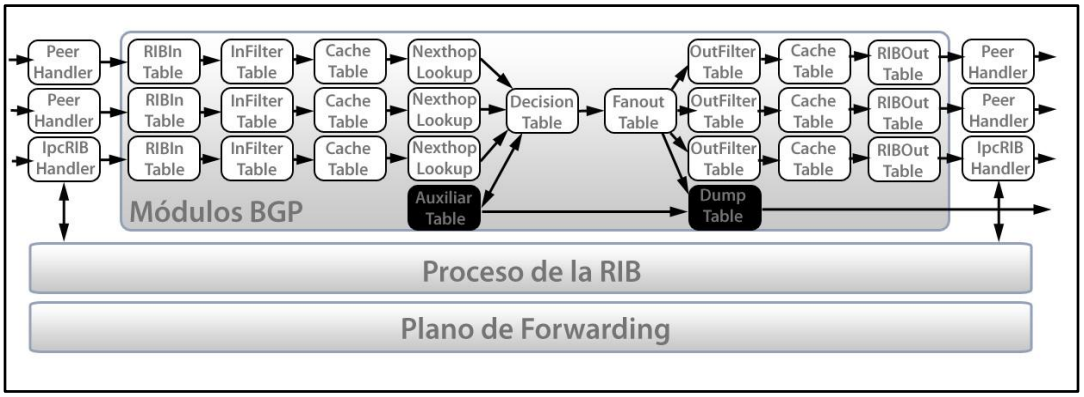


Figura 3. Módulos del proceso BGP de XORP.

En la Figura 2 se pueden apreciar los cambios necesarios sobre la arquitectura de C-BGP para dotarlo de soporte multi-path. Fue necesario ampliar el módulo "*BGP-graph & Config.*" para incluir las opciones relativas a los nuevos parámetros de configuración (tipo de variante de BGP a utilizar, máxima agregación). También se ampliaron los módulos correspondientes al modelo del router BGP ("*BGP Router Model*") para añadir los procesos de decisión alternativos y las estructuras de datos necesarias para almacenar información como los bucles detectados y el módulo correspondiente a las rutas BGP ("*BGP Routes*"), siendo necesario en este caso añadir las estructuras correspondientes a la FIB y a los AS_SETs (estructura utilizada en algunas soluciones y no soportada inicialmente por el simulador) así como las funciones necesarias para manejarlos.

Además, se observó que el simulador carecía de métodos para gestionar los AS_SETs en los AS_PATHs, de forma que se añadieron funciones encargadas de ello, y se modificaron los métodos encargados de mostrar las rutas en la salida, ya que en algunos casos podría ser necesario incluir la información contenida en dichos AS_SETs para el AS_PATH. El soporte de AS_SETs se proporcionó a través de una estructura dinámica de alto rendimiento (array dinámico de enteros con inserción y acceso basado en búsqueda binaria).

Igualmente se implementaron nuevas funciones correspondientes a los módulos "*FIB*", "*Best routes*", "*No. Of Exchanged Messages*" y "*No. of detected loops*" con el fin de mostrar la información relativa a dichos módulos por la salida del simulador.

IV. MXORP

En esta sección se detallan las modificaciones que se pueden realizar en el proceso BGP de XORP para implementar protocolos multi-path. Para comprender las modificaciones realizadas nos referiremos a la estructura del proceso BGP descrita en la Figura 3.

A. El Proceso BGP Estándar

Cada *PeerHandler* representa una sesión BGP sobre TCP. Cada vez que se recibe un UPDATE de BGP, se desglosa en uno o varios mensajes internos ADD_ROUTE, DELETE_ROUTE y REPLACE_ROUTE. Por ejemplo, cuando un *peer* anuncia que se puede alcanzar un nuevo prefijo a través de él a este router, un mensaje ADD_ROUTE atraviesa la cadena de componentes de la rama de entrada a la que está conectado el *PeerHandler*. El mensaje se va modificando a lo largo de la rama, hasta llegar al *DecisionTable* (o ser filtrado) donde la ruta que contiene se somete al proceso de decisión del protocolo BGP. Si la ruta resulta ganadora, se generarán dos mensajes que atravesarán todas las ramas de salida, un DELETE_ROUTE para la antigua ruta ganadora/anunciada y un ADD_ROUTE para la nueva, que se traducirá a un UPDATE de BGP al resto de *peers* de este router. Existe una rama especial que no conecta con otro *peer* sino con el proceso XORP que se encarga de popular la decisión en la RIB. En algunos protocolos (ver [1]), la información que atraviesa esta rama puede ser diferente de la que se propaga por el resto (hacia los *peers*).

El módulo *DecisionTable* a la hora de decidir la mejor ruta para un determinado prefijo de red, obtiene todas las rutas anunciadas para ese prefijo, consultando la *RibInTable* de cada una de las ramas de entrada y aplicando el proceso de decisión a ese conjunto de rutas. La ruta seleccionada para ser anunciada al resto de *peers* y ser instalada en la FIB se pasa al módulo *FanoutTable*. Este módulo duplica los mensajes internos resultados de la decisión en cada una de las ramas, así se consigue realizar cambios en el estado del proceso una vez y éstos son propagados independientemente para cada *peer*.

Además del anuncio o retirada de rutas para un determinado prefijo, otro evento bastante común es el establecimiento de una nueva sesión BGP con un *peer* que acaba de arrancar o recuperarse de una caída. Para ese caso particular XORP define un nuevo módulo (*DumpTable*) que se encarga de volcar la información de routing de este router al nuevo *peer* para que pueda construir su RIB de manera consistente. El volcado se realiza en segundo plano y utiliza un complejo proceso de sincronización, puesto que nuevos eventos de rutas pueden ocurrir en mitad del volcado y dejar al nuevo *peer* con información inconsistente o desactualizada. Para obtener esta sincronización, el módulo *DumpTable* no obtiene la información a volcar de la RIB directamente, sino que procesa una por una las *RibInTable* de cada rama y envía al nuevo *peer* las rutas que fueron marcadas como propagadas (o ganadoras en terminología XORP) la última vez que el proceso de decisión BGP se ejecutó para un prefijo en concreto.

B. Modificaciones en los bloques para soportar multi-path

Tras introducir el funcionamiento del proceso BGP de XORP, se pueden identificar varios módulos clave para posibles extensiones multi-path. Tanto el filtrado de los mensajes internos como la caché se pueden configurar y deshabilitar mediante los ficheros de configuración, y salvo que se necesiten añadir filtros más complejos que los existentes para BGP estándar, estos módulos no deberían ser modificados para soportar multi-path. El módulo *Next-HopLookup* simplemente se encarga de verificar que existe un siguiente salto para un prefijo determinado, por lo que tampoco necesita ser modificado.

Todos los módulos excepto el *PeerHandler* implementan una interfaz llamada *RouteTableBase*, la cual permite que los módulos intercambien mensajes internos y soliciten o notifiquen información sobre rutas entre ellos. La principal limitación de la definición de esta interfaz es que sólo permite operaciones sobre una ruta por prefijo en cada llamada entre módulos. Dependiendo de las necesidades de cada implementación se puede elegir entre modificar los mensajes internos para que encapsulen información sobre varias rutas de manera simultánea o sobrecargar la interfaz para que soporte operaciones que utilicen o devuelvan como resultado un set de rutas en lugar de una única ruta. Esta última opción, a pesar de que necesita reescribir todos los módulos que implementan *RouteTableBase* es la más amigable con el procesado que internamente realiza cada módulo, ya que se pueden implementar las funciones multi-path basándose en múltiples llamadas a las funciones originales.

1. Protocolos que preservan mensajes BGP

Una vez modificada la interfaz, para extensiones multi-path en las cuales cada *peer* anuncia única ruta por prefijo, las modificaciones se centran principalmente en (1) el *DecisionTable*, donde el proceso de selección de rutas puede ser modificado para marcar varias rutas como *ganadoras* del proceso. (2) En el *FanoutTable*, ya que en este tipo de modificaciones, sólo una de las rutas resultado del proceso de selección es propagada a través de las ramas que finalizan en un módulo *PeerHandler* para ser anunciada. El resto de rutas se almacenarán en la RIB, por lo que se propagarán por la rama acabada en el *IpcRIBHandler* que comunica con el proceso de control de la RIB.

2. Protocolos con múltiples rutas por anuncio

Si por el contrario, el protocolo que queremos evaluar soporta que cada *peer* pueda anunciar múltiples rutas para un mismo destino (BGP no soporta esta opción), entonces deben realizarse más cambios, especialmente en lo que concierne al *RibInTable* y al *RibOutTable*. En estos módulos toda la información enviada desde/hacia un *peer* queda registrada en una estructura de datos. Si múltiples rutas para un mismo prefijo son anunciadas por un mismo *peer*, los módulos actuales no necesitan ninguna estructura extra de datos (a pesar de que en BGP cada anuncio reemplaza al anterior). El problema viene a la hora de obtener información acerca de un determinado prefijo desde otros módulos en la *RibInTable* o pasar múltiples rutas desde la *RibOutTable* al *PeerHandler*.

Por ejemplo, la función correspondiente de la *RibInTable* obtiene todas las registradas en la estructura de datos cuando se solicita una búsqueda, pero sólo devuelve la marcada como *en uso*. Al sobrecargar la interfaz *RouteTableBase* este problema se soluciona, pasando al siguiente módulo un set de rutas marcadas como *en uso*. En el caso de la *RibOutTable*, si múltiples rutas con el mismo prefijo llegan al módulo mientras el *PeerHandler* está actualmente enviando, el módulo pondrá en la cola de espera para ser anunciada a la ruta más reciente. Esto debe modificarse para que se añadan a la cola múltiples rutas para un prefijo. Como construir los mensajes que intercambian los *peers* es tarea del *PeerHandler* y queda abierto a la definición del protocolo.

3. Protocolos que alteran las rutas recibidas

Si el protocolo crea la(s) ruta(s) a propagar a partir de las que reciba (por ejemplo agregando AS_NUMBERS en un AS_SET, ver [1]), se necesita un módulo adicional que extienda de *RibInTable* para almacenar esta(s) nueva(s) ruta(s) creada(s) en el proceso de selección (ver *AuxiliarTable* en la Figura 3). Si esto sucede, el procesado del módulo *DumpTable* se simplifica puesto que todas las rutas a volcar al nuevo *peer* se encuentran almacenadas en este módulo adicional.

4. Cambios en la RIB y FIB

El proceso que controla la RIB debe ser modificado para almacenar múltiples rutas por prefijo, la RIB debe contener el set de rutas *válidas* obtenido en el proceso de decisión, y éste puede ser un super-set o un sub-set de las rutas propagadas a los *peers*. Posteriormente, ese conjunto de rutas se instalarán en el plano de *forwarding* para su uso. En la siguiente sección se indican algunas alternativas compatibles con XORP para crear una FIB con múltiples entradas.

V. VALIDACIÓN

La validación de los entornos propuestos para verificación de multi-path BGP se realizó utilizando versiones modificadas de C-BGP y XORP. Para la ejecución de los routers XORP se utilizó el sistema de virtualización XenServer [24] por cumplir con todos los requisitos de la sección II.C. y basándonos en la comparativa entre sistemas de virtualización publicada en [25]. Además el proceso que controla la RIB y la FIB en XORP se ha modificado para hacer uso de la librería IPROUTE2 [26] para crear una FIB multi-entrada. La utilización de CLICK para este fin también hubiera sido posible y queda como trabajo futuro.

Para ayudar a evaluar los resultados de las simulaciones / emulaciones se desarrolló una herramienta software llamada "*StatOpology*". Es una aplicación escrita en lenguaje Java, cuyo propósito inicial consistía en convertir diversos formatos de topologías de red al formato admitido por C-BGP. A esta aplicación se le han ido añadiendo funcionalidades, entre ellas se encuentra la de proporcionar información sobre el número de sistemas autónomos de la topología, mostrar los nodos hoja, los Tier-1, el número medio de enlaces y de qué tipo (*peering* o *provider to client*), generar una imagen (tanto vectorial como *raster*) de la topología e incluso cargar la

información correspondiente a las rutas instaladas en los distintos routers BGP tras las simulaciones / emulaciones con el fin de analizar en una tabla datos como son la longitud de los caminos, los nodos involucrados en los caminos, el número de bucles detectados, etc.

Los datos procesados por *StatOpology* pueden ser guardados en un fichero para ser evaluados posteriormente sin tener que analizar de nuevo los resultados de las simulaciones / emulaciones, o las topologías.

Las propuestas multi-path que se han validado son las mencionadas en la introducción (LP-BGP y MpASS) tanto en simulación como en emulación. La idea tras LP-BGP es aplicar una serie de reglas de filtrado sobre el conjunto de rutas que el router ha recibido de sus *peers*. El conjunto resultante de eliminar las rutas durante el filtrado es el set multi-path que el router puede utilizar para hacer el *forwarding* de paquetes. Se puede demostrar que de acuerdo a las *Loop-Free Invariants* introducidas en [5], si de ese conjunto se propaga a los *peers* la de mayor AS_PATH_LENGTH, se garantiza que el resto de rutas están libres de bucles.

En el caso de MpASS, la idea es aplicar la agregación de rutas que se hace entre prefijos más y menos restrictivos a múltiples rutas para un mismo prefijo. La idea es aplicar también un filtrado al set de posibles rutas candidatas para descartar rutas de baja calidad o problemáticas. Sobre las restantes, se aplica el mismo proceso de decisión que en BGP estándar para determinar la mejor de las rutas (en general la de menor AS_PATH_LENGTH). A continuación, la ruta ganadora, se le añade un AS_SET. El contenido de ese AS_SET son todos los AS_NUMBERS del resto de rutas candidatas (ya filtradas) que no formen parte del AS_PATH de la ganadora más el AS_NUMBER local del router. Esta ruta agregada es la que se propaga al resto de routers y el set de rutas candidatas pasa a la RIB del router local.

Para realizar la implementación de multi-path utilizando la propagación del camino más largo (LP-BGP), fue necesario añadir un proceso de decisión de reglas específico a los cambios anteriormente mencionados, además de una función encargada de determinar si se aplica o no en base al protocolo seleccionado en el router. Estos cambios se aplicaron en las secciones correspondientes a "*BGP-Graph & Config*" y "*BGP Router Model*" de la Figura 2.

Para realizar la implementación de multi-path basada en el uso de AS_SETs (MpASS), además de modificar las funciones del proceso de decisión de BGP también fue necesario hacer uso de las nuevas funciones encargadas de gestionar los AS_SETs. El resto de cambios es semejante a LP-BGP.

Los resultados obtenidos en simulación y emulación fueron equivalentes, lo que supone que el entorno provee resultados consistentes. Brevemente comentar, que sobre la topología de la Figura 4, la cual respeta las directrices de [22], el número de caminos entre ASes aumenta en media en torno a un 60% para ambas soluciones.

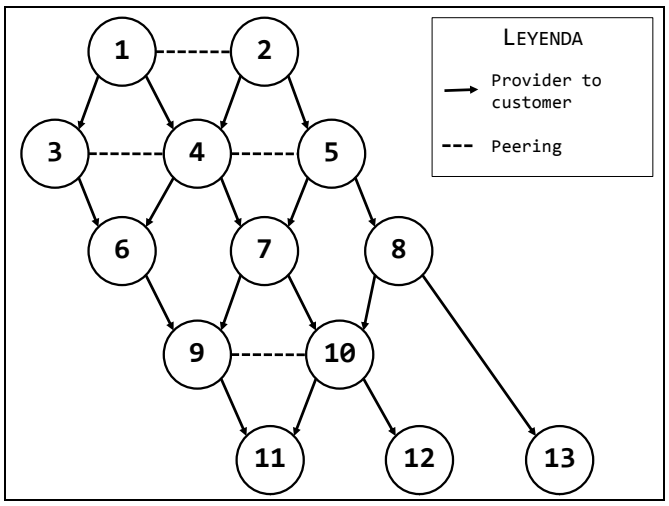


Figura 4. Topología de prueba

VI. CONCLUSIONES

El objetivo principal de la propuesta es poder comparar diferentes soluciones multi-path BGP de tal forma que sea posible no ya solo extraer automáticamente una serie de métricas para cada una objetivando así la comparación, sino que sea posible también combinarlas y evaluar su funcionamiento conjunto.

Para ello se ha combinado por un lado la sencillez de la simulación para valorar rápidamente aspectos como la convergencia así como la implementación real para evaluar la evolución en el tiempo del protocolo.

Todo esto se ha combinado además con herramientas de virtualización para posibilitar las pruebas en topologías con un elevado número de nodos.

Para validar la propuesta se han implementado tanto para el simulador como para el emulador dos soluciones concretas que se están desarrollando en el proyecto Trilogy, obteniendo unos resultados iniciales satisfactorios.

Como parte del trabajo que se sigue desarrollando en esta línea en este proyecto, está previsto una mayor exploración de las posibilidades de esta solución utilizando topologías de un mayor tamaño (las primeras pruebas realizadas con la arquitectura publicada en [23] son muy optimistas pero el proceso de simulación por ejemplo consume muchos recursos y se considera que puede optimizarse todavía más).

VII. AGRADECIMIENTOS

Este artículo ha sido parcialmente financiado por la Comisión Europa a través del proyecto Trilogy (ICT-216372), del VII Programa Marco y por la Cátedra Telefónica-UC3M en Internet del Futuro para la Productividad.

REFERENCIAS

[1] F. Valera, I. van Beijnum, A. García-Martínez, M. Bagnulo. "Next Generation Internet Architectures and Protocols", Ed., B. Ramamurthy, G. Rouskas, and K. Sivalingam, Cambridge University Press, 2010. ISBN: 978052111368

[2] Marcelo Bagnulo, Louise Burness, Philip Eardley, Alberto García-Martínez, Francisco Valera and Rolf Winter. "Joint Multi-path Routing

and Accountable Congestion Control". ICT-Mobile Summit 2009. June 2009, Santander, Spain
[3] Psenak P., Mirtorabi S., Roy A., Nguyen L., Pillay-Esnault P. "Multi-Topology (MT) Routing in OSPF".RFC4915.(2007).
[4] Albrightson B., Garcia-Luna-Aceves J., Boyle J. "EIGRP-A fastrouting protocol based on distance vectors". In Proc. Networld/Interop 94, Las Vegas. (1994). Proceedings. 136-147.
[5] S. Vutukury and J.J. Garcia-Luna-Aceves, "MPATH: A Loop-free Multi-path Routing Algorithm". Elsevier Journal of Microprocessors and Microsystems, 2000.
[6] Proyecto Trilogy (ICT-2007-216372). "Architecting the Future Internet". Disponible [Internet]: <http://trilogy-project.org/> [03 de julio de 2010]
[7] A. Ford, C. Raiciu, M. Handley. "TCP Extensions for Multi-path Operation with Multiple Addresses". IETF draft. Disponible [Internet] <http://tools.ietf.org/html/draft-ford-mptcp-multiaddressed-03> [03 de julio de 2010]
[8] Iljitsch van Beijnum, Jon Crowcroft, Francisco Valera and Marcelo Bagnulo. "Loop-freeness in multi-path BGP through propagating the longest path". International Workshop on the Network of the Future (Fut-Net 2009).June 2009, Dresden, Germany
[9] Página web oficial del simulador de red C-BGP. Disponible [Internet]: <http://cbgp.info.ucl.ac.be/index.php> [03 de julio de 2010]
[10] Página web oficial del módulo BGP++. Disponible [Internet]: <http://www.ece.gatech.edu/research/labs/MANIACS/BGP++/> [03 de julio de 2010]
[11] Página web oficial del simulador de red NS-2 . Disponible [Internet]: <http://www.isi.edu/nsnam/ns/> [03 de julio de 2010]
[12] Página web oficial del simulador de red GTNetS. Disponible [Internet]: <http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/> [03 de julio de 2010]
[13] Página web oficial del proyecto GNU Zebra. Disponible [Internet]: <http://www.zebra.org/> [03 de julio de 2010]
[14] Arquitectura del simulador C-BGP. Disponible [Internet]: <http://cbgp.info.ucl.ac.be/architecture.php> [03 de julio de 2010]
[15] W. Mühlbauer, A. Feldmann, O. Maennel, M. Roughan, S. Uhlig. "Building an AS-Topology Model that Captures Route Diversity". ACM SIGCOMM, 2006. Disponible [Internet]: <http://www2.net.in.tum.de/~muehlbaw/sigcomm06.pdf/> [03 de julio de 2010]
[16] Página web oficial del router software XORP. Disponible [Internet]: <http://www.xorp.org/> [03 de julio de 2010]
[17] XORP, Inc. "XORP Forwarding Engine Abstraction". XORP documentation. Jan. 2009. Disponible [Internet]: <http://www.xorp.org/releases/1.6/docs/fea/fea.pdf> [03 de julio de 2010]
[18] Página web oficial de Vyatta. Disponible [Internet]: <http://www.vyatta.com/> [03 de julio de 2010]
[19] The Click Modular Router Project. Disponible [Internet]: <http://read.cs.ucla.edu/click/> [03 de julio de 2010]
[20] Documentación online de OpenWRT, Disponible [Internet]: <http://kamikaze.openwrt.org/docs/openwrt.html> [03 de julio de 2010]
[21] Página web con características hardware de distintos routers existentes en el mercado (wiki de OpenWRT). Disponible [Internet]: <http://oldwiki.openwrt.org/Hardware%282f%29Linksys.html> [03 de julio de 2010]
[22] L. Gao, J. Rexford, "Stable Internet Routing Without Global Coordination", IEEE/ACM Transactions on networking, Vol.9, No.6, Dec. 2001
[23] Internet Topology Collection. Disponible [Internet]: <http://irl.cs.ucla.edu/topology/> [03 de julio de 2010]
[24] Citrix Xen Server. Disonible [Internet]: <http://www.citrix.com> [03 de julio de 2010]
[25] The Tolly Group. "Test report #209103. Citrix XenServer 5: Optimized Performance for XenApp compared to VMWare ESX 3.5u3".Abril 2009. Disonible [Internet]: <http://www.tolly.com/> [03 de julio de 2010]
[26] Linux Advanced Routing and Traffic Control. Disponible [Internet]: <http://lartc.org/> [03 de julio de 2010]

Caracterización Temporal de las Demandas de Ancho de Banda en Enlaces con Alta Agregación Mediante un Modelo Normal Multivariante

Felipe Mata, José Luis Garcia-Dorado, Javier Aracil
High Performance Computing and Networking Group
Universidad Autónoma de Madrid
Ciudad Universitaria de Cantoblanco
Calle Francisco Tomás y Valiente, 11
28049 - Madrid (España).
felipe.mata@uam.es, jl.garcia@uam.es, javier.aracil@uam.es

***Resumen*—Presentamos un modelo para caracterizar las demandas de tráfico en enlaces altamente agregados. El modelo está enfocado en capturar las variaciones que se producen a lo largo del día en dichas demandas de tráfico, comúnmente conocidas como patrón noche-día. Utilizamos la hipótesis de una distribución normal multivariante para nuestra caracterización, la cual validamos exhaustivamente con tests de normalidad univariantes y multivariantes sobre medidas de tráfico obtenidas de la red académica española RedIRIS. En concreto, los tests multivariantes nos permiten concluir que aunque la distribución de dichas demandas de tráfico no es rigurosamente normal multivariante, es bastante aproximada. Además, dicha aproximación es suficientemente buena para realizar inferencia, ya que las desviaciones de la multinormalidad de los datos no afectan severamente a la potencia de los tests multinormales para el vector de medias y la matriz de covarianzas.**

***Palabras Clave*—Distribución normal multivariante; Caracterización de tráfico; Patrón noche-día; Validación de modelado; Inferencia estadística.**

I. Introducción

La caracterización y modelado de Internet ha recibido mucha atención por la comunidad científica debido a su gran utilidad desde un punto de vista tanto comercial como científico [1]. En la literatura se pueden encontrar artículos que modelan distintas caracteristícas de Internet, algunas de las cuales son los dominios web [2], la carga se servidores [3], la popularidad de los puertos y direcciones IP [4], aplicaciones P2P [5], o juegos en red [6], por citar algunos ejemplos.

Por un lado, los operadores de Internet han aprovechado la posibilidad de modelar y caracterizar detalladamente su tráfico, beneficiándose de esta información en su objetivo final de proveer la calidad de servicio adecuada a sus clientes. De hecho, las demandas de los usuarios, así como la variedad de los requisitos de calidad de servicio, crecen de forma continua. Esto está forzando a los ISP a mejorar la caracterización y modelado de su tráfico con los fines de evaluar las prestaciones de las redes de comunicación, desarrollar tareas de asignación de capacidad o establecer políticas de control de congestión, entre otras aplicaciones.

Por otro lado, la comunidad científica ha considerado que para caracterizar el comportamiento y estudiar las dinámicas de Internet, los cuales son por naturaleza heterogéneos y cambientes, es imprescindible la identificación y definición de invariantes [7], [8]. En Internet, un invariante se define como una característica que existe en un amplio conjunto de redes durante un tiempo suficientemente representativo. En este sentido, hemos analizado todos los enlaces troncales de la red académica española RedIRIS [9], durante más de un año, desde febrero de 2007 a mayo de 2008, en busca de invariantes.

En este artículo, caracterizamos la carga de estos enlaces durante el periodo de medida. En concreto, hemos encontrado que este fenómomeno se puede modelar aproximadamente mediante distribuciones Gaussianas multivariantes, cuyos parámetros van cambiando con el tiempo (es decir, son no estacionarias). Existen trabajos previos que han modelado la demanda de ancho de banda de una red con modelos Gaussianos aproximados (cf. [10], [11], [12], [13]). Sin embargo estos estudios se han centrado en escalas de tiempo muy pequeñas, esto es, inferiores a las decenas de segundos. Estas escalas son de utilidad para ciertas tareas, como presentan los autores en dichos artículos, pero no para la planificación de capacidad de las redes de datos [14], que típicamente motiva estudios con un mayor horizonte temporal, como es el caso de este artículo que analiza datos durante un año.

En particular, proponemos un modelo que se ajusta a las variaciones inherentes del tráfico a lo largo del día, las cuales están directamente relacionadas con las variaciones en el número de usuarios consumiendo recursos de red. Asumimos para dicho modelo una distribución normal multivariante, basándonos en estudios previos de la normalidad del tráfico en enlaces altamente agregados [12], [11]. No obstante, comprobamos la validez del modelo utilizando nuestro conjunto de datos obtenidos de RedIRIS. El modelo propuesto es por tanto útil para la modelización de las variaciones temporales de las demanda de ancho de banda en enlaces de alta agregación, pudiéndose aplicar técnicas de inferencia estadística para detectar cambios en la distribución del tráfico [15] que estarían directamente relacionados con cambios en el uso de la red (por ejemplo aumento del número de usuarios o variaciones en sus patrones de uso de los recursos). Un análisis posterior de estos cambios detectados podría justificar decisiones relacionadas con la planificación de la red, como pueden ser la variación de las tablas de enrutado para hacer balanceo de carga o el aumento de la capacidad de aquellos enlaces donde la carga

tras el cambio supere un cierto umbral de utilización.

El resto del artículo está estructurado de la siguiente forma. En la Sección II describimos la red troncal de RedIRIS, de donde se han obtenido las medidas para este estudio. Seguidamente, describimos el patrón diario del tráfico agregado de los enlaces bajo estudio en la Sección III, que será la base para nuestro modelo normal multivariante, descrito y validado en la Sección IV. Finalmente, la Sección V resume y concluye el artículo.

II. Escenario de Medida

El escenario de medida utilizado en este artículo es el conjunto de enlaces troncales de la red académica española RedIRIS [9]. Esta red troncal está formada por varios Puntos de Presencia (PoP) localizados en las distintas comunidades autónomas del territorio español, utilizando una topología de interconexión semi-mallada, como se muestra en la Fig. 1. En dicha figura, además se esboza la estructura del sistema recolector de medidas, situado en las dependencias de la Universidad Autónoma de Madrid (UAM). Este sistema recibe y almacena reportes de la carga media y máxima de cada interfaz de cada router, obtenidos mediante consultas periódicas a la Base de Información Gestionada (MIB) utilizando el Protocolo Simple de Administración de Red (SNMP) con una granularidad de cinco minutos, configuración habitual de la herramienta Multi-Router Traffic Grapher (MRTG) [16].

De acuerdo con la Fig. 1, el sistema recolector de medidas está dividido en tres etapas. En una primera etapa, se almacenan las medidas tal y cómo se reciben de la red. Posteriormente, estas medidas son procesadas de manera conveniente, para que finalmente sean útiles para realizar tareas de gestión y supervisión de red asi como facilmente visualizadas. Con la granularidad de los reportes de MRTG, tenemos 288 medidas para cada sentido de cada enlace de cada router al día, durante un periodo mayor que un año, desde el 2 de Febrero de 2007 hasta el 31 de Mayo de 2008. Esto supone, para una red con unos 30 enlaces (troncales), como es el caso de RedIRIS, tener que supervisar unas 60 series temporales distintas al día en busca de patrones anómalos o cambios sostenidos en los valores de la carga, con el fin de realizar tareas de ingeniería de tráfico, tales como actualización de rutas o ampliación de capacidades de enlace, para mantener unas condiciones de funcionamiento estables que garanticen altas calidades de servicio. Obviamente, el hecho de tener que inspeccionar tan alto número de series temporales diariamente es una tarea tediosa y costosa para las operadoras. Es por esto que un modelo apropiado para las medidas del tráfico de red para enlaces altamente agregados, como lo son los enlaces troncales de la red RedIRIS, es de amplia utilidad para los gestores de red, permitiéndoles el desarrollo de algoritmos que detecten cambios de manera semi-automática, con el consecuente ahorro en gastos de operación (OPEX).

III. Patrones Diarios y Efecto Noche-Día

En esta sección analizamos las series temporales de las medidas de consumo medio de ancho de banda, MRTG, provenientes del sistema de monitorización previamente presentado, con el objetivo de entender mejor los patrones diarios y semanales del tráfico en RedIRIS, intentando encontrar algún patrón invariante. Sin embargo, para hacer comparables las medidas provenientes de diferentes enlaces, convertimos la carga media de cada enlace (nuestras medidas según se obtienen de MRTG) en valores de utilización de enlace, simplemente dividiendo cada medida obtenida de la herramienta MRTG por la capacidad total del enlace al que corresponde, obteniéndose así el porcentaje de ocupación de los enlaces, que varía entre 0 y 100 para todos ellos.

Las gráficas de las series temporales de la carga media evidencian la existencia de dos tipos de patrón diario del tráfico, uno para los días laborables y otro para los fines de semana y días festivos (véase la Fig. 2, donde se muestran las series temporales del tráfico para el sentido saliente y entrante de una semana que es representativa del fenómeno descrito). En dicha figura se observa como el tráfico durante los días laborables presenta variaciones a lo largo del día, que son similares entre los distintos días laborables. Así, partiendo de un patrón nocturno prácticamente plano, se observa un crecimiento en torno a las 08:00 de la mañana (cuando los empleados y alumnos llegan a los centros) que se estabiliza alrededor de las 10:00, manteniéndose así hasta la caída del tráfico a la hora de comer (en torno a las 14:00-15:00 horas), tras la que vuelve a haber una pequeña subida que finalmente va decreciendo a partir de las 18:00 horas (personal abandonando sus puestos de trabajo) hasta quedarse totalmente plano de nuevo al alcanzarse la noche. Sin embargo, este fenómeno oscilante no se observa para los fines de semana, donde el patrón es prácticamente plano durante todo el día, siendo su valor de utilización prácticamente el mismo que durante la noche en los días laborables. Este hecho lleva a pensar que el tráfico nocturno y de los fines de semana y festivos es debido a aplicaciones que están ejecutándose sin supervisión de un usuario, como por ejemplo aplicaciones P2P, backup, actualizaciones, Skype cuando se convierte en un supernodo [17], etc., y al tráfico relacionado con los servidores de correo y web de la institución. Se observa además que los valores de utilización del enlace en cuestión (y de los demás enlaces analizados) están típicamente por debajo del 20% (aunque son enlaces altamente agregados, con capacidades entre 2.5 y 10 Gbps). Por lo tanto, los enlaces no están nunca congestionados, lo que significa que las medidas obtenidas son independientes, es decir, no hay una restricción (la capacidad máxima del enlace) que las relacione. Pudiera ser que existiera una limitación en las redes de acceso a dichos enlaces, pero en otro estudio se ha comprobado que los enlaces de acceso de las universidades tampoco sufren de congestión en ningún momento.

Estas diferencias entre los patrones diarios de los días laborables y los festivos están directamente relacionadas con la variación del número de usuarios a lo largo del día. El patrón diario del tráfico aumenta cuando aumenta el número de IPs activas (donde consideramos una IP como activa si genera tráfico ascendente a granularidad de 1 minuto, para lo que hemos usado registros NetFlow, e identificamos a cada usuario con una dirección IP diferente), como evidencia la Fig. 3 para un día laborable. Esto quiere decir que las variaciones a lo largo del día de la carga (o utilización) no se debe a un cambio en el comportamiento de los usuarios a lo largo del día, sino que se debe a un aumento (o descenso) del número de usuarios consumiendo los recursos de red.

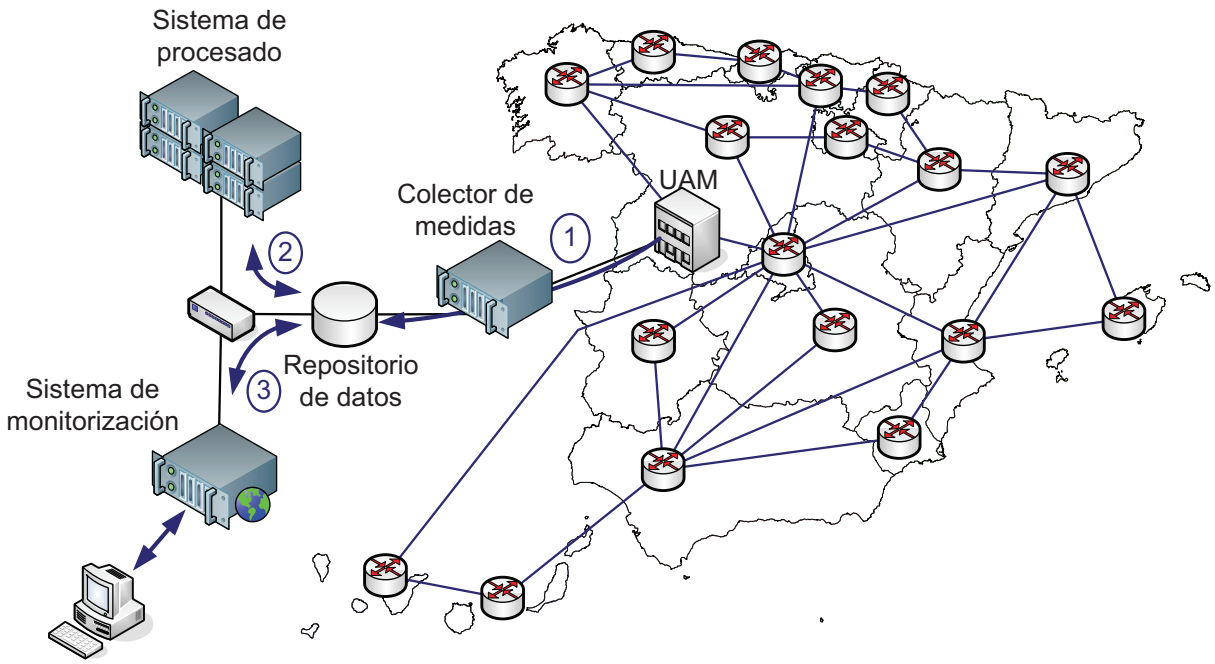


Fig. 1. Arquitectura de la red troncal de RedIRIS y esquema del sistema de captura de medidas situado en la Universidad Autónoma de Madrid.

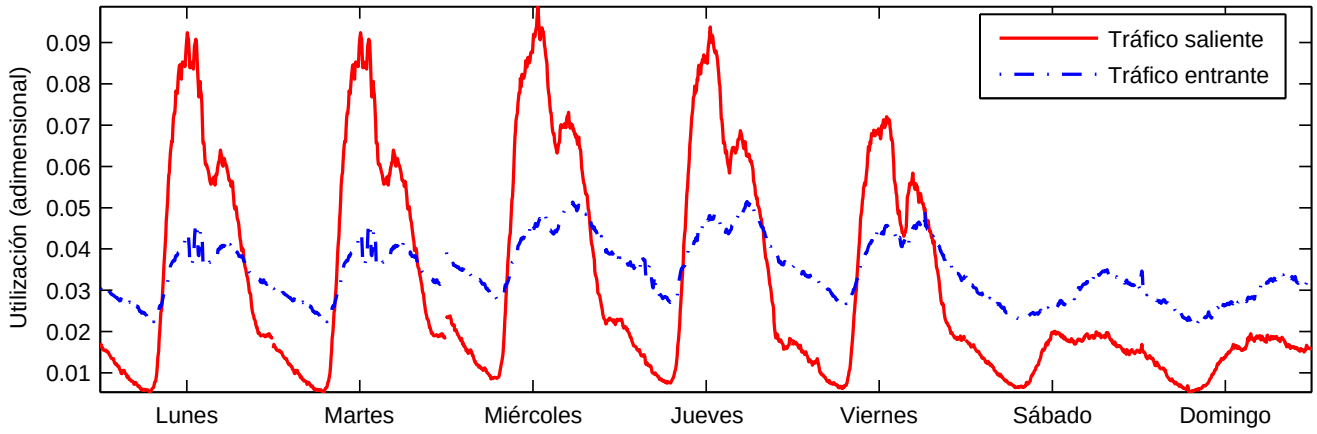


Fig. 2. Patrón diario para diferentes días de la semana para el sentido saliente y entrande del tráfico. Los días festivos muestran un patrón plano comparados con los días laborables que muestran un patrón oscilante con la hora del día. Las medidas se refieren a la semana del 10 al 16 de marzo de 2008.

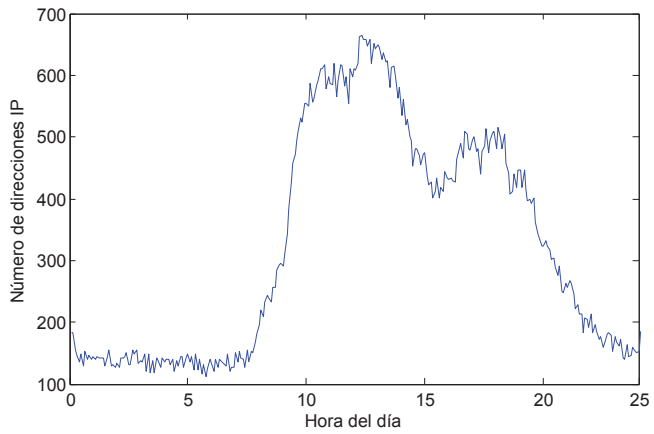


Fig. 3. Número de direcciones IPs activas a lo largo del día 12 de marzo de 2008 para una universidad de RedIRIS.

Esta variación del número de usuarios también explica que el patrón de tráfico sea diferente para los fines de semana y días festivos, ya que en estas fechas el número de usuarios (direcciones IP activas) es considerablemente menor, como se muestra en la Fig. 4. En esta figura, el número de usuarios activos en el horario de oficina (en concreto hemos establecido el rango de 10:00 a 18:00 horas) se muestra para los diferentes días de una semana en todo RedIRIS (la semana en cuestión es la misma que la de la Fig. 2). El resultado muestra como la atividad durante el fin de semana es mínima comparada con los días laborables, y refuerza la hipótesis de que el tráfico durante los fines de semana está relacionado con aplicaciones no interactivas como ya hemos comentado.

Consecuentemente, las grandes diferencias existentes entre los días laborables y festivos hacen inviable el desarrollo de un único modelo que caracterice de forma precisa ambos patrones. Además, desde el punto de vista de un operador, tiene

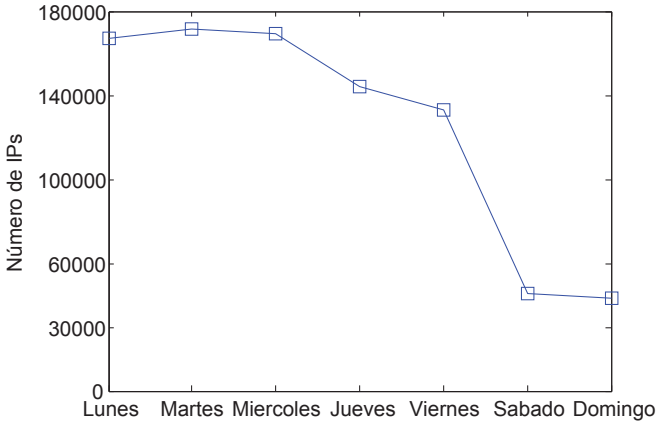


Fig. 4. Número de IPs activas durante las horas de oficina para RedIRIS.

mayor interés modelar los días laborables, pues representan un mayor volumen de tráfico. Estos hechos nos mueven a desarrollar un modelo que caracterice de forma precisa la carga o patrón diario para los días laborables, eliminando los días festivos (o con tráfico anómalo) de la muestra. De este modo, los días ignorados para el modelo son de cuatro tipos: fines de semana; verano, navidades y semana santa; fiestas nacionales y regionales; y finalmente los periodos de exámenes. Consideramos el verano desde el 1 de julio hasta el 31 de agosto, las vacaciones de Navidad desde el 22 de diciembre al 7 de enero, el periodo ordinario de exámenes del 15 al 30 de junio mientras que el periodo extraordinario de exámenes del 1 al 15 de septiembre. Finalmente, las distintas fiestas regionales y nacionales, así como la semana santa, son eliminadas año a año, ya que puede ser que no coincidan en fechas de un año para otro.

IV. Modelo Multivariante Aproximadamente Normal Para el Patrón Diario del Tráfico

A. Descripción del Modelo

A consecuencia de lo presentado en la sección anterior, proponemos un modelo para el tráfico diario que capture el patrón noche-día, centrándose en los días laborables porque son de mayor interés para ingeniería de tráfico, ya que son los días donde la demanda de recursos es mayor. Para ello, utilizamos medidas de carga media obtenidas cada cinco minutos con la herramienta MRTG (288 medidas al día para cada sentido de cada enlace). El modelo asume que las medidas del mismo intervalo de tiempo durante diferentes días provienen de la misma (en este punto desconocida) distribución de probabilidad. Basamos esta hipótesis en el hecho de que la forma de las series temporales es similar día tras día, y que las diferenicas entre las medidas en el mismo intervalo temporal de diferentes días no son significativas (es decir, nos basamos en la invarianza del patrón noche-día del tráfico). Sin embargo, esta distribución de probabilidad no tiene porqué tener los mismos parametros en los distintos intervalos en los que está dividido el día. De este modo, una distribución multivariante para modelar la carga diaria a diferentes momentos del día es necesaria, pudiéndose así caracterizar el tráfico durante cada subdivisón temporal a lo largo del día con parámatros distintos. Sin embargo, una distribución con tan alta dimensionalidad es poco práctica [18]. Para hacerla más manejable, dividimos el día en intervalos disjuntos del mismo tamaño, tomando sobre cada intervalo la media de las medidas de MRTG que caen en dicho intervalo como su representante. Para la elección de la longitud de los intervalos, hay que tener un compromiso entre intervalos pequeños que nos ofrecen la ventaja de capturar de manera más precisa las variaciones del tráfico, a costa de tener un mayor número de dimensiones en nuestro modelo (con los problemas que ello conlleva [18]) e intervalos grandes que nos reducen la dimensionalidad del modelo haciéndolo más manejable a costa de perder precisión al modelar los datos. Teniendo en cuenta estas y otras restricciones, hemos seleccionado una duración de los intervalos de 90 minutos. Existen varias razones para escoger este periodo de agregación: primera, el periodo de agregación debe ser múltiplo de la granularidad de medida (5 minutos) y divisor del número de minutos del día (1440 minutos). Segunda, dado que es posible que algunas de las medidas de MRTG no sean correctas (o haya *missing values*), promediar los valores en intervalos de 90 minutos reduce el impacto que pueden tener estos valores incorrectos o *missing values* (por ejemplo, si falta alguna medida del intervalo, se promedia un número menor de valores, pero la media sigue siendo representativa). Sin embargo, merece la pena remarcar que si todas las muestras de un mismo intervalo son inválidas, se descarta el día completo, evitando cualquier contaminación por esta causa. Tercera, los diferentes puntos de medida pueden no estar perfectamente sincronizados (de hecho, es lo más normal). Promediar los valores en intervalos de 90 minutos reduce considerablemente el efecto indeseado de dicha desincronización. De hecho, una escala de 90 minutos se muestra suficiente para evitar este problema como se mostró en [19]. Esto nos permite que el modelo sea aplicable para hacer correlaciones de los datos entre diferentes enlaces. Cuarta, el promedio de las medidas reduce el sesgo introducido en los resultados por valores extremos y medidas incorrectas que pueden existir en el conjunto de datos. Esto permite centrárnos en nuestro objetivo, que es aplicar nuestro modelo al análisis de medidas de red en escalas de tiempo largas, reduciendo la influencia que sobre los resultados puedan tener valores con alta variabilidad a escalas pequeña. Por último, la premisa de que el tráfico es aproximadamente Gaussiano es válida cuando la agregación temporal es significativa [12], [11]. Consecuentemente, además de simplificar el modelo, obtenemos una distribución razonable del promedio de las medidas. Sin embargo, hacemos notar que posteriormente mostraremos evidencias empíricas de que esta premisa es válida.

Después del preprocesado de los datos, tenemos más de 300 muestras por enlace y dirección, cada una de ellas representando un día de medidas que modelamos con una distribución normal con 16 dimensiones. Es importante remarcar que este preprocesado puede ser realizado durante la captura de datos puesto que los días sin interés pueden ser determinados por adelantado. Finalmente, la Tabla I muestra las componentes del modelo y los intervalos temporales a los que se corresponden. Esta información ha sido también incorporada en la Fig. 5, donde están superimpuestas sobre el patrón noche-día medio en las redes analizadas (línea

continua) las divisiones utilizadas en nuestro modelo para cada intervalo (líneas discontinuas verticales).

Tabla I
EQUIVALENCIA EN TIEMPO DE LAS VARIABLES.

Número de variable	Intervalo de Tiempo	Número de variable	Intervalo de tiempo
1	00:00-01:30	9	12:00-13:30
2	01:30-03:00	10	13:30-15:00
3	03:00-04:30	11	15:00-16:30
4	04:30-06:00	12	16:30-18:00
5	06:00-07:30	13	18:00-19:30
6	07:30-09:00	14	19:30-21:00
7	09:00-10:30	15	21:00-22:30
8	10:30-12:00	16	22:30-00:00

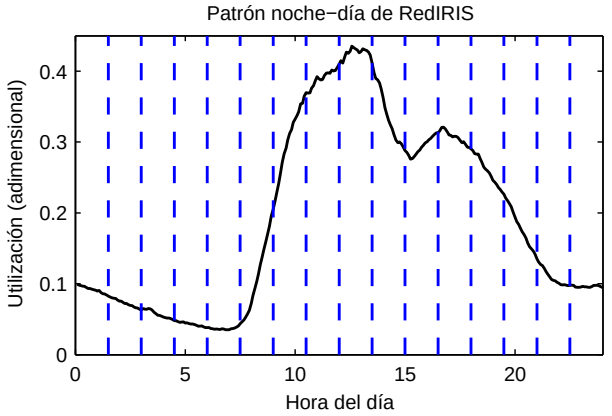


Fig. 5. Patrón diario medio de las redes analizadas y divisiones utilizadas por el modelo multivariante.

B. Metodología

Para validar la aplicabilidad del modelo para realizar inferencias sobre las medidas del tráfico de una red, hemos realizado varias verificaciones de la hipótesis de normalidad del tráfico una vez procesado acorde al modelo propuesto. Hemos adpotado la metodología usada en [11] para verificar la normalidad de las distribuciones marginales de nuestro modelo multivariante. Además, hemos comprobado la normalidad multivariante. Esto es necesario porque el hecho de que las marginales de la distribución sigan distribuciones normales univariantes no implica que la distribución conjunta sea normal multivariante [20]. En lo que sigue, describimos brevemente los tests de normalidad aplicados tanto a las distribuciones marginales univariantes como a la distribución conjunta multivariante.

Los autores de [11] mostraron que el coefciente de correlación lineal γ entre el estadístico ordenado de la muestra y los correspondientes cuantiles normales del modelo de la distribución (esto es, un distribución normal con parametros estimados de la muestra) es, esencialmente, equivalente al test Kolmogorov-Smirnov (KS) para comprobar normalidad univariante. Es decir, observaron que existe una alta correlación entre valores altos de γ, típicamente mayores que 0,9, y el hecho de que la hipótesis nula que establece normalidad no pueda ser rechazada por el test KS a un nivel de significación $\alpha = 0,05$. Por tanto, en lugar de aplicar el test KS a nuestras muestras, calculamos el coeficiente γ, considerando que la población es aproximadamente normal si $\gamma \geq 0,9$. Para calcular γ, sea $x_1, x_2, \ldots, x_n$ una muestra univariante de tamaño n. Sean además $\bar{x}$ and s^2 los estimadores insesgados para la media y varianza muestral, respectivamente, esto es, $\bar{x} = n^{-1}\sum_{i=1}^{n} x_i$ y $s^2 = (n-1)^{-1}\sum_{i=1}^{n}(x_i - \bar{x})^2$. Definimos $x_{(i)}, i = 1, 2, \ldots, n$, como el estadístico ordenado de la muestra, esto es, $x_{(1)} < x_{(2)} < \ldots < x_{(n)}$, y q_i sus correspondientes cuantiles dados por $q_i = \Phi^{-1}(\frac{i}{n+1})$, donde Φ^{-1} es la función cuantílica de la distribución normal acumulada con media $\bar{x}$ y varianza s^2. Sea $\bar{q}$ la media de los cuantiles, entonces el coeficiente de correlación lineal γ está dado por:

$$\gamma = \frac{\sum_{i=1}^{n}(x_{(i)} - \bar{x})(q_i - \bar{q})}{\sqrt{\sum_{i=1}^{n}(x_{(i)} - \bar{x})^2 \sum_{i=1}^{n}(q_i - \bar{q})^2}}. \quad (1)$$

Respecto a la multinormalidad, hemos elegido los tests para desviaciones en la asimetría y la curtosis asumiendo normalidad multivariante publicados por Mardia [21], $b_{1,p}$ y $b_{2,p}$ respectivamente. Las principales razones para elegir estos estadísticos son su invarianza afín y que Mardia demostró que las potencias de los tests de normalidad para el vector de medias y la matriz de covarianzas están negativamente afectadas por la asimetría [22] y la curtosis [23], respectivamente. De este modo, usando estos tests evaluamos la bondad del ajuste del modelo a los datos y además, podemos tener una idea de su validez para realizar inferencia sobre el vector de medias y la matriz de covarianzas.

Sea $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_n$ una muestra p-dimensional de tamaño n, entonces los coeficientes de asimietría y curtosis están dados por:

$$b_{1,p} = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} r_{ij}^3 \quad \text{y} \quad b_{2,p} = \frac{1}{n}\sum_{i=1}^{n} r_i^4, \quad (2)$$

donde $n > p$ y

$$r_{ij} = (\mathbf{y}_i - \bar{\mathbf{y}})'\mathbf{S}_n^{-1}(\mathbf{y}_j - \bar{\mathbf{y}}), \;\; r_i^2 = (\mathbf{y}_i - \bar{\mathbf{y}})'\mathbf{S}_n^{-1}(\mathbf{y}_i - \bar{\mathbf{y}}), \quad (3)$$

$$\bar{\mathbf{y}} = \frac{1}{n}\sum_{i=1}^{n}\mathbf{y}_i, \qquad \mathbf{S}_n = \frac{1}{n}\sum_{i=1}^{n}(\mathbf{y}_i - \bar{\mathbf{y}})(\mathbf{y}_i - \bar{\mathbf{y}})'. \quad (4)$$

Para poder aplicar la tablas estadísticas ya tabuladas, la siguiente estandarización es usada en la práctica [21]:

$$sb_{1,p} = \frac{nb_{1,p}}{6} \xrightarrow{d} \chi^2_{df}, \quad (5)$$

$$sb_{2,p} = \frac{b_{2,p} - p(p+2)(n-1)/(n+1)}{\sqrt{8p(p+2)/n}} \xrightarrow{d} \mathcal{N}(0,1), \quad (6)$$

donde $df = p(p+1)(p+2)/6$ son los grados de libertad de la distribución χ^2 y $\xrightarrow{d}$ significa convergencia en distribución ($n \to \infty$). De este modo, valores grandes de $b_{1,p}$ y $|b_{2,p}|$ permiten rechazar la normalidad multivariante.

C. Resultados de la Validación

Para aplicar los métodos presentados en la sección anterior, hemos procesado los datos descritos en la sección II de acuerdo con nuestro modelo normal multivariante.

A continuación, calulamos el coeficiente de correlación lineal γ para todas las muestras existentes para cada dirección en cada enlace. Los resultados fueron pobres, y la hipótesis de normalidad univariante era rechazada para todas las distribuciones marginales. Sin embargo, esto no quiere decir que el modelo sea inapropiado, sino que los parámetros pueden estar cambiando con el tiempo, es decir, la muestra es no estacionaria. De todos modos, es posible asumir que el tráfico es estacionario en ventanas temporales inferiores, es decir, los parámetros de la distribución subyacente permanecen inalterados durante periodos de tiempo, que si bien no abarcan la muestra total, si duran varias semanas (20-30 dias). Esto nos motiva a comprobar la hipótesis de normalidad en subconjuntos de muestras. Por esta razón dividimos la muestra en subpoblaciones de $n = 20$ realizaciones, lo cual es equivalente a un perido de 25-28 dias naturales (ya que fueron filtrados varios días, como festivos, fines de semana, etc.). Consecuentemente, calculamos el coeficente γ para cada distribución marginal de cada una de las subpoblaciones. Los resultados se muestran en la Fig. 6, donde mostramos el porcentaje de subpoblaciones, ordenadas por el valor de bondad de ajuste γ, que presentan un coeficiente inferior a γ_0 para cada posible valor de γ_0.

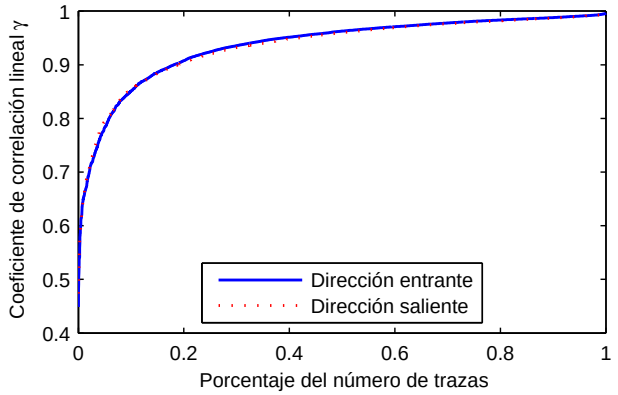


Fig. 6. Resultados de los test de normalidad univariante.

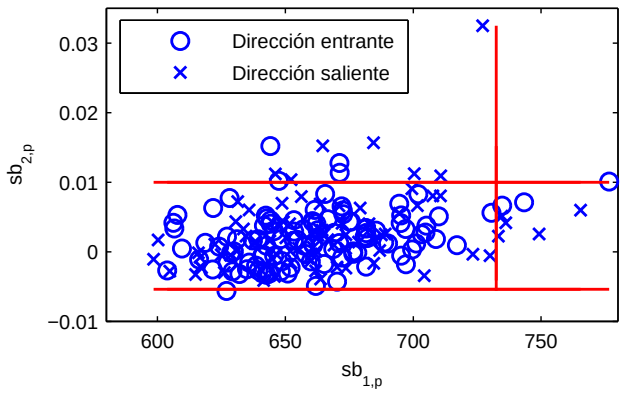


Fig. 7. Resultados de los test de normalidad multivariante.

Respecto a la normalidad multivariante, es bien conocido que si una o más de las variables muestra un comportamiento no Gaussiano, la multinormalidad puede ser rechazada [20, p. 133]. Por tanto, no verificamos la multinormalidad para el conjunto completo ni tampoco para las subpoblaciones descritas anteriormente en las cuales alguna de las distribuciones marginales mostraron no normalidad (en estos casos, los tests para normalidad multivariante deberían rechazar la hipótesis de normalidad). Para aplicar apropiadamente los correspondientes valores estandarizados de los estadísticos para comprobar la asimetría y curtosis multivariante, no podemos usar las correspondientes distribuciones límite, porque las muestras (subpoblaciones) a las que aplicamos los tests son demasiado pequeñas. Por tanto, estimamos los valores críticos de las formas estandarizadas de los estadísticos mediante simulación. Para ello, realizamos $N = 100.000$ simulaciones tipo Monte Carlo en N muestras independientemente generadas, $\mathbf{Z}_i \sim \mathcal{N}_p(\mathbf{0}, \mathbf{I}_p)$; $i \in 1, \ldots, N$, de tamaño $n = 20$, donde $\mathbf{0}$ es un vector de 16 componentes todas iguales a 0, y $\mathbf{I}_p$ es la matriz identidad de rango $p = 16$. Los valores críticos obtenidos están resumidos en la Tabla II para tres niveles distintos de significación α.

Tabla II
VALORES CRÍTICOS PARA LOS TESTS ESTADÍSTICOS PARA LA ASIMETRÍA Y CURTOSIS MULTIVARIANTE

Nivel de Significación (α)	$cv_{sb_{1,p}}$	$cv_{sb_{2,p}}$	
		inferior	superior
0,1	695,7828	$-0,004$	0,0054
0,05	708,6464	$-0,0046$	0,0069
0,01	732,4614	$-0,0054$	0,01

En esta tabla, $cv_{sb_{1,p}}$ se refiere a los valores críticos para los valores estandarizados de $b_{1,p}$. Los valores de $sb_{1,p}$ mayores que $cv_{sb_{1,p}}$ indican asimetría. Al contrario, $cv_{sb_{2,p}}$ son los valores críticos para comprabar la curtosis. Nótese que dicho test es bilateral, por lo cual se tienen dos valores críticos, uno inferior y otro superior, en ambos lados de la cola de la distribución. Valores de $sb_{2,p}$ menores que $cv_{sb_{2,p}}$ inferior, o mayores que $cv_{sb_{2,p}}$ superior indican curtosis en la muestra.

La Fig. 7 muestra los resultados de los tests estadísticos cuando son aplicados a los datos en estudio. Mostramos en el eje x los valores de $sb_{1,p}$ mientras que en el eje y podemos encontrar los valores de $sb_{2,p}$. Cada subpoblación está representada con un $\circ$ si esta pertence a medidas de tráfico descendente o por un simbolo $\times$ si es tráfico de la dirección ascendente. Hemos representado con líneas rectas los umbrales dados por los valores críticos a nivel de significación $\alpha = 0,01$. El porcentaje de los tests cuyo estadístico caen en la región de rechazo están resumidos en la Tabla III, donde mostramos esos valores para el test de asimetría, de curtosis y para aquellos que en los que se rechaza uno de los dos.

D. Discusión de los Resultados

Los valores de los tests de normalidad univariante mostrados en la Fig. 6 evidencian que los resultados en ambos sentidos, ascendente y descendente, están muy próximos, ya que sus correspondientes gráficas están parcialmente superpuestas. En cualquiera de ellas, puede comprobarse que en más del 80% de los casos estudiados, la medida de bondad

Tabla III
PORCENTAJE DE RECHAZO DE NORMALIDAD MULTIVARIANTE PARA LOS TESTS DE ASIMETRÍA Y CURTOSIS.

Dirección	Tasa de Rechazos		
	Test asimetría	Test curtosis	Bien asimetría o curtosis
Entrante	2,80%	4,60%	6,54%
Saliente	5,88%	8,24%	14,12%
Ambas	4,17%	6,25%	9,90%

de ajuste γ se situa por encima del umbral 0,9 recomendado por los autores de [11]. Estos resultados son similares a los mostrados en dicho artículo, por lo que obtenemos de este modo conclusiones equivalentes, esto es, el valor promedio de ancho de banda consumido en cada uno de los intervalos disjuntos seleccionados en nuestro modelo multivariante se puede considerar aproximadamente Gaussiano.

Con respecto a la normalidad multivariante, los resultados de la Tabla III muestran que la multinormalidad puede ser rechazado en el 10% de los casos. Aunque no podemos generalizar la validez rigurosa del modelo normal multivariante, los resultados muestran evidencia suficiente para aceptar que un modelo multinormal se aproxima a los datos reales. Además, estos resultados nos permiten ver que el modelo es útil para aplicar inferencia multinormal sobre el vector de medias, porque el porcentaje de rechazo para los tests de asimetria (4,17%) es significativamente bajo y por tanto, la potencia de los tests de multinormalidad para el vector de medias [22] no se verá severamente afectada. La misma conclusión puede extraerse al observarse los porcentajes de rechazo de los tests de curtosis (6,25%), los cuales por su parte evidencian que la potencia de los tests de multinormalidad para matrices de covarianzas [23] tampoco se verá significativamente afectada de manera adversa.

De todos modos, hacemos notar que la hipótesis de normalidad no puede ser rechazada en la mayoría de las subpoblaciones en el caso univariante, que junto evidencias que indican que la premisa de multinormalidad es también correcta, nos permiten concluir que un modelo multivariante aproximademante Gaussinao puede ser aceptado para caracterizar el tráfico procesado según la Sección IV-A, y posteriormente utilizado para hacer inferencia estadística asumiendo la distribución multinormal.

Esta validez del modelo para hacer tests multinormales nos permite utilizar el modelo para hacer inferencia sobre aspectos del tráfico relacionados con tareas de ingeniería de tráfico. En concreto, el modelo presentado y validado en este artículo ha sido utilizado en un algoritmo de detección de cambios en la demanda del tráfico de manera automática [15]. El algoritmo toma como partida el modelo, y busca el punto entre dos regiones donde la media del tráfico (es decir, el vector de medias del modelo) ha cambiado, utilizando para ello la versión multivariante del problema de Behrens-Fisher [24], que es el problema de contraste de hipótesis sobre la media de poblaciones normales, cuando no se hace ninguna asunción sobre las matrices de covarianzas. Este algoritmo está por tanto enfocado a detectar cambios (para lo que utiliza el test multinormal sobre el vector de medias) sostenidos (ya que el modelo está enfocado a largas escalas) en enlaces altamente agregados, como los de la red troncal de RedIRIS, presentando la ventaja de ahorrar en gastos de operación (OPEX), puesto que con su ayuda no es necesario supervisar todos los enlaces de la red diariamente, si no solamente aquellos enlaces en los que se ha detectado un cambio, y solamente cuando el cambio ha sido detectado (es decir, si no se reporta ninguna detección, los enlaces se suponen estables). Sobre estas detecciones, el gestor de red tomará las consideraciones necesarias para decidir si es necesario actualizar algunas rutas de tráfico o aumentar la capacidad de los enlaces en cuestión, o si el cambio no ha sido lo suficientemente grande como para tener que tomar acción alguna.

V. CONCLUSIONES Y RESUMEN

En este artículo hemos utilizado una distribución normal multivariante para modelar la demanda de tráfico de enlaces con alto nivel de agregación (tales como enlaces troncales). La forma multivariante de la distribución se debe a la necesidad de adaptarse a las variaciones inherentes del tráfico a lo largo del día en dicho tipo de enlaces, conocido como patrón diario o patrón noche-día. Estas variaciones diarias del tráfico responden principalmente a la variación del número de usuarios consumiendo recursos de la red a lo largo del día, como evidencia la comparación de la Fig. 2 con la Fig. 3. Cabe remarcar que este patrón es diferente en RedIRIS a los existentes en redes residenciales, donde el pico principal se produce cuando los usuarios vuelven a casa de trabajar [25], mientras que en RedIRIS el pico más alto se produce a media mañana, cuando el número de trabajadores es máximo.

Aunque el modelo multivariante aparece de forma natural al tratar de adaptarse a la variación diaria de la demanda de tráfico, la distribución multivariante resulta una incógnita a priori. Basándonos en estudios previos de enlaces de tráfico agregado [12], [11], utilizamos la hipótesis de una distribución normal para cada una de las componentes del vector multidimensional. A priori, esto ya había sido demostrado por dichos estudios, pero aún así, comprobamos que también se cumplía en el conjunto de datos utilizados para nuestro estudio: medidas de la demanda tráfico entrante y saliente para cada enlace de la red troncal de RedIRIS, la red académica española.

Realizamos verificaciones de la normalidad univariante y multivariante de nuestros datos, con el fin de determinar la validez del modelo propuesto. Para la verificación de la multinormalidad, los tests para asimetría [22] y curtosis [23] de Mardia han sido seleccionados, ya que el propio autor demostró que desviaciones en estas medidas reducen significativamente la potencia de las técnicas estadísticas asumiendo la distribución. Por lo tanto, la validación positiva de que estas desviaciones no son significativas nos permiten demostrar que, aunque el modelo propuesto no sea rigurosamente normal multivariante, lo es de forma aproximada, y concluir que dicha aproximación es suficientemente buena a la hora de hacer inferencia estadística.

AGRADECIMIENTOS

Los autores quieren agradecer el soporte del Ministerio de Ciencia e Innovación (MICINN) a este estudio bajo el proyecto *ANFORA* (TEC2009-13385) y los programas de becas FPU y FPI que han financiado parcialmente este trabajo, así como a los revisores anónimos por sus valiosos comentarios que han servido para mejorarlo.

REFERENCIAS

[1] M. Crovella and B. Krishnamurthy, *Internet Measurement: Infrastructure, Traffic and Applications*, John Wiley and Sons Inc., New York, USA, 2006.

[2] R. Baeza-Yates, C. Castillo, and E. N. Efthimiadis, "Characterization of national Web domains," *ACM Transactions on Internet Technology*, vol. 7, no. 2, pp. 9, 2007.

[3] M. F. Arlitt and C. L. Williamson, "Internet Web servers: workload characterization and performance implications," *IEEE/ACM Transactions on Networking*, vol. 5, no. 5, pp. 631–645, Oct 1997.

[4] J. L. García-Dorado, J. A. Hernández, J. Aracil, J. E. López de Vergara, F. J. Montserrat, E. Robles, and T. P. de Miguel, "On the duration and spatial characteristics of Internet traffic measurement experiments," *IEEE Commununications Magazine*, vol. 46, no. 11, pp. 148–155, Nov. 2008.

[5] M. Izal, G. Urvoy-Keller, E. W. Biersack, P. A. Felber, A. Al Hamra, and L. Garcés-Erice, "Dissecting Bittorrent: Five months in a Torrent's lifetime," in *In Proceedings of Passive and Active Network Measurement Workshop*, Juan Les Pins, France, Apr. 2004, pp. 1–11.

[6] M. S. Borella, "Source models of network game traffic," *Computer Communications*, vol. 23, no. 4, pp. 403–410, 2000.

[7] Sally Floyd and Vern Paxson, "Difficulties in simulating the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 4, pp. 392–403, Aug. 2001.

[8] Kun-Chan Lan and John Heidemann, "Rapid model parameterization from traffic measurements," *ACM Trans. Model. Comput. Simul.*, vol. 12, no. 3, pp. 201–229, 2002.

[9] RedIRIS, "What is RedIRIS," http://www.rediris.es/rediris/index.en.html.

[10] R. van de Meent, M. R. H. Mandjes, and A. Pras, "Smart dimensioning of IP network links," in *In Proceedings of IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*, San José, USA, Oct. 2007, pp. 86–97.

[11] R. van de Meent, M. Mandjes, and Aiko Pras, "Gaussian traffic everywhere?," in *IEEE International Conference on Communications*, June 2006, vol. 2, pp. 573–578.

[12] J. Kilpi and I. Norros, "Testing the Gaussian approximation of aggregate traffic," in *ACM SIGCOMM Workshop on Internet Measurment*, 2002, pp. 49–61.

[13] Aiko Pras, Lambert Nieuwenhuis, Remco Meent van de, and Michel Mandjes, "Dimensioning network links: A new look at equivalent bandwidth," *IEEE Network*, vol. 23, no. 2, pp. 5–10, March 2009.

[14] Michal Pióro, *Routing, Flow, and capacity Design in Communication and Computer Networks*, Morgan Kaufmann, 2004.

[15] F. Mata, J. Aracil, and J. L. García-Dorado, "Automated Detection of Load Changes in Large-Scale Networks," in *International Workshop on Traffic Monitoring and Analysis*, May 2009, pp. 34–41.

[16] T. Oetiker and D. Rand, "MRTG: The Multi Router Traffic Grapher," in *USENIX Conference on System Administration*, 1998, pp. 141–148.

[17] Dario Rossi, Marco Mellia, and Michela Meo, "Understanding skype signaling," *Computer Networks*, vol. 53, no. 2, pp. 130 – 140, 2009, QoS Aspects in Next-Generation Networks.

[18] D.L. Donoho, "High-dimensional data analysis: The curses and blessings of dimensionality," *AMS Math Challenges Lecture*, 2000.

[19] K. Papagiannaki, N. Taft, Zhi-Li Zhang, and C. Diot, "Long-term forecasting of Internet backbone traffic," *IEEE Transactions on Neural Networks*, vol. 16, no. 5, pp. 1110–1124, Sept. 2005.

[20] R. A. Johnson and D. W. Wichern, *Applied multivariate statistical analysis*, Prentice-Hall International Editions, 1992.

[21] K. V. Mardia, "Measures of multivariate skewness and kurtosis with applications," *Biometrika*, vol. 57, no. 3, pp. 519, 1970.

[22] K. V. Mardia, "Assessment of multinormality and the robustness of Hotelling's T 2 test," *Applied Statistics*, pp. 163–171, 1975.

[23] K. V. Mardia, "Applications of some measures of multivariate skewness and kurtosis in testing normality and robustness studies," *Sankhyā: The Indian Journal of Statistics, Series B*, vol. 36, no. 2, pp. 115–128, 1974.

[24] T. W. Anderson, *An introduction to multivariate statistical analysis*, Wiley New York, 1958.

[25] A. Aurelius, C. Lagerstedt, M. Kihl, M. Perényi, I. Sedano, and F. Mata, "A Traffic Analysis in the TRAMMS Project," *Telekomunikacije*, vol. 4, pp. 29–37, 2009.

Arquitectura de una Entidad Middleware para la Gestión Cognitiva de las Comunicaciones en Terminales Multiradio

Luis Sánchez[†], Jorge Lanza[†], Johnny Choque[†], Luis Muñoz[†], Daniel González[‡]
Universidad de Cantabria[†], AT4Wireless[‡]
Laboratorios de I+D de Telecomunicaciones. Plaza de la Ciencia s/n, 39005, Santander (Cantabria)[†]
C/ Severo Ochoa, 2. Parque Tecnológico de Andalucía, 29590, Campanillas (Malaga) [‡]
{lsanchez,jlanza,jchoque,luis}@tlmat.unican.es[†], dgonzalez @at4wireless.com[‡]

***Resumen*- La próxima generación de sistemas inalámbricos deberá proveer acceso a un amplio rango de servicios de manera transparente para el usuario, embebiendo la tecnología en su entorno. La heterogeneidad será una característica fundamental y la tecnología tiene que aprovecharse de ella en lugar de verla como un obstáculo insalvable hacia el paradigma *"Always Best Connected"*. El principal objetivo de este artículo es describir una solución novedosa a uno de los principales retos a los que se van a enfrentar la futura generación de sistemas inalámbricos, la gestión óptima y transparente de múltiples redes de acceso inalámbrico heterogéneas. Para ello, se presenta la arquitectura de alto nivel de una entidad middleware, llamada Gestor de Comunicaciones, que, por un lado actuará como una capa superpuesta a nivel de Enlace de Datos que permita una interacción uniforme y transparente con las diferentes tecnologías de acceso de las que un dispositivo disponga, y por otro habilite una gestión cognitiva de los recursos disponibles que optimice la experiencia del usuario. Conjugar todas esas características en una arquitectura orientada a ser implementada en plataformas reales, con las restricciones tecnológicas que ello implica y bajo escenarios de aplicación novedosos, hacen del Gestor de Comunicaciones una propuesta innovadora.**

***Palabras Clave* - Gestor de Comunicaciones, Heterogeneidad, Gestión Cognitiva, middleware.**

I. INTRODUCCIÓN

En los últimos años se ha vivido una época que se podría considerar de despliegue en lo que a tecnologías de acceso radio se refiere. En esta fase, numerosas tecnologías han aparecido, cada una de ellas centrándose en un entorno de operación con diferentes características en términos de capacidad, área de cobertura o servicios soportados. Del mismo modo que estas tecnologías han ido siendo desarrolladas, los terminales móviles han ido incorporándolas por lo que en la actualidad no es raro disponer de dispositivos equipados con varias de estas tecnologías inalámbricas.

La heterogeneidad será por tanto un aspecto fundamental de la futura generación de comunicaciones inalámbricas. Con ella se inicia una nueva fase, cuya denominación podría ser de convergencia. El concepto de red se ha trasladado hacia la búsqueda del paradigma de conectar al usuario siempre de la mejor manera posible (ABC, *Always Best Connected*) [1]. Es necesario, por tanto, desarrollar mecanismos que —atendiendo a las necesidades de los servicios de los que disfruta el usuario en cada momento, así como a las propias preferencias de éste y a las posibilidades que cada una de las tecnologías de acceso radio disponibles ofrezcan— puedan manejar de manera inteligente y transparente para el usuario todos los recursos de los que dispone su terminal para proveer la mejor calidad de experiencia posible.

De manera paralela y gracias a la libertad que todas estas tecnologías dan al usuario, es posible pensar en un usuario permanentemente conectado ya no únicamente a la red (usuario-red), sino con otras personas (usuario-usuario) mediante servicios de voz, datos, videollamada, etc., lo cual le permitirá interactuar con el universo de servicios que hay, y habrá cada vez más, a su alrededor (información, entretenimiento, relaciones sociales, servicios públicos, etc.). En estas circunstancias se enmarca la estrategia del proyecto mIO! [2], centrada en sentar las bases para la creación de una nueva generación de servicios en movilidad, en la que las personas son el centro de la propuesta. Una de estas bases es poder sacar todo el partido posible a un dispositivo que viaja con el usuario en todo momento y que está siempre conectado, de tal forma que se convierta en una ventana abierta a la información relevante y personalizada que cada usuario requiere. Esto se define en el proyecto mIO! como información de contexto, considerando dentro de ella toda información significativa que sirve para caracterizar la situación de un usuario con el fin de seleccionar y personalizar los servicios más apropiados a dicha situación. En este sentido, la arquitectura mIO! define el Gestor de Contexto [3] como una entidad global que aglutina y formaliza semánticamente toda la información de contexto asociada al entorno del usuario y provee las interfaces necesarias para la actualización y uso de esta información por parte de los servicios y entidades definidas dentro de dicha arquitectura.

El objetivo de este artículo es especificar y definir la arquitectura, mecanismos y herramientas necesarios para la selección en tiempo real de la tecnología de comunicación más apropiada para acceder a los servicios, en función del entorno y las capacidades multiradio de los terminales, así como de los requerimientos de los servicios demandados por los usuarios. Para cumplir este objetivo y tener en cuenta todos los requerimientos que tiene asociado, se plantea la introducción de un middleware cognitivo, denominado Gestor de Comunicaciones (GC). Éste, haciendo un uso

inteligente de la información de contexto, gestionará las diferentes tecnologías de acceso con las que estén equipados los terminales de usuario mediante algoritmos de control de admisión de las llamadas, de selección de las interfaces inalámbricas o de decisión del traspaso entre las diferentes tecnologías de comunicaciones. De esta forma se consigue garantizar, por ejemplo, la Calidad de Servicio (QoS) requerida por los usuarios móviles o el justo balance de la carga entre las múltiples redes que componen el escenario heterogéneo considerado.

El resto del artículo se estructura de la siguiente forma. En la Sección II se hace una breve descripción de algunas de las iniciativas y proyectos de investigación que han planteado soluciones en la línea del presente trabajo y que constituyen el estado del arte en cuanto a la gestión de las comunicaciones en terminales multiradio. El escenario que se describe en la Sección III permite ilustrar una situación tipo en la que el GC se hace necesario. Además de presentar en la Sección IV el esquema global de la arquitectura del GC, se detallan las funcionalidades de cada uno de los componentes que forman parte de dicha arquitectura. La Sección V presenta en detalle el proceso de gestión y decisión que se lleva a cabo en el GC ante la aparición de un nuevo flujo de datos. Definida las funcionalidades del GC en el lado del terminal, en la Sección VI se realiza un análisis de la aplicación de dichas funcionalidades en el lado de la red. Por último, la Sección VII concluye este artículo resumiendo las principales contribuciones y planteando las líneas futuras que se pretenden abordar.

II. Estado del Arte e Iniciativas Relacionadas

En la actualidad se encuentran disponibles un amplio abanico de tecnologías de acceso radio con capacidades en continuo aumento, las cuales exigen una alta interoperabilidad entre sistemas y servicios. Las arquitecturas all-IP han sido las que, de manera tradicional, se han propuesto para dar respuesta a los retos tecnológicos impuestos por la heterogeneidad que implican los escenarios donde coexisten múltiples redes de acceso.

Las soluciones que se han propuesto tradicionalmente adoptaban mecanismos a nivel de red, en las cuales la movilidad se apoya fundamentalmente en soluciones IPv6, donde se dispone de un abanico más amplio de posibilidades de direccionamiento. Entre las soluciones planteadas, las que más respaldo han tenido son aquellas basadas en MIPv6 [4], como MEXT [5]. Sin embargo, los trabajos realizados se centran en la especificación de los mecanismos de traspaso entre redes sin definir el proceso que determine en qué momento se toma la decisión de ejecutar dicho traspaso. Además, uno de los principales problemas de este tipo de soluciones siempre ha sido su rigidez lo que hace que su comportamiento no sea a menudo suficientemente transparente [6]. En cualquier caso, la movilidad es sólo uno de los retos impuestos por los futuros sistemas de comunicaciones inalámbricas. La heterogeneidad es otra componente que es necesario abordar, así como la multiplicidad de interfaces de acceso en el mismo terminal y el multidominio (multihoming). En este sentido, MultiHoming Transport Protocol (MHTP) [8] es una propuesta realizada como protocolo para soportar multidominio en la capa de red IPv6. El principal problema de este tipo de soluciones es que usan entidades intermedias y por tanto puede ocurrir que eventualmente alguno de los enrutadores intermedios necesite informar al origen de alguna circunstancia de la red (Ej. mensaje ICMP), lo cual no es posible al haber sido modificada su dirección después del traspaso. Por su parte, el protocolo SHIM6 (Site Multihoming by IPv6 Intermediation) [7] especifica una propuesta para enfocar el problema de habilitar multidominio. Basa su funcionamiento en la definición de una subcapa localizada entre el enrutamiento IP y la salida de los paquetes a los diferentes aplicativos. Se trata por tanto de una solución extremo a extremo que se puede aplicar de forma transparente sobre cualquier red. Este tipo de soluciones basadas en middleware ofrecen mayor flexibilidad a la vez que no implican modificaciones en ningún elemento de la red.

Si bien las soluciones a nivel de red dotan de transparencia y compatibilidad al sistema y a los servicios que se proveen sobre él, como se ha visto, no existe una solución única para los dos principales problemas que subyacen en entornos con múltiples tecnologías de acceso, la continuidad de la sesión ante situaciones de traspaso y el soporte del multidominio.

Una de las aproximaciones que se han propuesto como alternativa a las soluciones tradicionales se basa en el desarrollo de una entidad middleware que se sitúe entre la capa de red y las tecnologías de acceso subyacentes. El estándar IEEE 802.21 [9] se enmarca dentro de este tipo de soluciones. El principal propósito del estándar IEEE 802.21 es permitir el traspaso entre tecnologías heterogéneas (incluyendo las IEEE 802 y las de acceso celular) sin necesidad de interrumpir el servicio. Muchas de las funcionalidades necesarias para soportar la continuidad de las sesiones en curso dependen de mecanismos complejos específicos de cada tecnología. IEEE 802.21 proporciona un marco que permite a los niveles superiores interactuar con los niveles subyacentes para que estos soporten la continuidad del servicio sin necesidad de conocer las características intrínsecas de cada tecnología en particular. Aún cuando ésta sea la funcionalidad básica que se persigue, los requerimientos de tipo contextual relacionados con el usuario no están enteramente recogidos en la arquitectura y servicios propuestos por IEEE 802.21. Estas posibilidades sí se estudian en proyectos como MAGNET [10] y Ambient Networks [11], utilizando estrategias, [12] y [13] respectivamente, que a su vez ocultan a las capas superiores la complejidad subyacente. Además, se implementan mecanismos basados en optimización intercapa con el objetivo de asegurar el paradigma ABC, a través de la gestión inteligente de las interfaces de comunicaciones de las que disponen los terminales móviles, mejorando así el rendimiento de las comunicaciones. No obstante, dicha optimización intercapa solo tiene en cuenta métricas de nivel de enlace a la hora de seleccionar la interfaz con el mejor rendimiento en cada momento.

Teniendo en cuenta lo mencionado, este artículo propone la arquitectura de un Gestor de Comunicaciones que pretende ir más allá de dichas limitaciones. Por una parte, recoge información de diversas fuentes, entre ellas:

- Información de las interfaces radio que incorpora el terminal móvil (Ej. relación señal a ruido (SNR), potencia de señal recibida, carga del canal, etc.)
- Requerimientos de los servicios (Ej. ancho de banda, seguridad, etc.)
- Información del propio usuario (Ej. preferencias en cuanto a coste, prioridades, etc.)
- Información de entorno que rodea al usuario (Ej. capacidades adicionales de la infraestructura, etc.).

Por otra parte, toma decisiones en función de la información adquirida para actuar sobre los módulos encargados del manejo de los flujos de datos y de la gestión de los recursos radio disponibles. En este sentido el GC incorpora capacidades cognitivas al tener un pleno conocimiento del estado actual del usuario, el terminal y el entorno que los rodea. En la sección V se describe con detalle el alcance de las capacidades cognitivas del GC.

III. Escenario de Gestión de las Comunicaciones

En esta sección se describe a modo de ejemplo ilustrativo una situación en la que se requiere la actuación del Gestor de Comunicaciones, con el objetivo de ilustrar de manera sencilla las funcionalidades que ejecuta.

Se parte de la situación en la que el usuario enciende su dispositivo móvil equipado con las últimas tecnologías de comunicaciones, HSPA, WiMAX y WiFi.

En un momento dado inicia una aplicación para realizar un backup de la información de su terminal en un servidor remoto. En su perfil de usuario está definido que esta aplicación tiene baja prioridad y, debido a la gran cantidad de datos que transfiere, preferentemente deben emplearse redes de acceso en las que el usuario esté subscrito a una tarifa plana o que no impliquen ningún coste para él.

En ese momento el usuario se encuentra dentro del área de cobertura de la red WiMAX de la universidad a la que pertenece por lo que, cuando el flujo comienza, el GC analiza los requerimientos del servicio y las restricciones impuestas por el usuario y se configura para dar a ese flujo el mayor ancho de banda disponible de forma gratuita.

Cuando entra en su edificio, se detecta la existencia de un acceso a la red WiFi de la universidad. Dado que esta red también es gratuita, el GC decide multiplexar el flujo de datos sobre las dos redes de acceso para aumentar el ancho de banda. Al cabo de un tiempo se pierde la cobertura de la red WiMAX, continuando el servicio de backup únicamente a través de la red WiFi.

En un instante posterior el usuario inicia un streaming de video, disparando nuevamente el análisis de los requerimientos de este servicio por parte del GC . El usuario tiene definido que este servicio tiene una prioridad media (superior a la del servicio de backup) por lo que a la vista de los recursos disponibles el GC decide reservar los recursos necesarios para el streaming y dejar el resto para el servicio de backup. Como en este caso sólo dispone del acceso por WiFi, el GC tendrá que imponer mecanismos de priorización y reserva de recursos para asegurar el ancho de banda y cumplir con los parámetros exigidos por el flujo del servicio de streaming dejando el resto para el flujo del servicio de backup.

Una vez terminada la jornada laboral y mientras se dirige a casa, nuestro usuario inicia una videollamada. Este servicio está definido como de alta prioridad y además en su perfil ha indicado que no le importa realizar un pago adicional para mantener el servicio si fuera necesario. Al iniciar la videollamada se encuentra en la cobertura de las redes WiFi, WiMAX y HSPA. El GC determina que la mejor opción en este caso es WiMAX debido a que proporciona un mayor ancho de banda comparado con WiFi y HSPA y por tanto fuerza a que el flujo vaya a través de esta interfaz. Al alejarse de la universidad la red WiMAX no ofrece las garantías necesarias debido a la pérdida de cobertura, por lo que el GC decide traspasar el flujo a la red HSPA ya que, a pesar de que ofrece un menor ancho de banda, sigue cumpliendo con los requerimientos impuestos por el perfil de usuario.

IV. Arquitectura del Gestor de Comunicaciones

Tal y como se refleja en la Figura 1, la arquitectura propuesta tiene una estructura modular en la que cada uno de los módulos se encarga de las diferentes funciones previstas para el Gestor de Comunicaciones.

A. Capa de Adaptación

Este módulo es el encargado de unificar el acceso a las diferentes interfaces de comunicaciones con las que el terminal multiradio pueda estar equipado. De esta manera, el resto de componentes de la arquitectura tendrán una interfaz única con la que interactuar tanto a nivel de control como a nivel de plano de datos. Mientras que el plano de control se encarga de extraer información relevante sobre las diferentes tecnologías de acceso disponibles y los mecanismos que soportan para la gestión de los flujos de datos, el plano de datos gestiona de manera transparente los paquetes de acuerdo a las decisiones tomadas por el Motor Cognitivo de Decisión (Ej. empleando la mejor interfaz radio previamente seleccionada).

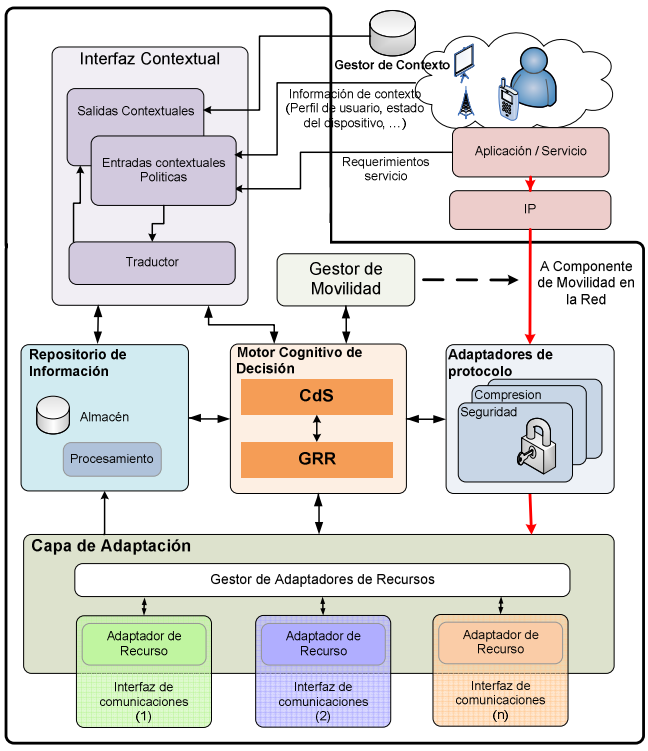


Fig. 1 Arquitectura del Gestor de Comunicaciones

Los componentes que forman la Capa de Adaptación son:

- Adaptadores de Recursos: Se trata de módulos específicos que interactúan con cada uno de los interfaces de comunicaciones. Son los encargados de transformar los comandos genéricos en implementaciones específicas del interfaz correspondiente. Asimismo, son los encargados de extraer las estadísticas de cada interfaz.
- Gestor de Adaptadores de Recursos: Se encarga de coordinar los distintos Adaptadores de Recursos. Exporta a través de un interfaz único las estadísticas de cada interfaz de red, ofrece una serie de comandos genéricos mediante los cuales se puede actuar sobre el proceso de envío y recepción de tráfico, y gestiona los diferentes flujos de datos orientándolos hacia el interfaz de salida oportuno. Alguna de las modalidades de gestión que se pueden implementar en el GC son las siguientes: multiplexación del tráfico sobre varias interfaces de red simultáneamente; asignación de los flujos de tráfico a la interfaz de red especificada; priorización de flujos de tráfico asignados a una misma interfaz de red; aplicación de técnicas de mejora propias de las interfaces de comunicaciones (Ej. QoS basado en 802.11e).

B. Motor Cognitivo de Decisión

Se trata de la inteligencia del GC. El Motor Cognitivo de Decisión está dividido en dos sub-módulos que se reparten la jerarquía de decisión. En este sentido, las decisiones sobre qué requisitos necesitan ser considerados como candidatos potenciales a la hora de asignar recursos a los servicios, se toman en el Módulo de Calidad de Servicio (CdS), que es el encargado de maximizar la experiencia del usuario. Por otro lado, los mecanismos que deciden la forma de asignar esos recursos haciendo el mejor uso de las capacidades subyacentes se implementan en el Gestor de Recursos Radio (GRR).

- Módulo de Calidad de Servicio: Sobre este módulo recae la toma de decisiones basadas en las diferentes entradas provenientes de los servicios, Gestor de Contexto, preferencias, perfiles de usuario, etc. El CdS procesa toda esta información y selecciona el subconjunto de requisitos que necesariamente deben ser mapeados sobre los recursos disponibles de las interfaces de red a través del GRR. Si es necesario, el CdS activará los Adaptadores de Protocolo necesarios para cumplir con los requisitos que no han sido seleccionados. El módulo CdS desconoce las características de todos los interfaces de comunicación y por tanto realiza el procesamiento basándose en la información que el GRR le proporcione. Por su parte, y gracias a mecanismos de inferencia y aprendizaje, el CdS será capaz de adaptar sus decisiones dinámicamente.
- Gestor de Recursos Radio: Es el encargado de asignar y coordinar los recursos de comunicación de los que dispone el terminal móvil en función de las especificaciones de calidad de servicio definidas en el CdS y del conocimiento que posee acerca de las capacidades del terminal. Para ello, obtiene toda la información acerca de los recursos radio del terminal a través de la Capa de Adaptación, selecciona la mejor interfaz o grupos de interfaces, y asigna los recursos radio necesarios, imponiendo a la Capa de Adaptación cuál debe ser la modalidad de gestión a emplear. Esto permite al GRR dar un tratamiento individualizado a cada flujo de datos, asignándoles de manera óptima los recursos que, en la medida de lo posible, cumplan los requisitos exigidos.

C. Adaptadores de Protocolo

Operan en el plano de datos de la arquitectura y se encargan de aquellas funcionalidades que puedan ser necesarias para soportar los requerimientos impuestos bien por el usuario o por los servicios. Algunos ejemplos pueden ser seguridad (cifrado y autenticación), compresión de datos, corrección de errores, etc.

D. Repositorio de información

En él se concentra toda la información que el Gestor de Comunicaciones es capaz de recolectar por sus propios medios. Las estadísticas relativas al estado de los interfaces de comunicaciones gestionados en la Capa de Adaptación se almacenan en este repositorio para que estén disponibles para el Motor Cognitivo de Decisión. Manteniendo toda esta información en un solo repositorio se evitan problemas de ineficiencia tanto por la posibilidad de tener información duplicada como por la dispersión de la información. Asimismo, cabe la posibilidad de implementar mecanismos que permitan inferir parámetros más representativos de las estadísticas provenientes de la Capa de Adaptación. Este procesamiento previo será de bajo nivel, pero ayudará al Motor Cognitivo de Decisión (al GRR de manera más específica) a la hora de tomar sus decisiones.

E. Módulo de gestión de la Movilidad

Uno de los aspectos fundamentales que deben soportarse en el GC es el de dar cabida a la movilidad durante la provisión de los servicios. Para ello, no es suficiente con especificar la arquitectura interna del terminal sino que es necesario dotar a la infraestructura de acceso de los mecanismos necesarios para garantizar la continuidad y transparencia de las sesiones ante situaciones de traspaso, multihoming, etc. La solución que se plantea dentro del GC se basa en el principio de traspasos asistidos desde el terminal. En este tipo de arquitectura, la gestión de la movilidad se realiza principalmente en la red pero ésta recibe la colaboración por parte del terminal móvil. En el caso en que una de las peticiones del Motor Cognitivo de Decisión implique el cambio de red de acceso o el uso de varias de éstas, este módulo informará a la parte de gestión de la movilidad que reside en la red, de forma que la provisión del servicio pueda continuar de manera transparente. Aunque el soporte de la movilidad por parte de la red de acceso se describe en la Sección VI, cabe destacar que la arquitectura del GC, en cuanto a la movilidad se refiere, es lo suficientemente flexible como para adoptar cualquier solución y para ello se han creado interfaces software genéricas que faciliten su adopción.

F. Interfaz Contextual

Gran parte de la información que el GC necesita para manejar de manera inteligente los flujos de información proviene de las necesidades y requisitos impuestos por el usuario, de la propia infraestructura que le rodea en un

momento dado o de los servicios a los que corresponden esos flujos, son adquiridos a través del Interfaz Contextual. Además, el propio GC se puede convertir en un proveedor de información relevante para otras entidades. En este sentido, y de forma genérica, el Interfaz Contextual es el encargado de interactuar con el Gestor de Contexto, tanto para extraer de él información como para proveerla llegado el caso. Los sub-módulos que lo componen son:

- Entradas contextuales y Políticas: Es el interfaz entre el Motor Cognitivo de Decisión y los requerimientos y políticas de nivel de servicio impuestas. Esta información es la que emplea el Motor Cognitivo de Decisión para asegurar que el usuario siempre tenga la mejor calidad de experiencia posible cuando accede a los servicios. En la mayoría de los casos, este módulo interactuará con algún tipo de gestor de información de contexto.
- Salidas contextuales: Este módulo se encarga de proveer la información de la que dispone el GC hacia el Gestor de Contexto. Así, la información sobre el estado de las diferentes redes de acceso disponibles, la manera en que se gestionan los diferentes flujos, las estadísticas de tráfico, etc. puede estar disponible para otros elementos.

V. GESTIÓN COGNITIVA DE LOS RECURSOS DE COMUNICACIÓN

Se han considerado varios principios de diseño a la hora de elaborar la arquitectura del GC, los cuales han quedado reflejados en los módulos descritos en la Sección III. Uno de estos principios es el acceso uniforme y transparente a las diversas características intrínsecas de las tecnologías de red que incorpora el terminal. Este principio se ha empleado con éxito en propuestas anteriores, como en [13] y [14] donde se describen arquitecturas de nivel de enlace que permiten comparar y evaluar diferentes tecnologías de acceso como parte del proceso de selección de las mismas y también comparar las diferentes capacidades y rendimientos del nivel de enlace a la hora de asignar los recursos de red adecuados que cumplan con los requerimientos del servicio. Sin embargo, el alcance del presente trabajo va más allá, teniendo en cuenta no sólo la información del nivel de acceso radio a la hora de elegir la mejor interfaz, sino también otras fuentes de información como el perfil y las preferencias del usuario u otra información de contexto.

En este sentido, uno de los principios más relevantes del diseño del Gestor de Comunicaciones es la utilización de algoritmos de decisión multi-paramétricos que permiten elegir la mejor interfaz de comunicaciones en función de la información recibida de diversas fuentes, actuando en consecuencia sobre los flujos de información de acuerdo a esas decisiones. Considerando que posiblemente el GC maneje un gran número de criterios de decisión, se diseña la parte cognitiva del mismo en base a técnicas Multi-Attribute Decision Making (MADM) de manera similar a como se han utilizado en [15], [16], y [17]. Dichas técnicas emplean algoritmos cuya eficiencia y carga computacional permiten su ejecución en tiempo real, aunque en general el resultado que obtienen solo es una aproximación al valor óptimo [18]. A su vez, muchas de ellas emplean modelos de ponderación que permiten dar el peso adecuado a cada parámetro a tener en cuenta durante la toma de decisiones. La elección del peso correcto de cada variable permite finalmente obtener la decisión más adecuada. En este caso se podría recurrir al uso de técnicas de optimización para obtener los valores óptimos de dichos pesos previamente a la ejecución del GC [19], permitiendo de esta forma encontrar el límite superior del rendimiento del algoritmo empleado.

La gestión cognitiva de la información a la hora de elegir la interfaz de red más adecuada, en base a los algoritmos de decisión multi-paramétricos, queda reflejada en la interacción que existe entre los módulos CdS y GRR. La Figura 2 muestra un ejemplo de la relación existente entre dichos módulos y sirve para mostrar la lógica que se utilizará a la hora de la toma de decisiones. Si bien a modo de ejemplo se han particularizado algunas métricas para la toma de decisiones en la descripción, es importante reseñar que la definición de éstas es genérica y se admiten tantas como sean capaces de soportar los algoritmos de decisión y aprendizaje que se implementen en el Motor Cognitivo de Decisión.

En primer lugar, se asume que el GC ha detectado la presencia de dos redes de acceso, una WiFi de 5 Mbps, gratuita y sin seguridad; y otra UMTS de 2Mbps, con un coste de 0,01€/Mbyte y con baja seguridad. El usuario desea hacer uso de dos servicios, uno denominado S1 con requerimiento de ancho de banda (BW) mínimo de 4 Mbps y seguridad alta; y otro denominado S2 con ancho de banda mínimo de 3 Mbps y baja seguridad. Por su parte el usuario prefiere utilizar un servicio sin coste alguno pero está dispuesto a asumir un coste reducido si es necesario. También ha definido dar una alta prioridad al servicio S1 y una baja prioridad al S2.

Los pasos a seguir son los siguientes:

1.- Inyección de parámetros básicos para la toma de decisiones:
   - Características del servicio S1, S2
   - Preferencias del usuario
   - Estadísticas de contexto (batería, etc.)

2.- Detección de tráfico de los servicios

3.- CdS ejecuta algoritmo de decisión
   Generación de funciones de utilidad:
   U_{S1}*(BW, seguridad, coste, prioridad)*
   U_{S2}*(BW, seguridad, coste, prioridad)*
   Y utilidades mínimas:
   T_{S1} = (BW>4Mbps, seg=alta, coste=0, prior=alta)
   T_{S2} = (BW>3Mbps, seg=baja, coste=0, prior=baja)

4.- Informar de resultado al GRR

5.- GRR trata de cumplir con los umbrales T_{S1} y T_{S2} definidos para U_{S2} y U_{S1} . En base a la prioridad de los servicios intenta primero asignar recursos a S1 y luego a S2.

6.- GRR dispone de dos interfaces de red, una WiFi de 5Mbps, a coste cero y sin seguridad; y otra UMTS de 2Mbps, a 0,01€/Mbyte y con baja seguridad. Por tanto no cumple $U_{S1} > T_{S1}$ ni $U_{S2} > T_{S2}$ y devuelve respuesta a CdS con información de los recursos que dispone:
   S1 – BW 4Mbps, sin seguridad
   U_{S1}*(4 Mbps,* ***NO****, 0€/Mbyte)*
   S2 – BW 3Mbps, con coste y seguridad baja
   U_{S2}*(3 Mbps, baja,* ***0,01€/Mbyte****)*

   Para el caso de S2, el GRR asume la posibilidad de multiplexar el flujo de datos sobre ambas interfaces, tal como se explica en el paso 11.

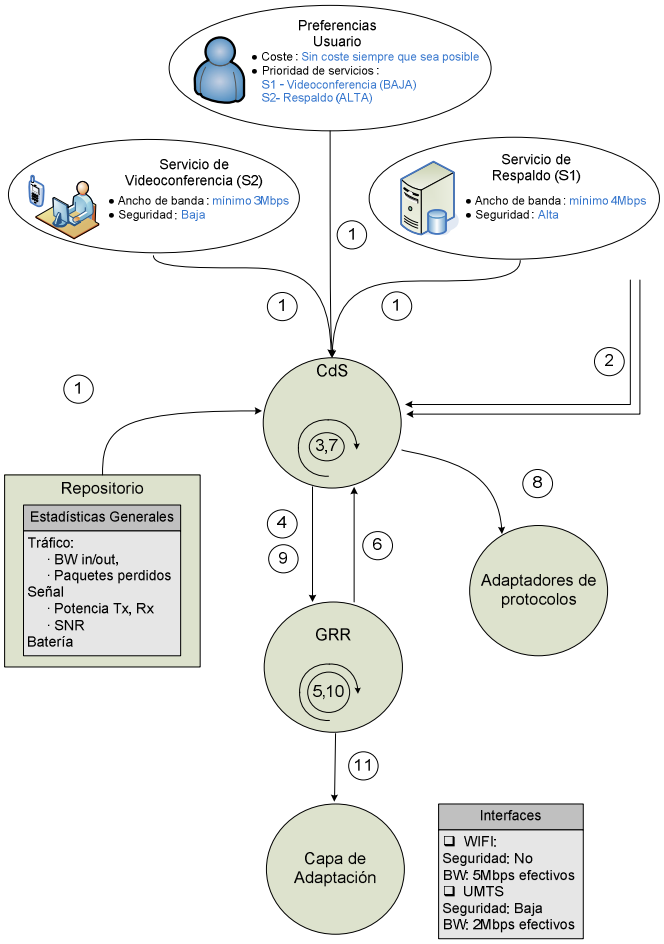


Fig. 2 Diagrama de flujo de la gestión cognitiva de las comunicaciones

7.- CdS ejecuta nuevamente el algoritmo a partir de la respuesta de GRR.
Define nuevas de funciones de utilidad debido a que la prioridad ya ha sido utilizada:
$U'_{S1}(BW, seguridad, coste)$
$U'_{S2}(BW, seguridad, coste)$
Calcula las correspondientes utilidades mínimas. Debido a que dentro de su perfil indica que puede asumir cierto coste, entonces en este caso el parámetro de coste puede ser diferente de cero.
T'_{S1} = (BW=4Mbps, seg=no, coste=0)
T'_{S2} = (BW=3Mbps, seg=baja, coste=0,01€/Mbyte)

8.- CdS decide activar el Adaptador de Protocolo correspondiente para cumplir con los requisitos de seguridad del servicio S1. Por consiguiente, le pasa como parámetro un nivel de seguridad alto.

9.- CdS informa del resultado al GRR.

10.- GRR trata de cumplir con los umbrales T'_{S1} y T'_{S2} definidos para U'_{S2} y U'_{S1}

11.- Al no poder asignar el ancho de banda para el servicio S2 sobre los recursos de una única interfaz, el GRR ordena a la Capa de Adaptación dirigir el flujo de datos de S2 sobre el remanente de WiFi (1Mbps) y el disponible de UMTS (2Mbps).

VI. Soporte para la Gestión Inteligente de las Comunicaciones en la Infraestructura

Como ya se mencionó en la Sección III, la solución para la gestión de la movilidad propuesta en este artículo, pasa por la implantación de algunos módulos del GC en la red, que, coordinados con los disponibles en los terminales, permitan ofrecer valor añadido no sólo a los usuarios, sino también a los operadores de red. En este sentido, nuevamente el GC pretende ofrecer una solución que implique una extensión a las soluciones tradicionales.

Parece claro, y las diferentes implementaciones de soluciones de movilidad, Ej. MIPv6, así lo corroboran, que la movilidad debe ser soportada desde la red, pues esta será la encargada de regular los traspasos y dar a conocer los nuevos identificadores de red asignados a los terminales de usuario. No obstante, los módulos del GC en la red se sustentan en una infraestructura inteligente capaz de soportar en la mayoría de los casos una alta carga computacional, por lo que inicialmente serían capaces de proporcionar funcionalidades adicionales. Por tanto, se plantea un GC en la red (Figura 3) que disponga de una inteligencia, de forma similar a los terminales, pero enfocándola al entorno proveedor y su modelo de negocio específico. La colaboración entre las entidades de red y los terminales de usuario permitirá un uso optimizado de los recursos que reporte beneficios tanto para el usuario como para el proveedor que gestiona la infraestructura de acceso.

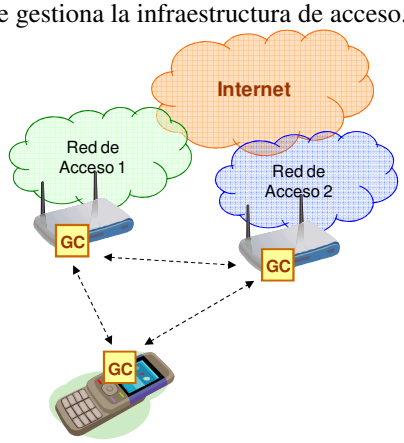


Fig. 3 Disposición de los gestores de comunicaciones en el entorno

Si se ahonda en el problema del soporte de la movilidad entre redes se observa que es necesaria una gestión inteligente de los traspasos sobre todo en el caso que un usuario se desplace entre diferentes redes de múltiples proveedores. Los servicios de roaming de las redes de comunicaciones móviles son el paradigma de los acuerdos entre empresas para dar continuidad a los servicios de usuario. Sin embargo estos acuerdos, preestablecidos de antemano, no incluyen el acceso a redes inalámbricas de área local ni metropolitana. Resolver la necesidad de gestionar la movilidad entre redes, estableciendo acuerdos de uso en tiempo real, considerando la asignación de recursos de forma dinámica para los usuarios en movilidad, garantizando la confidencialidad y privacidad de los datos en la transmisión entre redes, etc., es una cuestión que las redes de nueva generación deben resolver, más aun teniendo en cuenta el masivo despliegue de infraestructuras 802.11abgn que se está realizando por parte de múltiples proveedores y que deberán coexistir en este nuevo ambiente. Los módulos del GC en la infraestructura constituyen las pasarelas inteligentes que negociarán e intercambiarán toda la información relativa a la gestión de los recursos y la movilidad.

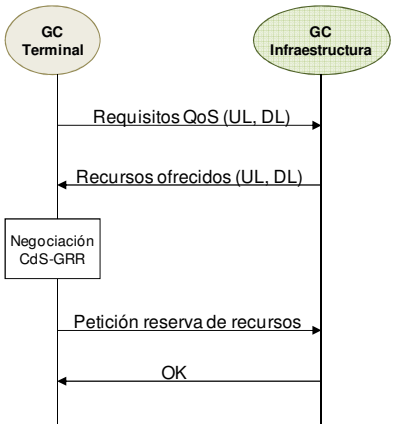


Fig. 4 Negociación de asignación de recursos de comunicaciones entre terminal e infraestructura

Otro aspecto que en el corto plazo se va a erigir como una de las principales líneas de negocio por parte de las compañías proveedoras de servicios es ofrecer servicios diferenciadores que hagan que el usuario se sienta único. La tarea del GC en la red o infraestructura del proveedor juega en este punto un papel relevante. Hasta el momento la red ofrece a los usuarios unas capacidades en cierto modo estáticas y es el usuario quien desde su terminal las gestiona. No obstante, la gestión de flujos de servicios puede depender del tipo de usuario generador de esos flujos, asignando prioridades a usuarios preferenciales, cortando o reduciendo las capacidades de la conexión de otros usuarios, etc.. A pesar de que algunas de estas acciones ya se llevan a cabo en algunas situaciones, el disponer de una entidad distribuida entre los clientes y el operador permite que la reacción ante los posibles cambios sea más suave y fluida, pudiendo incluso disponer de información adicional (señalización entre entidades) para implementar la decisión más favorable para ambas partes. La Figura 4 muestra un ejemplo básico de la negociación entre el terminal y la infraestructura para la asignación de recursos de comunicaciones. El terminal de usuario conocedor de las necesidades de un servicio negocia con la red unos recursos mínimos y la red, mediante la inteligencia inherente en los GCs, es capaz de asignarlos de forma eficiente no sólo al servicio en cuestión, sino compartiéndolos con otros servicios que puedan estar corriendo.

VII. Conclusiones y Líneas Futuras

La utilización inteligente y transparente para el usuario de las tecnologías de acceso radio será uno de los elementos que nos llevarán hacia la Red de Redes y la Red de Servicios que se prevé sea la Internet del Futuro. El empleo de información de contexto a la hora de manejar las comunicaciones de un usuario que accede a todo tipo de servicios mientras se mueve será sin duda el aspecto clave para poder llevar a cabo este paradigma. En este artículo se ha presentado la arquitectura de alto nivel de un Gestor de Comunicaciones destinado a contribuir de manera efectiva en estos paradigmas. Sobre la base de una entidad middleware, cuyo primer objetivo es el de ocultar la heterogeneidad en cuanto a tecnologías de acceso se refiere a los niveles superiores de la arquitectura, se implementan tanto los módulos que recogerán la información de contexto relevante, así como un motor de decisión que, de manera cognitiva, gestionará los flujos de información asociados a cada uno de los servicios de los que disfruta el usuario, optimizando la calidad de experiencia de éste. Esta arquitectura representa una solución avanzada para habilitar la creación de una nueva generación de servicios en movilidad, en la que el usuario, situado como centro del diseño, esté en todo momento conectado de la manera más adecuada no sólo atendiendo a las circunstancias del entorno sino también a sus propias preferencias.

La implementación del Gestor de Comunicaciones se enmarca dentro de la planificación del Proyecto mIO! [2]. Así se desarrollará una plataforma de demostración ajustada los requerimientos de los escenarios de aplicación especificados en [20] y sobre la que se realizarán diversas pruebas de concepto de los diferentes módulos del Gestor de Comunicaciones, teniendo en cuenta su operativa como entidad lógica única. Se pretende con ello evaluar la viabilidad y el rendimiento de los diversos módulos, validando de esta forma la adecuada interoperabilidad entre ellos. A su vez, se adoptarán soluciones de movilidad y multihoming, en principio MIPv6 y SHIM6 respectivamente, como bases para la implementación del proceso de traspaso controlado por el Motor Cognitivo de Decisión. Adicionalmente se está trabajando en entornos de validación que involucran tecnologías de comunicación tan diversos como Bluetooth, WiFi y 3G(HSPA), con el objetivo de abarcar desde redes de área personal hasta las de área extensa. Los resultados de las pruebas de rendimiento y viabilidad serán especificados en futuros entregables comprometidos dentro del Proyecto mIO!.

Agradecimientos

Este artículo se ha generado dentro del proyecto mIO! (Expediente CENIT-2008 1019) subvencionado por el Centro para el Desarrollo Tecnológico Industrial (CDTI). Los autores quieren agradecer al resto de socios participantes la participación en las discusiones que han desembocado en el refinamiento de los resultados presentados.

Referencias

[1] E. Gustafsson, A. Jonsson, “Always best connected”, IEEE Wireless Communications, vol. 10, nº 1 , pp. 49–55, February 2003.

[2] Proyecto mIO! – Programa CENIT-Ingenio 2010, http://www.cenitmio.es/

[3] iSOCO, Telefónica I+D, “Diseño de la infraestructura de gestión de contexto”, Entregable E1.2.2 del Proyecto mIO!, 7 de Agosto del 2009.

[4] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, RFC 3775, Jun. 2004.

[5] IETF, “Mobility EXTensions for IPv6 (mext) charter”. Diciembre de 2008.

[6] Yoon-Young An, Chang-Min Park, Sung Back Hong, “The method for Reducing Packet Loss in Handover Service of Mobile IPv6,” AIC 29th Conference, Dic. 2003.

[7] E. Nordmark, M. Bagnulo, “Multihoming L3 Shim Approach,” IETF Internet Draft, January 2005.

[8] M. Py, “Multi Homing Translation Protocol (MHTP),” Internet Draft, IETF, November 2001.

[9] IEEE P802.21/D14.0 Media Independent Handover Services, Sept. 2008.

[10] FP6-IST-IP-507102 ‘My personal Adaptive Global Net’ IST-MAGNET project. http://www.ist-magnet.org/

[11] FP6-IST-IP-507134 WWI Ambient Networks. http://www.ambient-networks.org/

[12] Sanchez, L., Lanza, J., Muñoz, L.: 'Performance Evaluation of a Cross-layer based Wireless Interface Dynamic Selection on WPAN/WLAN Heterogeneous Environments: An Experimental Approach', Proceedings from 6th International Workshop on Applications and Services in Wireless Networks, May 2006.

[13] Sachs, J., et al, "Generic Abstraction of Access Performance and Resources for Multi-Radio Access Management", 16th IST Mobile and Wireless Communications Summit, 2007, Page(s): 1 – 5.

[14] Munoz, L., et al, "Empowering next-generation wireless personal communication networks", IEEE Communications Magazine, Volume: 42 , Issue: 5, Year: 2004 , Page(s): 64 – 70.

[15] Hao Hu; Wenan Zhou; Shu Zhang; Junde Song, "A Novel Network Selection Algorithm in Next Generation Heterogeneous Network for Modern Service Industry", IEEE Asia-Pacific Services Computing Conference, 2008. APSCC '08. Page(s): 1263-1268.

[16] Xing, B.; Nalini Venkatasubramanian, "Multi-constraint dynamic access selection in always best connected networks", The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. Page(s): 56-64.

[17] Chen Gu; Yong Zhang; Wenjing Ma; Ningning Liu; Yi Man, "Universal Modeling and Optimization for Multi-Radio Access Selection", 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. Page(s): 1-4.

[18] Olabisi E. Falowo, H. Anthony Chan, "Joint call admission control algorithms: Requirements, approaches, and design considerations", Computer Communications, v.31 n.6, p.1200-1217, April, 2008.

[19] Yi Sun; Yuming Ge; Jue Yuan; Jihua Zhou; Herborn, S.; Dongdong Chen;, "PAWES: A Flow Distribution Algorithm Based on Priority and Weight Self-Production", IEEE Wireless Communications and Networking Conference, 2009. WCNC 2009. Page(s): 1 - 6.

[20] Telefónica I+D, "Escenarios mIO! Primera Revisión", Entregable E7.1.2 del Proyecto mIO!, 15 de Marzo del 2010.

E3MS: A traffic engineering prototype for autoprovisioning services in IP/DiffServ/MPLS networks

Xavier Hesselbach[1], Joan Antoni García-Espín[2], Miquel González[3,] Javier Gonzalo[4], Sergi Figuerola[2]
[1]Departamento de Ingeniería Telemática, Universidad Politécnica de Cataluña UPC. C/ Jordi Girona, 1 y 3, Mod. C3 – Campus Nord, 08034 Barcelona.
[2] Fundación i2CAT, C/ Jordi Girona, 1 y 3. Edificio Nexus. 08034 Barcelona.
[3] Tecsidel. Avda. Príncipe de Asturias, 43-45, 2º, Barcelona.
[4] Vodafone R&D. Software Lab. Huesca.
xavierh@entel.upc.edu, joan.antoni.garcia@i2cat.net, miquel.gonzalez@tecsidel.es, javier.gonzalo@vodafone.com, sergi.figuerola@i2cat.net.

***Abstract*- This paper presents the testbed definition, implementation and trials of a new strategy for traffic autoprovisioning for MPLS and IP/DiffServ. This is the proof of concept of a new scenario for traffic engineering, for self-configuring control and end-to-end quality of service management by means of a tool based on Web Services. The system is structured in 3 layers: A Graphical User Interface, a Network Elements layer (an interface to physical devices) and, in the middle, a Network Management System layer, where decisions about admission, load balancing, path selection, re-routing and bandwidth allocation per class are taken. The system includes Dynamic Resource Allocation (DRA) and Background Monitoring System (BMS) modules to globally manage network resources. The so-called Squatter and Legalization mechanisms are introduced as novelties added to traffic engineering. Those strategies permit the use of part of the available resources from other classes only while unused by the class owning them. The trials have validated the management system, using Cisco routers.**

***Keywords*- MPLS, autoprovisioning, traffic classification, dynamic resource allocation, rerouting.**

I. INTRODUCTION

Currently, MPLS (MultiProtocol Label Swithing) is considered one of the mechanisms that better performs the network service convergence of voice, video and data required nowadays, mainly due to its traffic engineering functionalities, which provides class of service tagging, traffic prioritization and resource optimization, by means of LSP (Label Switched Paths). However, in order to support the trend of IP towards the universal transport network - even in operator transport networks - new mechanisms to assure quality-of-service (QoS) need to be provided, since these networks have been so far designed for best effort traffic, which means that no guarantees are provided to the data flow. Up to now, in the best situation, quality is provided with limited QoS mechanisms.

DiffServ-over-MPLS architecture provides differentiated services with guaranteed QoS. For the end to end QoS guaranteed service provisioning, current IP networks need to be enhanced in availability and guaranteed QoS provisioning, although they offer flexibility and scalability. To guarantee the user-requested demands and to keep the network utilization as best as possible, the performance management of DiffServ-over-MPLS is essential. Therefore, there is a need to enhance MPLS network functionalities to fully support integrated mechanisms with DiffServ, providing automatic provisioning based on class of service mapping on queues, queues dimensioning and scheduling schemes. UMTS (Universal Mobile Telecommunications System) networks support four traffic classes: Conversational, Streaming, Interactive and Background, each of them requiring different QoS parameters. Conversational and streaming require end to end QoS to provide bandwidth, delay and jitter guarantees. Interactive and background classes are less strict for QoS parameters but even require service differentiation. The strategies presented on this paper will provide end to end QoS guarantees for UMTS services on MPLS networks [1], [2].

In order to achieve and provide the end-to-end QoS level required in the Next Generation Internet, this paper considers two essential schemes: (i) Differentiated Services (DiffServ) and (ii) MPLS-TE capabilities [3], [4], under a management tool architecture based on a Web Service approach for the automatic resource provisioning based on service differentiation, queue mappings, dimensioning and scheduling schemas. In this proposal, the QoS is provided by means of the strategy and actions taken by some of the E3MS subsystems: The CAC, the DRA and the BMS. The first one controls the admission of new calls only when resources are available (taking into account not only bandwidth but also delay, jitter and losses), the second one manages the resource allocation and set up parameters in the devices, and the third one reorganize the resources on an specific link or even along the whole network.

This paper is organized as follows: In the next section, we define the main concepts and goals. Next, the system architecture is presented. Section IV, V and VI introduces its main components: GUI, NMS and NEM. Section VII describes the strategy for admission control, and section VIII the so called Background Monitoring System. Next section summarizes a set of new strategies also included in the

testbed. Section X describes some selected trials done to validate the functionalities, and finally the paper concludes with the most important conclusions and some future works.

II. Definitions, goals and approach

The global scope of this work is to demonstrate the practical usefulness of the mechanisms of autoprovisioning in the future Internet, based on classification of IP traffic in classes of service from the DiffServ architecture and MPLS networks, creating a management and configuration system to make IP/MPLS-TE networks useful for operators in order to support the end to end QoS requirements that incoming UMTS services demand. The requirements put on the solution to be developed are:

- Configure the network from a central point in a friendly way, reducing the configuration time.
- The stability in the network configuration.
- Automate the reconfiguration of IP networks depending on the real traffic.
- Scalability in terms of number of routers that can be managed.
- On-line monitoring of network performance.
- Dynamic network resource allocation.
- Self-optimization of resources.
- Multi-manufacturer solution.
- Definition of different profiles for accessing the configuration and monitoring interface.

The management system provides QoS mechanisms at network elements to guarantee the SLA (Service Level Agreement). These mechanisms are:

- Traffic classification and metering: To identify and classify the traffic into different classes.
- Traffic marking: To mark the traffic, if necessary, and assign the matching DSCP value.
- Policing: To discard the traffic that doe not conform to the required policies.
- Load Balancing: To balance the load among different paths.
- Bandwidth reservation: To reserve the required bandwidth for a service class.
- Connection Admission Control: To admit or deny new traffic flows based in checking the available resources.

The system is able to make decisions itself about the optimum network configuration that must be used in each moment to obtain highest network performance.

III. System architecture and elements

The prototype Enigma3 Management System (E3MS) has been designed following a central, layered approach. Central architecture has been considered for concentrating the intelligence of the management plane in one unique entity. Nevertheless, this entity might be replicated for robustness and failure-proofing of the whole system. Layering has been taken into account to provide flexibility and modularity to E3MS.

The gluing between different layers has been implemented using Web Services and following a Service Oriented Architecture. This SOA/WS implementation enables E3MS as an open, advanced network resource provisioning service for the clients, that is, it is neither restricted to any provider/user platform nor technology dependent.

A. Layered architecture

E3MS is composed of four layers: User Interface (UI), Network Management (NM), Network Element (NE) and Physical Network (PN).

UI layer is composed by either Graphical User Interface (GUI) or Gateway entities. GUI is a piece of software adapting from standard HTTP browsing showed to human users to SOAP/WS used by NM layer. GUI also allows the user to comfortably configuring access-lists, policies, tunnels and routing within the PN, remotely.

When the user of E3MS is an external communication bus supporting either HTTP browsing or SOAP/WS communication model, a Gateway entity is used to translate the incoming requests to E3MS operation requests. From a practical point of view, the Gateway is not further than a translator, because no requests can be generated within E3MS to be sent towards the external bus.

Thus, E3MS is as an advanced network service, from the external bus point of view, since it provides advanced functionalities for self-management and planning. NM layer concentrates the major intelligence of E3MS. This piece of software is in charge of serving the provisioning requests coming from the user. Moreover, it handles advanced mechanisms for managing the QoS of the different LSPs established along the PN, as it will be described in the coming sections. NM layer is composed by the Network Management System entity, acting as the controller of the whole system, that is, the head of the hierarchical architecture.

NMS uses an abstract image of the network, which is periodically updated either polling the Network Element managers at the NE layer or performing actions as a response to alarms coming from them. NE layer is composed of multiple Network Element Manager entities, each one dealing with one or more routers at the PN layer. NEM entities perform configuration and polling tasks over routers. Moreover, NEM can handle different SNMP traps sent by the router when events happen at PN layer (e.g. link failure, lost signaling, interface overload, etc.).

In general, the NE layer accomplishes three functions: First one is concerned with collecting and writing values from/to the Physical Network routers. The router configuration is done via remote CLI (Command Line Interface) execution command, as most of the MIBs provided by routers assemblers are read-only, which disables configuration via SNMP.

On second place, the router eventually sends notifications (traps) to the NEM, informing it about exceptional events within the network nodes. NEM correlates alarms in order not to overload the NMS with irrelevant notifications via the Alarm WS located at the NMS. Finally, the NEM is also responsible for monitoring the network to guarantee QoS commitments, performing polling tasks via the Background Monitoring System (BMS).

The PN layer used in E3MS must support the following features:

- DiffServ capable [5].
- MPLS-TE enabled [6].

- SNMP to access to MIB objects.
- MPLS CoS Enhancements.
- Resource Reservation Protocol (RSVP).
- Terminal access agent to manage LLQ, WRED and CB-WFQ.
- Policing, shaping and metering.

B. *System interfaces*

As introduced in the previous section, E3MS has three interfaces: UI-NM, NM-NE and NE-TN and an external interface. Interface towards remote administrators (upper interface) is based on SOAP-in-HTTP and needs Graphical User Interface entity to be deployed at UI layer. Therefore, all the entities that compose E3MS are deployed in web services, providing simplicity and service flexibility. The system architecture is shown at the Fig.1.

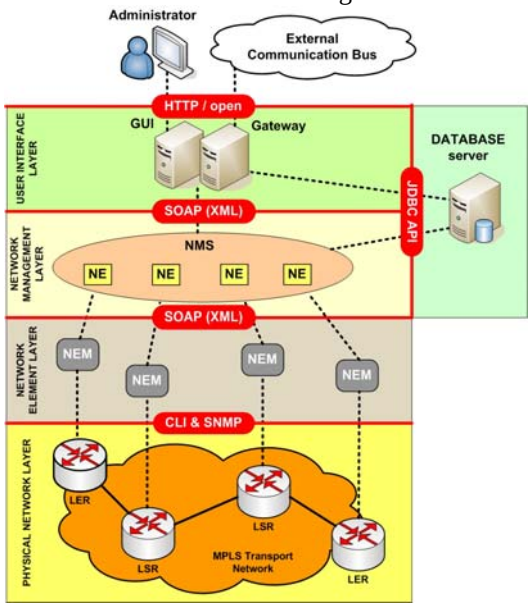


Fig. 1. MPLS-QoS management system architecture.

Interfaces between GUI-NMS and NMS-NEM are implemented using SOAP/XML, as commented before. Both are complaint with WSRF 1.2, as they are implemented with WSDL, deployed under Globus containers and using SOAP/XML. This strategy decouples in a high degree the different layers and eases their integration.

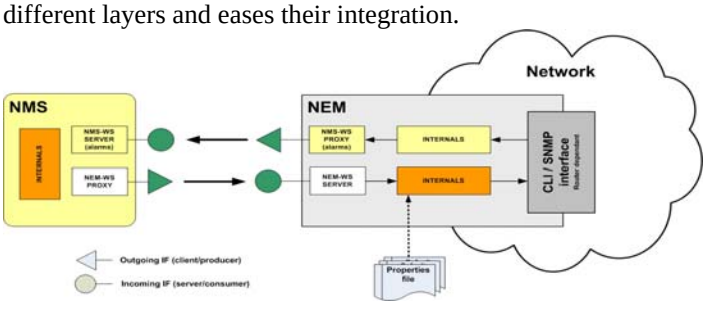


Fig. 2. NM-NE interface in detail. NEM and NMS provide services for network configuration and alarm, respectively.

NMS shows two services: The provisioning WS (NMS-WS) towards the GUI (UI-NM interface) and the alarm WS (Alarm-WS) towards the NEM (NM-NE interface). The NEM offers only one service: the router configuration service (NEM-WS). Fig.2 depicts the NM-NE interface.

Finally, the interface towards routers or network nodes considers two protocols: CLI-over-Telnet for executing remote command line operations and SNMP for either polling information or receiving alarm/events.

IV. THE GUI IMPLEMENTATION

The graphical user interface (GUI) in the Enigma E3MS system provides access to all the functionality of the NMS. It has been implemented as a web application, so network management can be done remotely and concurrently by multiple users.

A. *Technologies*

The GUI software consists of a standard web application, making use of standard open-source technologies such as:

- Apache Tomcat Server: Web application server (servlet and JSP container) [7].
- Java for implementation of classes supporting the business logic.
- JSP for presentation of dynamic web pages.
- Struts: Framework following the Model View Controler (MVC) architecture, for decoupling presentation from business logic [8].
- AJAX: Asynchronous Javascript And XML, for improving speed and usability in interactive web applications. It has been implemented using the DWR library [9].
- WebServices: for communication with the NMS, implemented with Globus Toolkit libraries.

B. *Functionality*

The network management functionality that can be accessed through the GUI includes the following:

- Node administration. Provides a way to create, modify and delete LER or LSR routers from the NMS inventory.
- Initial configuration of nodes. Allows the creation and modification of the initial configuration that is sent to the routers before any service provision is made. This initial configuration is divided in two steps:
  - Initial classes: Definition of service classes (from IPPrecedence0 to IPPrecedence5) and packet size for each one, which will be used by the initial policies.
  - Initial policies: Definition of policies applied in each interface sending MPLS traffic. For each service class, several parameters are defined such as bandwidth and queue size, and optionally RED and shaping parameters of traffic.
- Service provisioning. This is the main part, allowing the provision of services (MPLS LSP's) between any pair of LER's in the network. The available operations are creation, modification, rerouting and deletion of LSP's. In each operation the following parameters have to be introduced by the user:
  - General parameters such as LSP name, origin and destination, priorities.
  - Traffic sources, defining an access list for each class of service that will be injected into the LSP.

- Quality classes, defining the minimum quality requirements for each class of service, in terms of bandwidth, delay, jitter and packet loss.
- Routing, for choosing the LSP route calculation method, which can be explicit, OSPF or calculated by the CAC (Call Admission Control) algorithm.

- Network maps, showing a topological view of nodes and links in the network, marking the state of each element and allowing access to detail data about nodes and link occupation.
- Alarm console, for real time display of alarms generated by the NMS, related to network and service events.

Fig. 3. Main screen for service provisioning.

C. *Communication with NMS*

The GUI module is a client to the different WebServices offered from the NMS, and defined in a WSDL (WebServices Definition Language) contract. These services are accessible in a standard way from the GUI.

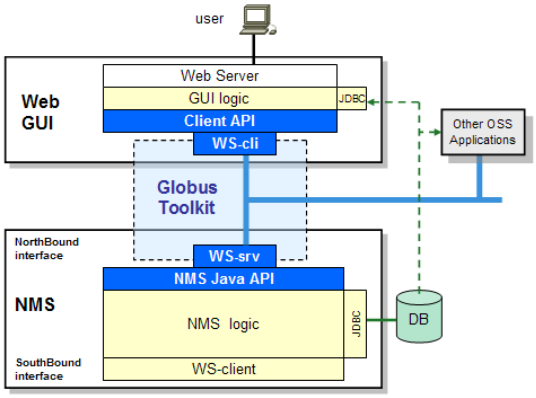


Fig. 4. Layered structure between GUI and NMS.

The client communication layer has been developed using the Globus Toolkit library, implementing the calls defined in the WSDL contract. It follows the IETF standard WS-RF (WebServices Resource Framework) for storing certain status variables between successive calls.

The implementation follows a layered architecture with clearly defined interfaces, which facilitates the independent development or even substitution of the composing parts shown in Fig.4.

V. THE NMS

The Network Management Systems (NMS) module controls the main functionalities of the system, such as admission control, route selection, auto-rerouting and per-node resources allocation.

The NMS is in between the GUI module and the set of NEM modules. Therefore, it attends the demands coming from the GUI (administrator), and manages the resources. As a result, the NMS sends configuration requests to the NEMs, and so, to the physical devices.

Alarms and management messages are also processed by the NMS, in order to provide an integrated environment. Three elements define the main features:

- The NMS includes an image of the network topology, in order to reduce the amount of requests commands to the NEMs.
- Integrates a Call Admission Control strategy (submitted to the European Patents Office) and a Background Monitoring System.
- Controls the management network (LSPs and events and/or alarms).

VI. THE NEM MODULE

The Network Element Management is the module in charge of managing the routers of the network. The Network Management System invokes configuration or performance services to the NEM in order to perform desired operations on the devices. The NEM design has been done under two objectives: The first one is the communication with NMS and with routers in order to satisfy the needed requirements. The second consists on getting a hierarchy that can facilitate the NMS invocations treatment and the required planning in order to perform all processes that have to be done.

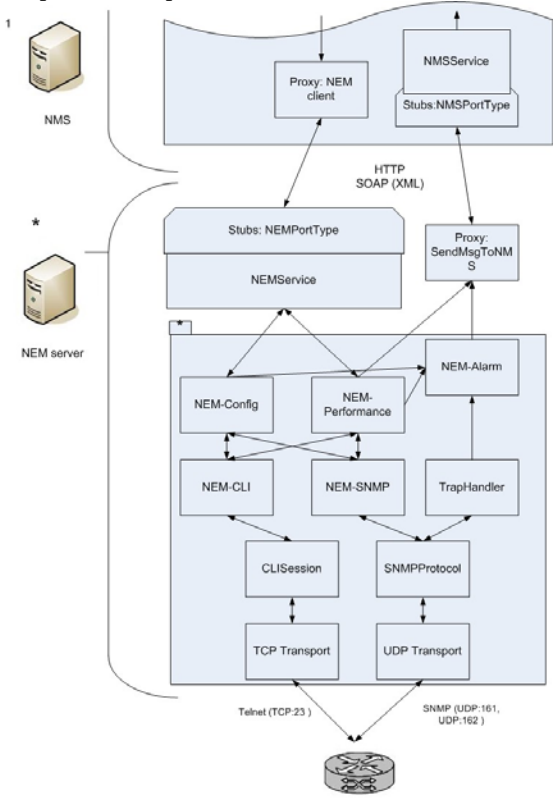


Fig. 5. NEM internal architecture overview.

In order to achieve these objectives, NEM has been designed following the class architecture shown in Fig. 5.
Messages arriving from NMS that invoke a Service of the NEM are received through a communication interface: NEMPortType, which uses stub translators implemented in Globus Toolkit 4 in order to de-serialize XML (SOAP) messages and translate them into Java operations. These operations are allocated on the main module: NEMService.

Once NMS has started, it calls the AddNEM service in order to create a new NEM instance for managing a specific router, sending into this request all parameters needed by the NEM in order to communicate later with the router. The first things that it will perform in this survey is the creation of all the objects needed in order to threat the NMS requests and also querying the router for his inventory (by SNMP) through the Configuration Module. Once the router has answered with its interfaces, then they are returned as a response for the AddNEM.

From there on, the NMS can invoke the different services defined on the NEMService and these class acts as a bridge calling the corresponding operation in the Configuration or Performance Modules and responding to the NMS once the operation has been finished.

Inside the NEM, 3 main modules have been defined:

1. The NEM-CONFIG is the responsible of orchestrate the router configuration concrete methods of the CLI module and its SNMP verifications in order to perform the complex requested operation. The main operations that this module can do are:
   - InitialClass: Configures or deletes Classes of Survey (CoS) on the router.
   - InitialPolicy: Configures one or several policy-maps in order to configure some of the previously configured CoS on corresponding router interfaces.
   - LSPRoute: Creates a new LSP on the source router of the desired Tunnel, obtaining the path by two possibilities: explicit route and implicit route. With explicit router the request has to contain all IP addresses of the nodes that conforms it. In the other hand, if it is implicit, the path is obtained by a dynamic routing protocol as OSPF.
   - Filter: With this operation, the type of traffic that has to be transported through the LSP can be defined. It configures into the router corresponding access-lists and it creates a route-map in order to redirect traffic classified by previous access-lists inside the LSP. Finally all this policy is applied to the corresponding LER interface. With this operation the traffic filtering can be created, modified or deleted. The mapping of the Survey Classes (CoS) defined into the interface with the corresponding access-list lines is done by IPPrecedence correspondence (because in the InitialPolicy a specific value has been assigned for each CoS configured in the interface).
2. The NEM-PERFORMANCE monitors different router parameters under NMS Monitoring requests and after obtaining the values from routers it is showing them and sending them, and also it can create alarms when it detects anomalies. Monitorings are based on measurements by SNMP requests but sometimes CLI commands are needed and they have to be parsed. After requested values have been obtained, they are stored or will be used in order to perform some calc. After Notification Time a set of calculated values in that Time Interval are sent to the NMS by a provideStatistics (service allocated into NMSPortType). The SendMsgToNMS module is needed in order to call that service. For each start Monitoring request, a scheduling process is created and it is executed every Monitoring Time, querying the needed values and storing corresponding results. There are the following types of Monitoring: LSP Traffic Rate, Interface Traffic Rate, Queue Delay, Jitter, Delay, Packet Losses, CPU usage and Bandwidth Utilization for Class inside LSP. The last type is the one used by the BMS Module of the NMS. It checks if BW configured for the different classes inside an LSP aren't infra-used or over-used. Thus, this module sends alarms to the Alarm module in case of one of these situations. The values obtained on each measurement execution are used for calculating a mean that will be used for the comparison with the configured BW in order to know if they are over or under the BW thresholds. If this situation occurs, then a message is queued into NEM-ALARM module that it will invoke the trapNotification Service of the NMS in order to communicate that situation.
3. The NEM-ALARM is the responsible of capturing and organizing the alarms that arrive from the router or also from NEM-PERFORMANCE and sent them to the NMS by the NMSPortType services invocation, using the SendMsgToNMS module.

In order to communicate with devices modules for configuration, query and monitor functionalities are needed, and also for retrieving alarms from them. In order to get it, the NEM supports different protocols: CLI and SNMP. CLI needs to use TCP as transport protocol and in order to configure devices by this way a TELNET session has to be opened. Current CLI interface communication is particular for Cisco's routers and CLI commands can be a little different with other vendors, but design and implementation have been done with modularity in order to be easily adaptable to other devices or vendors.

On the other hand, SNMP uses UDP as transport protocol. SNMP is used for monitoring routers and to do verifications for the configurations (sending messages through port 161) and also in order to receive alarms from the devices by TrapHandler module, that listens on port 162. To ensure that no process interferes other process operation (i.e. performing BMS operations when configuration operation is being done), a Mutual Exclusion System by occupation semaphores has had to be implemented. With them, two processes that send CLI commands to the same router can be executed at the same time and their respective responses from the router will not be mixed.

While the NEM application is being executed, many errors can be taken. So that, an error control system has been implemented in order to detect these situations and to solve them or to return a remote exception to the NMS with the error code and description.

In order to monitor the NEM execution while it is making configurations, an event logging system with several levels has been implemented using Apache Log4j.

There are a set of constants stored into a property file (XML format). The design of every part of the code can depend of the function of these constants when NEM application is executed.

VII. PER CLASS ADMISSION CONTROL

The E3MS controls the admission of new connections taking into account a specialized new CAC (Call Admission Control) strategy. This module, considers a set of classes. A new incoming call can be allocated in the own class of service, dropping a low priority connection, or even using resources of an upper class (when this resources are still unused). This last strategy is call squattering. The CAC algorithm takes decisions affecting to the routing. This can be on-line (when routing decisions are taken on the fly, according to the available information for the establishment of a path, without any additional optimization mechanism) or off-line (when a global research in the network is considered).

The general strategy proposed in this work and implemented is: For each LSP, each class is checked:

- First checks the available BW (bandwidth) for each class.
- If not available enough BW, try to establish as a squatter (in the upper class).
- If not available enough BW, try to provide BW by dropping lower priority LSPs.

The available routes considered (from a node A to a destination B) are:

1. The explicit route: the one provided – suggested - by the user. This is optional.
2. The route provided by the OSPF-TE protocol.
3. Rest of available routes: The set of routes can be build by means of an off-line research. Several protocols can be considered for this, such as Dijkstra. The result of this is a set of Potential Routes. Every route is considered potential route, because it still should be checked according to the QoS parameters demanded.

In order to allocate new connections, a Dynamic resource allocation (DRA) module can alter the per-class configuration of each node. This module is commented in the section IX.

VIII. THE BMS

The background monitoring system (BMS) is a specific module placed in the network management system (NMS) (see Fig.6). This module is responsible for listening the different notifications sent by the network element management (NEM) and, based on the information sent in every notification, apply some changes on the network when necessary. These notifications are state and error messages from the different routers of the MPLS network.

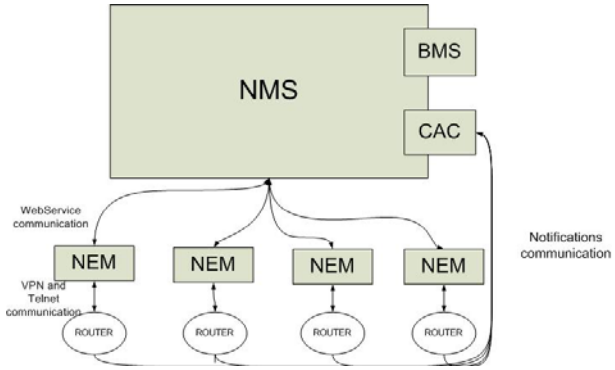


Fig. 6. Software modules involved in the BMS operation.

Actually, the two messages that trigger BMS working are the notifications about infra utilization and over utilization of bandwidth for a specific LSP. These two messages are sent when a LSP has reserved some bandwidth (say X Mbps) and the user specifies he wants to monitor this LSP. He specifies a maximum and minimum threshold percentage. If the router detects that the data traffic flow is under or over the specified percentage of the X Mbps reserved by the user, it sends a message of under or over utilization to the NEM and the NEM forwards this message also to the BMS.

First of all, the BMS checks if this message is the 5th message or more in order to permit the NEM to have a real value (the first 5 measurements normally are peaks values, not the medium value that it is the one that the BMS needs to perform real changes). The BMS then processes the information and tries to check if any change has to be applied on the network: the BMS set up this new bandwidth use measurement and convert this measurement into the next upper 8 multiple value (always upper because the goal is to permit this data flow). Once it has the next upper 8 multiple value (the routers in the testbed only supports reservations of 8 multiple values), it compares with the value reserved. If the value is different than the reserved by the user, the BMS tries to apply some changes on the network.

In the case of under utilization, a change is always applied because the action to be done is freeing resources and this is always possible to do. In the case of over utilization another module is needed to check if the changes can be applied, the CAC (this module checks if enough resources are in the network to apply the changes that the user/BMS wants to apply). BMS asks the CAC if the changes needed for this new measurement are possible and, if it is possible, BMS starts to apply the changes. The way to apply the changes is the same for the two cases, infra and over utilization: First of all the BMS updates the data base. Afterwards it sends a message to the NEM to stop the monitoring of this LSP in order to permit changing the original bandwidth reservation (the routers need to stop the monitoring to change a bandwidth reservation). Then, it sends another message to the NEM to modify the original reserved bandwidth with the new 8 multiple value. Finally, the BMS sends the last message to the NEM to perform the changes, the start monitoring for this LSP.

Consequently, there is a problem: If the BMS changes the state of the network, it is necessary to modify the network in mutual exclusion because if the BMS is changing the network status at the same time as a user request, both of them are changing a network that it is not consistent. For example, BMS changes the network status at the same time that the user asks the CAC to check if a LSP creation can be done. The CAC checks this creation in a network status that will be changed during the LSP creation, consequently this LSP is not going to be created in the network status the CAC thought that the network was. The solution is using a semaphore (see Fig.7) to access to the network state. When a user requests, for example, the creation of a new LSP, the NMS has to check if the BMS is changing at this time the network status (the routers configuration and also the data base). If the BMS is working on the network, the NMS has to wait to perform the LSP creation. Once the BMS has finished, the NMS can proceed by changing or consulting the network status depending on the user request.

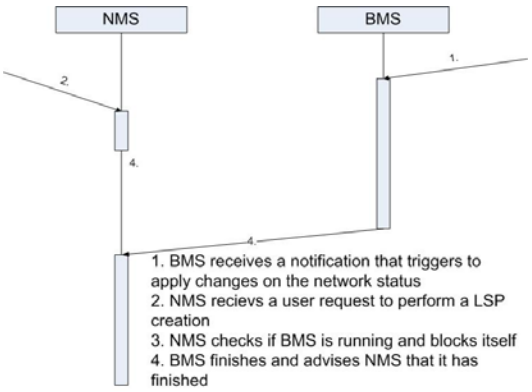


Fig. 7. NMS-BMS semaphore operation example.

While BMS is working, it blocks the rest of the NMS functions that can change/consult the network status.

IX. Other functionalities

The E3MS implements other functionalities, in order to support per-node resources administration, taking into account classes of services: DRA, Marking, Load Balancing, Legalization and Off-line monitoring.

An enhancement of the nodes utilization can be applied by means of a specific control of per-class allocated bandwidth and queue sizes. This is made by means of the Dynamic Resource Allocation (DRA) module. This module can tune detailed performance parameters, such as per class queue length and schedulers in every node (router), according to the functionalities of every vendor. The NEM module translates the command according to acceptable messages in the device. Bandwidth and size of the queues created in output interfaces for each class should be changeable automatically by the CAC.

The Marking Module marks the routes that are showed in the compliant routes table from the most recommended to the least one. The criteria can be changed according to the administrator needs. In our testbed, we have considered a weighted formula, balancing the hop count, delay and remaining per-link bandwidth.

Besides, a Load Balancing strategy is implemented. This feature permits an enhancement in the network usage. Because the NMS have the knowledge about global network utilization, routing decisions are taken according to load balancing parameters, not only shortest path as in traditional networks such as internet using OSPF.

When some amount of BW is free in a queue (LSP deletion, rerouting, modification) it should be possible to legalize old squatter LSP. This mechanism is called legalization and is implemented in a Legalization module.

The Off-line Monitoring Module checks the status of the network in real time, monitoring statistics and looking for new and better network configurations. Some recommendations can be provided to the administrator by means of the GUI interface.

X. Samples of trials and validation

E3MS has been deeply validated over a testbed supporting multi-technology on the physical layer (from E1 radio links to WDM, also including Fast/Gigabit Ethernet). The testbed is composed of Cisco IP routing equipment from series 2800, 3600 and 3800. All routing devices are MPLS-TE capable.

For the tests shown in this paper, let be:

- LSP_name: name of an LSP.
- IPPi: IP traffic class. In the testing performed, an LSP carried traffic of several classes (IPP0-IPP2), being IPP2 the one with highest priority and IPP0 the less one.
- Route: sequence of routers crossed by an LSP. It is an array of output interfaces of each router involved in the path.
- QoS_bw_i: bandwidth demanded by each class carried by the LSP.

Moreover, for each class "IPPi" defined at an interface must be considered:

- Bw_original_i: portion of the bandwidth in a link which is reserved for class i. This allocation is not static, so it can change depending on the demanded bandwidth for any incoming LSP (DRA).
- Bw_used_i: aggregated bandwidth used for each class (by all LSPs). A distinction must done:
  - by a legal LSP: bandwidth used by the own class.
  - by a squatter LSP: bandwidth is used by another class j (and we say that class j is squattering class i
- Available_bw_i: bandwidth computed as Bw_original_i minus Bw_used_i.

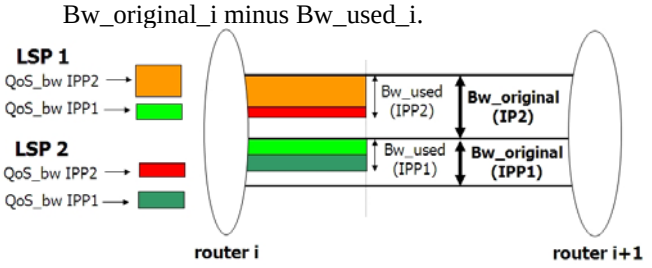


Fig. 8. A set of bandwidth specifications within E3MS.

A. *Test 1. Squatter allocation and squatter LSP dropping*

This test shows that, when there are not enough spare resources (in this case, bandwidth) in current class, E3MS can get bandwidth from another class. That is to say, if the desired bandwidth to be allocated is higher that the remainder from the original reserved for the class (remainder is equal to reserved minus currently allocated/in use), E3MS will logically establish the new LSP as a squatter LSP using part of the bandwidth reserved for another class. E3MS always tries to use the remainder resources in the legal class and add the necessary resources to establish the LSP by getting them from the spare ones in another class.

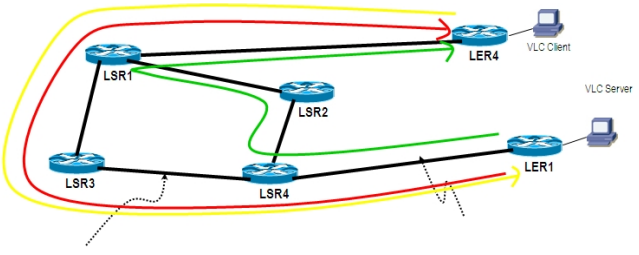


Fig. 9. Test 1 scenario.

Class	From LSR4 to LSR3			
	Original	Used		Available
		Legal	Squatt.	
Ipp2	800	0	0	800
Ipp1	800	480	0	320
Ipp0	200	16	0	194
Class	**From LER1 to LSR4**			
	Original	Used		Available
		Legal	Squatt.	
Ipp2	800	0	168	632
Ipp1	800	800	0	0
Ipp0	200	16	0	194

Table 1. Bandwidth allocation (kbps) in Fig.9 for Test 1.

The specifications and performance of this test are:

1. Tunnel41: 2 classes of traffic (IPP1 with 520 Kbps, IPP0 with 16Kbps) from LER1 to LER4. Route: LER1-LSR4-LSR2-LER1-LER4.
2. Tunnel42: 1 class of traffic (IPP1 with 448 Kbps) from LER1 to LER4. Route: LER1-LSR4-LSR3-LSR1-LER4. So IPP1 will be squattering IPP2 at output interface of LER1 and LSR1, as:
   a. it will get the 280 kbps available from IPP1 → so at output interface of LER1 and LSR1, Bw_used_1 (all legal) is 800 Kbps.
   b. it will get 168 Kbps from IPP2 → so at output interface of LER1 and LSR1, Bw_used_2 (all squatter) is 168 Kbps.
3. Tunnel14: 1 class of traffic (IPP1 with 96 Kbps) from LER4 to LER1. Route LER4-LSR1-LSR3-LSR4-LER1.
4. Video is transmitted correctly through tunnel42 despite of tunnel42 has not enough resources for IPP1 at output interface of LER1.

B. Test 2. Squatter allocation and squatter LSP dropping

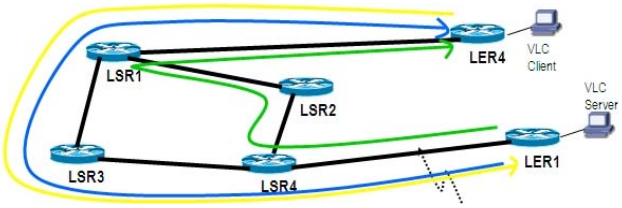


Fig. 10. Test 2 scenario.

Class	From LER1 to LSR4			
	Original	Used		Available
		Legal	Squatt.	
Ipp2	800	696	0	104
Ipp1	800	520	0	280
Ipp0	200	16	0	194

Table 2. Bandwidth allocation (kbps) in Fig.10 for Test 2.

The specifications and performance of this test are:

Tunnel43: 1 class of traffic (IPP2 with 696 Kbps) from LER1 to LER4. Route: LER1-LSR4-LSR3-LSR1-LER4, so squatter LSP2 will be dropped (as it is squattering IPP2 at output interface of LER1 and LSR1). So at output interface of LER1 and LSR1:

a. Bw_used_2 is 696 Kbps (all legal).
b. Bw_used_1 is 520 Kbps (all legal).
c. Bw_used_0 is 16 Kbps (all legal).

A lot of other validation tests have been successfully done, but they are not included in this paper.

XI. Conclusions

In this paper, the E3MS system has been introduced, described and analyzed. This system enables the operators to provide an end to end QoS auto-provisioning across an MPLS-Diffserv transport network, as a solution to support the new services requirements demanded by the Mobile Operators. It integrates a connection admission control and routing algorithms within the Network Management System in an innovative way to optimize the network resource allocation depending on the real traffic distribution and network performance. It also provides an intuitive interface to manage and configure the network, catching alarms and monitoring the traffic and the network performance.

The system design is modular, so new modules or components can be easily added to the system to provide other features in the future.

The results coming from project open a lot of further works to be done: Mainly, an analytical study to show the performance, scalability and the reliability of the system working on real scenarios. Also, the numerous variable values that have been introduced in the control algorithms must be tuned in order to work optimally in different real scenarios. We also consider the extension to routers from other vendors, such as Juniper Networks.

Acknowledgements

This work has been partially supported by the national spanish Project CICYT TSI2007-66637-C02 and the Enigma3 project from i2CAT foundation and Vodafone.

References

[1] 3GPP.TS23.107V6 UMTS; QoS Concepts and Architecture, TS23.107V6, March 2004.
[2] 3GPP.TS29.207V6 UMTS; QoS Concepts and Architecture, TS29.207V6, September 2004.
[3] S.Blake et.al. "An Architecture for Differentiated Services", RFC 2475, Dec. 1998.
[4] E.Rosen, A.Viswanathan and R.Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001
[5] F. Le Faucheur, "Requirements for Support of Differentiated Services-Aware MPLS Traffic Engineering", RFC 3564, June 2003.
[6] I.Minei, "MPLS DiffServ-Aware Traffic Engineering", Juniper, Published 2004, Posted March 30, 2005.
[7] http://tomcat.apache.org/
[8] http://struts.apache.org/
[9] http://directwebremoting.org/dwr

Detección Distribuida de la Conectividad en Redes Ad-hoc de Comunicaciones Vehiculares

Michele Rondinone y Javier Gozálvez
Ubiquituos Wireless Communications Research Laboratory
Uwicore, http://www.uwicore.umh.es
Universidad Miguel Hernández de Elche
Avenida de la Universidad, s/n 03202 Elche
mrondinone@umh.es, j.gozalvez@umh.es

***Resumen*- Estudios recientes han demostrado que las prestaciones de los protocolos de enrutamiento en redes vehiculares pueden mejorarse mediante la utilización de información dinámica sobre las condiciones de tráfico. Dicha información puede emplearse para seleccionar los caminos de enrutamiento o nodos retransmisores más apropiados. Sin embargo, la mayoría de las técnicas de estimación de las condiciones de tráfico causan una importante sobrecarga en el canal radio lo cual puede comprometer su futura viabilidad. En este contexto, este artículo introduce y evalúa DiRCoD, una novedosa técnica para estimar la conectividad *multi-hop* de segmentos de carretera que permite obtener la capacidad de estos segmentos para enrutar de manera fiable paquetes de datos. Como se demostrará en el artículo, esta técnica es capaz de proporcionar información de conectividad con gran periodicidad, sin incurrir en un elevado incremento de la sobrecarga de señalización y con un bajo coste de implementación.**

I. INTRODUCCIÓN

Las redes vehiculares cooperativas son actualmente objeto de estudio en numerosos trabajos de investigación que proponen novedosos servicios y aplicaciones ITS (*Intelligent Transportation Systems*) con el objetivo de proporcionar una mayor seguridad y eficiencia vial. Para ello, se han planteado sistemas cooperativos que permiten a los vehículos comunicarse directamente entre sí (comunicaciones *Vehicle-to-Vehicle* o V2V), o con elementos de infraestructura (comunicaciones *Vehicle-to-infrastructure*). A través del intercambio de información dinámico y cooperativo entre vehículos, los conductores obtienen una información sobre el estado de la carretera y, más en general, del tráfico de forma anticipada y más allá de su campo visual. Además, los sistemas vehiculares cooperativos permiten el establecimiento de redes ad-hoc vehiculares (*Vehicular Ad-hoc Networks* o VANETs) que permiten el intercambio de datos entre vehículos, aunque no se encuentren dentro de su rango de comunicación. Para ello, se establecen comunicaciones *multi-hop* entre origen y destino empleando las retransmisiones de nodos intermedios que pueden ser vehículos o estaciones base fijas de apoyo llamadas *roadside units*. Un ejemplo de utilización de VANETs podría ser la notificación de un atasco a vehículos que se estén acercando al área congestionada, de forma que puedan modificar sus rutas. La eficiencia de las comunicaciones *multi-hop* para VANETs puede verse notablemente afectada por el diseño de los protocolos de enrutamiento empleados para permitir el encaminamiento de la información de forma correcta desde el nodo fuente al nodo destino mediante una adecuada selección de nodos retransmisores. El diseño de estos protocolos es significativamente complejo debido a la alta movilidad de los nodos vehiculares, y a las difíciles condiciones de propagación del medio inalámbrico. Estas condiciones se complican aún más en el caso de las comunicaciones V2V, donde la altura de las antenas transmisora y receptora es reducida, y en entornos urbanos, donde la presencia de obstáculos dificulta la propagación de la señal radio.

La mayoría de los protocolos de enrutamiento presentados en la literatura [1-10] utiliza la posición geográfica de los nodos para seleccionar los retransmisores. Entre estos protocolos, es importante destacar aquellos que seleccionan caminos de enrutamiento basándose en las condiciones actuales del tráfico en las carreteras teniendo en cuenta para ello la presencia potencial de nodos retransmisores. Los trabajos planteados anteriormente en la literatura para estimar estas condiciones de tráfico conllevan normalmente una alta sobrecarga de comunicaciones. En este contexto, este artículo presenta DiRCoD (*Distributed and Real Time Communications Road Connectivity Discovery mechanism*), un mecanismo distribuido que permite detectar la conectividad de las carreteras en tiempo real. Este mecanismo ha sido diseñado para mejorar el rendimiento de los protocolos de enrutamiento en redes vehiculares a través de la estimación dinámica de la capacidad de los segmentos de carretera para soportar retransmisiones *multi-hop* fiables. Como se mostrará, DiRCoD es capaz de estimar esta capacidad con una baja sobrecarga de comunicaciones y con un coste de implementación mínimo gracias al empleo de mensajes *broadcast* denominados *beacons*, los cuales han sido introducidos en los estándares de comunicaciones cooperativas vehiculares.

II. ESTADO DEL ARTE

Con el objetivo de mitigar la inestabilidad de las comunicaciones inalámbricas *multi-hop* en entornos

vehiculares, se han propuesto protocolos de enrutamiento que utilizan la posición geográfica de los nodos para seleccionar de manera dinámica el próximo nodo retransmisor. Por ejemplo, los protocolos GPSR (*Greedy Perimeter stateless Routing*) [1] y CBF (*Contention-Based Forwarding*) [2] adoptan el esquema denominado "*greedy forwarding*", el cual selecciona como retransmisores los nodos que se encuentran más cerca del nodo o área de destino. Sin embargo, las técnicas de enrutamiento *greedy forwarding* pueden presentar el problema del "máximo local". El máximo local hace referencia a la situación en la que un paquete de datos que está siendo enrutado mediante *greedy forwarding* alcanza un nodo que no tiene vecinos más cerca del destino que él mismo. En este caso, dado que el retransmisor actual (o máximo local) es el nodo más cercano al destino, no puede continuar retransmitiendo el paquete. Cuando se presenta esta situación, el paquete de datos se descarta, salvo que se empleen técnicas para seleccionar rutas alternativas hacia el destino. Por otra parte, distintos trabajos han demostrado que la presencia de edificios en entornos urbanos puede afectar significativamente al funcionamiento de estos protocolos, al ocultar el mejor nodo retransmisor o al establecer múltiples rutas hacia el destino de manera ineficiente [3]. Algunos protocolos tales como Spatially Aware Routing (SAR) [4] o Geographic Source Routing (GSR) [5] emplean mapas digitales para intentar resolver los problemas mencionados anteriormente, enrutando los paquetes mediante *greedy forwarding*, pero usando caminos geográficos fijos que conectan el nodo fuente al destino a través un determinado número de intersecciones. La selección de estos caminos está basada en información estática de la red de carreteras (por ejemplo el camino más corto entre fuente y destino), o en datos estadísticos que no son continuamente actualizados. Por consiguiente, el camino seleccionado podría no ofrecer una adecuada conectividad de comunicaciones *multi-hop* que asegure la entrega de los paquetes desde la fuente al destino. Para superar algunas de estas limitaciones, recientemente han sido propuestos protocolos como VADD (*Vehicle-Assisted Data Delivery*) [6] y TBD (*Trajectory-Based Data forwarding*) [7]. Estos protocolos seleccionan dinámicamente en cada intersección la ruta por la que encaminar los paquetes basándose en estadísticas de tráfico a largo plazo como por ejemplo el número medio de vehículos que circulan por una cierta calle. Aunque estos mecanismos puedan resultar en rutas *multi-hop* estables en término medio, no son capaces de proporcionar instantáneamente caminos de enrutamiento que aseguren conectividad *multi-hop* en un momento dado.

Nuevas propuestas tales como LOUVRE (*Landmark Overlays for Urban Vehicular Routing Environments*) [8] y RBVT (*Road-Based using Vehicular Traffic Routing*) [9] tienen como objetivo seleccionar caminos de enrutamiento que garanticen la conectividad entre los nodos, empleando para ello estimaciones de tráfico como por ejemplo la densidad de vehículos en una calle. Ambos enfoques pueden ser considerados como protocolos proactivos de enrutamiento basados en la posición donde los nodos se intercambian periódicamente mensajes para disponer de un mapa de conectividad de la red de carreteras. Cuando se desea enrutar un paquete, esta información es utilizada por los vehículos para calcular el camino más conveniente que asegure la conectividad de extremo a extremo y entregar de forma fiable los paquetes. Se ha demostrado que este tipo de protocolos obtiene buenas prestaciones en términos de ratio de paquetes entregados. Sin embargo, a fin de obtener un conocimiento actualizado en todo momento de la conectividad de la red de carreteras, estos protocolos incurren en una considerable sobrecarga de comunicaciones, debido al intercambio periódico de mensajes entre vehículos.

GyTAR (*Improved Greedy Traffic Aware Routing protocol*) [10] es otro protocolo de enrutamiento para redes vehiculares basado en un enfoque distinto al ofrecido por los mecanismos anteriores. Este protocolo computa de manera dinámica en cada intersección el camino de enrutamiento basándose en evaluaciones de la densidad de tráfico en tiempo real. Cada vez que un paquete llega a una intersección, GyTAR lo encamina (entre todas las rutas que parten de esta intersección) hacia la calle que más se acerca al destino y cuya densidad de tráfico estimada sea la más alta; a mayor densidad de tráfico, mayor será la probabilidad de que exista conectividad *multi-hop* de extremo a extremo. Para calcular la densidad de una calle y hacer llegar esta información a las intersecciones, se utiliza un algoritmo llamado IFTIS (*Infrastructure-Free Traffic Information System*) [11]. IFTIS es una técnica totalmente distribuida de estimación de la conectividad *multi-hop* en segmentos de carreteras que calcula dinámicamente la densidad de tráfico. Sin embargo, como será demostrado en la sección IV, IFTIS introduce una sobrecarga de señalización relativamente alta, que se compensa con una menor frecuencia de actualización de la información de tráfico. Aunque esta capacidad de compensación es muy interesante para controlar la sobrecarga, el resultado final puede afectar de alguna manera la capacidad de IFTIS de proporcionar información actualizada a protocolos de enrutamientos para VANETs que se basen en estos datos.

Con el fin de reducir la sobrecarga de comunicación y al mismo tiempo proporcionar información de conectividad *multi-hop* actualizada a los protocolos de enrutamiento, este artículo presenta la técnica DiRCoD. DiRCoD ha sido diseñado para asistir a los protocolos de enrutamiento en la selección del siguiente segmento de carretera por el que retransmitir los paquetes de datos, mediante la estimación directa de su conectividad *multi-hop*. En este contexto, existe conectividad en un segmento si existe un conjunto de vehículos que ofrezca la capacidad de retransmitir paquetes de un extremo a otro utilizando comunicaciones *multi-hop*. Como será explicado en las próximas secciones, el protocolo propuesto estima directamente la conectividad *multi-hop* de una calle generando una menor sobrecarga en comparación con los métodos que la evalúan calculando la densidad de tráfico. Además, esta estimación puede emplearse para evitar que los protocolos de enrutamiento escojan repetidamente las calles más densas para enrutar paquetes, lo cual aumenta la congestión en el canal de comunicaciones en estas calles. El diseño de protocolos de enrutamiento basados en la estimación directa de la conectividad *multi-hop* mejoraría la distribución espacial y el balanceo de la carga de comunicaciones. De hecho, estos protocolos permitirían el enrutamiento de paquetes por calles que ofrezcan conectividad *multi-hop*, aunque estas no presenten las densidades de tráfico más elevadas.

III. DIRCOD

A. Principio de funcionamiento

Como ha sido explicado, DiRCoD ha sido diseñado para proporcionar información sobre la conectividad *multi-hop* de segmentos de carreteras con el fin de asistir a los protocolos de enrutamiento en VANETs en la selección dinámica de los próximos caminos de enrutamiento. Para describir el mecanismo de DiRCoD, este trabajo considera segmentos de carreteras delimitados por dos intersecciones como muestra la Figura 1. Supongamos que un vehículo en la intersección Is tenga que transmitir un mensaje hacia un área geográfica X. A diferencia de los protocolos que determinan los caminos de enrutamiento de origen a destino sin considerar las condiciones dinámicas de trafico o de conectividad, este trabajo se centra en esquemas que, como GyTAR, intentan seleccionar las calles que asegurarían la probabilidad más alta de retransmitir los paquetes de extremo a extremo, estimando esta probabilidad en términos de conectividad *multi-hop*. Considerando el ejemplo ilustrado en Figura 1, cuando un paquete fuente alcanza la intersección I1, el nodo receptor debería instantáneamente decidir si enrutar el paquete hacia I2, I3 o I4. Para contribuir a la decisión de enrutamiento, DiRCoD proporciona una medida de la conectividad *multi-hop,* es decir de la disponibilidad de vehículos capaces de retransmitir el paquete por medio de transmisiones *multi-hop* de I1 a Ix para cada uno de los tres posibles caminos (I1-I2, I1-I3, y I1-I4). Una innovación clave de DiRCoD es que este mecanismo utiliza el mensaje *broadcast* llamado *beacon* o *Connectivity Awareness Message* (CAM) para estimar la conectividad *multi-hop* de cada segmento de carretera. Es importante clarificar que DiRCoD ha sido diseñado considerando las actuales convenciones europeas que armonizan la arquitectura de comunicaciones ITS [12]. Estas convenciones establecen que los mensajes CAM se transmitan en el canal de control (*Control Channel* o CCH) y que las comunicaciones *multi-hop* se transmitan en el primer canal de servicio (*Service Channel 1* o SCH1)[1]. Para estimar la conectividad *multi-hop* de una calle, DiRCoD la divide en varias secciones con una longitud igual al rango de comunicación de los vehículos en el SCH1[2]. El mecanismo define también la distancia virtual de una cierta intersección Ix como el número de secciones de la calle, o saltos (*hops)*, que separan el vehículo más cercano de Ix. El ejemplo de la Figura 2a) representa una calle con conectividad *multi-hop* completa dado que hay suficientes vehículos para retransmitir paquetes de un extremo (I1) a otro (I2). En este caso, la distancia virtual es igual a 0 saltos. Al contrario, la Figura 2b) representa una calle con conectividad *multi-hop* parcial y una distancia virtual de 2 saltos.

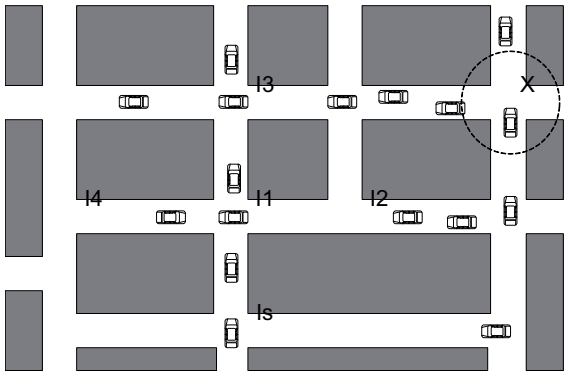


Figura 1. Escenario de aplicación de protocolos de enrutamiento *multi-hop* en VANETs.

Para estimar la conectividad *multi-hop* o la distancia virtual de una intersección dada, DiRCoD introduce un campo de conectividad (o *connectivity field*) que es agregado a los CAMs transmitidos por los vehículos. El *connectivity field* inicialmente indica la sección de la calle en que el vehículo se encuentra en el momento de la transmisión del CAM. Sin embargo, si un vehículo es consciente de la presencia de otros vehículos más cercanos que él a la intersección destino (I2) o situados en la intersección misma, el *connectivity field* indicará aquellas secciones o la intersección destino. Considerando el ejemplo de la Figura 2a), el vehículo F, en vez de agregar un '1' (su sección actual), agregará a su CAM un *conectivity field* igual a '0', ya que detecta la presencia de un vehículo en I2. De forma parecida, el vehículo B, pondría en principio un *connectivity field* igual a '2', pues está a dos saltos de I2. Sin embargo, al recibir desde F un CAM que incluye un *connectivity field* igual a '0', agregará este mismo valor en el *connectivity field* de su CAM. A través de un procedimiento de propagación secuencial (ver sección III.B), los vehículos que entran en la intersección I1 recibirían desde el vehículo D un mensaje CAM con un *connectivity field* igual a '0', y por lo tanto serían informados de que la calle ofrece una conectividad *multi-hop* completa desde I1 hasta I2. Al contrario, los vehículos que entran en I1 en el ejemplo de la Figura 2b) recibirían del vehículo D un mensaje CAM con un *connectivity field* igual a '2', lo cual indicaría que esta calle sólo ofrece conectividad parcial: cuanto más alto sea el valor indicado en el *connectivity field* del CAM, menor será la conectividad *multi-hop* de la calle.

[1] Los mensajes CAM son utilizados por los vehículos para notificar periódicamente su presencia a los vecinos más cercanos.

[2] Diferentes rangos de comunicaciones pueden ser supuestos en el CCH y en los SCHs. En particular, la utilización de diferentes rangos de comunicaciones y el diseño de otras políticas de control de congestión del canal radio para el CCH es un área de investigación abierta. Esto es debido a la naturaleza de este canal, caracterizada por niveles altos de carga de comunicaciones. Al contrario, un rango de comunicaciones más alto puede ser supuesto para el SCH1, que sería el canal inicialmente utilizado para trasmisiones *multi-hop*. Es importante destacar que, aunque la implementación actual de DiRCoD se basa en configuraciones estándar actuales, el mecanismo podría ser fácilmente modificado y adaptado a configuraciones diferentes.

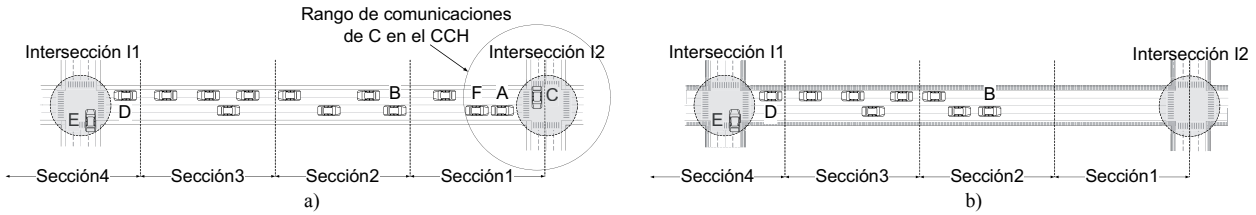


Figura 2. Segmento de carretera con conectividad *multi-hop* total (a), y con conectividad *multi-hop* parcial (b).

B. *Aspectos de implementación*

Para asegurar la escalabilidad de DiRCoD, varios aspectos de implementación tienen que ser considerados. En primer lugar, es importante limitar y controlar la generación de los *connectivity fields* por parte de los vehículos en las secciones de la calle. Para explicar cómo, se considera el escenario representado en la Figura 2a), donde el vehículo E, al entrar en la intersección I1, necesita una estimación de la conectividad *multi-hop* de la calle I1-I2, a fin de decidir si enrutar los paquetes que recibe por esta calle o por otras. La zona de intersección se define como un círculo cuyo centro coincide con el de la intersección y con un radio bastante pequeño para que los vehículos en su interior estén en condiciones de visibilidad radio directa con todas las calles que salen de la intersección. Sólo a los vehículos en la parte interior de la calle, excluyendo las dos intersecciones, se les permite generar un *connectivity field*. Antes de hacer el *broadcast* de un mensaje CAM normal, cada vehículo controla en su tabla de vecinos si aparecen nodos que estén más cerca que él a la intersección I2. Si no se encuentra ningún vehículo con estas características, se agrega al mensaje CAM un *connectivity field* que indica la sección de la calle donde el vehículo está actualmente. Este es el caso del vehículo B en la Figura 2b). Al contrario, si por lo menos un vehículo más cercano a I2 se encuentra en la tabla de vecinos, ningún *connectivity field* será agregado. Esto se debe a que el vehículo detecta que la generación de una información de conectividad según el mecanismo de DiRCoD se realiza en vehículos que están mas cerca de la intersección I2 que él mismo, y por lo tanto solo debe esperar recibirla y retransmitirla hacía I1. El *connectivity field* es también generado y agregado a mensajes CAM por los vehículos que reciben un CAM desde nodos ubicados en la intersección I2. En este caso el *connectivity field* es igual a '0', ya que la intersección I2 puede ser alcanzada por medio de comunicaciones *multi-hop*. En algunos casos, puede pasar que nodos vecinos quieran generar un *connectivity field* con la misma información en el mismo instante. Una situación de este tipo es mostrada en la Figura 2a) donde los vehículos F y A reciben ambos un mensaje CAM desde el vehículo C ubicado en I2. Esto debería evitarse porque resultaría en información redundante que podría comprometer la escalabilidad de DiRCoD. Con este propósito, cada vehículo, al recibir un *connectivity field* (o un mensaje CAM normal desde un vehículo ubicado en I2), activa un temporizador cuya duración es proporcional a su distancia a la intersección I1 (cuanto más pequeña sea esta distancia, más breve es el temporizador). El vehículo cuyo temporizador termina primero es el que antes transmite el CAM con el *connectivity field* añadido. El resto de vehículos que tienen el temporizador activo, al recibir de este vehículo el mensaje CAM con el *connectivity field* añadido, cancelan la inclusión del *connectivity field* en sus mensajes CAM. Otra situación que tiene que ser cuidadosamente controlada es cuando hay dos o más vehículos en la intersección I2 al mismo tiempo. En este caso, un vehículo en la Sección 1 recibiría varios mensajes CAM desde varios nodos ubicados en la intersección. Según lo explicado anteriormente, la recepción de mensajes CAM por los vehículos situados en I2 haría que los vehículos en la Sección 1 generaran un *connectivity field* y lo añadieran a su propio CAM. Sin embargo, esto implicaría la generación de información de conectividad redundante en intervalos temporales muy breves. A fin de evitar esta redundancia, DiRCoD define un segundo temporizador de x segundos. Los vehículos en la Sección 1 deben esperar hasta la conclusión de este temporizador antes de volver a generar otro *connectivity field,* en caso necesario. Si se reciben muchos mensajes CAM desde vehículos diferentes situados en I2, sólo un *connectivity field* será generado y agregado a un CAM por los vehículos ubicados en la Sección 1.

Para terminar con la descripción de DiRCoD, es importante describir el contenido del *connectivity field*. El tamaño de este campo se ha limitado a sólo un octeto (*byte*). El primer bit se utiliza para distinguir si la estimación de la conectividad se refiere a la dirección desde I1 a I2 o desde I2 a I1. Los restantes 7 bits cuantifican la distancia virtual que separa el nodo más cercano a la intersección destino (I2 en la Figura 2) en términos de saltos necesarios en el SCH1 para alcanzar esta intersección[1]. Finalmente, la identificación de la calle a la que se refiere la información de conectividad *multi-hop* no requiere bits adicionales. De hecho, esta información puede ser deducida a partir de la posición del vehículo que transmite el *connectivity field* hacia la intersección I1 (esta posición siempre está presente en los mensajes CAM) y de la utilización de mapas digitales.

IV. Evaluación de las Prestaciones

A. *IFTIS*

En este trabajo, la técnica IFTIS ha sido implementada como banco de prueba sobre el que comparar las prestaciones y la sobrecarga de DiRCoD.

En IFTIS [11], las calles son divididas en celdas uniformemente distribuidas y de radio igual al rango de comunicaciones de los vehículos. Las celdas de IFTIS son círculos situados uno a lado del otro y parcialmente superpuestos en su borde de tal manera que la distancia entre

[1] Considerando un pequeño rango de comunicaciones de 100m, 7 bits son suficientes para representar la distancia virtual en calles de hasta 12.7 km de longitud.

los centros de celdas adyacentes sea aproximadamente igual a dos veces el rango de comunicación. Siguiendo el ejemplo de la Figura 2, los vehículos que implementan IFTIS generan y transmiten un *cell density packet* (CDP) al llegar a la intersección I2. Este paquete es trasmitido después hacía I1 utilizando transmisiones sucesivas *multi-hop geounicast* de un centro de celda a otro. Concretamente, estas transmisiones sucesivas se dirigen al vehículo que esté más cerca del centro de la próxima celda en cada una de las celdas a lo largo de la calle desde I2 hasta I1. Los vehículos que reciban el paquete CDP cerca del centro de una celda, cuentan el número de sus vecinos actuales (utilizando los CAMs recibidos) y guardan este valor en el CDP antes de que el paquete sea retransmitido hacia la próxima celda. De esta manera, el paquete CDP es actualizado cada vez con el número de vehículos presentes en las diferentes celdas de la calle. Cuando al final llega a la intersección I1, el CDP es trasmitido de forma *geobroadcast* para que los vehículos que entren en la intersección I1 reciban una estimación de la densidad de esta calle y puedan decidir si enrutar los paquetes *multi-hop* por ella o por otras calles. Para garantizar la escalabilidad, sólo aquellos vehículos que han actualizado el CDP anteriormente generarán un nuevo CDP al llegar a la intersección I2. Según lo explicado en la sección III, dado que el CDP se transmite en modo *multi-hop*, debe utilizar el canal SCH1. Sin embargo, las orientaciones más recientes de la ETSI acerca de la gestión de los canales de comunicaciones [13] establecen que cada transmisión en cada uno de los SCHs tiene que ser previamente anunciada en el CCH por medio de *service advertisements* (SAs). Esto implica que por cada transmisión de un CDP, un SA preliminar debe ser trasmitido en el CCH. Además, con el fin de garantizar que ningún vehículo en la intersección I1 pierda el *broadcast* final del CDP, la implementación de IFTIS considerada en este trabajo ha asumido que la transmisión *geobroadcast* del CDP en la intersección I1 se efectúe en el CCH. Dado que el CDP transporta información de cada una de las celdas en que está dividida la calle, su *payload* es proporcional al número de las celdas, que a su vez depende del rango de comunicaciones. La porción del CDP dedicada a cada celda consta de tres subcampos: el identificador de la celda, su posición y su densidad. Sin embargo, el *payload* del CDP incluye una sección de tamaño fijo, que lleva información sobre el identificador de la calle y el tiempo de generación del mensaje. Para la porción fija del *payload* del CDP, este trabajo supone la utilización de ocho octetos para representar el identificador de la calle y de cuatro octetos para el tiempo de generación del paquete. Ocho octetos adicionales se han añadido para indicar las coordenadas geográficas de la intersección I1, ya que ésta es el último destino hacia al cual el CDP tiene que dirigirse después de haber atravesado todas las celdas de la calle. Para la parte del *payload* dedicada a cada celda, se han considerado ocho octetos para representar las coordenadas de su centro (posición de la celda), seis bits para su identificador, y diez bits para su densidad[1]. A fin de calcular el tamaño total de los paquetes CDP incluyendo cabeceras de capa MAC y NET/TR, se han utilizado las actuales definiciones de la ETSI sobre los paquetes de *geonetworking* [14]. En este caso, los paquetes CDP *geounicast*, *geobroadcast* y SA requerirían 153, 149 y 95.5 octetos respectivamente sin considerar la parte de tamaño variable del *payload* del CDP.

B. Entorno de evaluación

Las prestaciones de DiRCoD han sido evaluadas mediante simulaciones basadas en el análisis de trazas vehiculares obtenidas por el simulador de tráfico SUMO (Simulation of Urban MObility) [15]. El escenario bajo consideración es una calle de 750m, similar a las mostradas en la Figura 2, con un carril por sentido de marcha y dos intersecciones en sus extremos. Las zonas de intersección han sido dimensionadas con un radio de 20m, mientras que las secciones en que DiRCoD divide la calle se han fijado a un valor de 300m que, como ha sido explicado en la sección III.A, representa el rango de comunicaciones en el SCH1. Se considera una densidad media de 21 vehículos por kilómetro y por carril en la calle. Los vehículos utilizan un rango de comunicaciones constante en el CCH que será variado para analizar su influencia. Es asumido además que los mensajes CAM sean trasmitidos con una frecuencia de 1Hz, aunque tendencias parecidas se pueden obtener a frecuencias distintas. Los resultados de simulación han sido conseguidos a través de simulaciones con una duración de 5000 segundos a fin de asegurar su precisión estadística.

C. Resultados de las prestaciones

La Figura 3 indica la probabilidad de que los vehículos en la intersección I1 reciban por lo menos un mensaje de conectividad (un CAM con un *connectivity field* en el caso de DiRCoD, o un paquete CDP en el caso de IFTIS) antes de abandonar la zona de intersección[2]. Esta métrica representa la capacidad de las técnicas para proporcionar a los vehículos que entran en la intersección I1 información de conectividad actualizada. Esta información es utilizada para decidir por cual de las calles que salen de la intersección enrutar paquetes de datos en el caso de transmisiones *multi-hop* donde estos vehículos actúen como nodos retransmisores. Como se muestra en la Figura 3, DiRCoD siempre proporciona esta información con una probabilidad más alta, independientemente del rango de transmisión y de su configuración. Además, las prestaciones de DiRCoD aumentan al aumentar el rango de comunicaciones. Los resultados obtenidos demuestran que DiRCoD es capaz de actualizar la información de conectividad *multi-hop* de las

[1] Estos últimos dos valores han sido escogidos para tener en cuenta los escenarios más pesimistas. De hecho, utilizando un pequeño rango de comunicaciones de 100m, 6 bits para el identificador de la celda son suficientes para representar 64 celdas sobre calles de hasta 12.8km. Al contrario, si se consideran elevados rangos de comunicaciones de, por ejemplo, 500m, la codificación de la celda con 10 bits permite representar escenarios de muy alta densidad con más de 1000 vehículos por celda.

[2] Las prestaciones de DiRCoD son presentadas para tres configuraciones diferentes en las que el *connectivity field* se agrega a cada mensaje CAM (1), o a uno de cada dos (2), o de cada tres (3) mensajes CAM.

calles con una periodicidad más alta que la de IFTIS. Esto, a su vez, mejora el funcionamiento de los protocolos de enrutamiento en VANETs que eligen de forma dinámica el próximo camino de enrutamiento. Las prestaciones menores de IFTIS se deben a que los paquetes CDP solo pueden ser generados en la intersección I2 por vehículos que anteriormente actualizaron paquetes CDP mientras atravesaban las celdas antes de alcanzar la intersección I2. Como los autores de IFTIS explican, esta característica es necesaria por razones de escalabilidad.

Además de analizar la capacidad de cada técnica de proveer información útil de conectividad a protocolos de enrutamiento, es muy importante investigar la sobrecarga de comunicaciones que estas técnicas crean. En este contexto, la Figura 4 presenta la sobrecarga de comunicaciones media que cada técnica genera para retransmitir la información de conectividad desde la intersección I2 a I1 según el ejemplo mostrado en la Figura 2a). Es importante recordar que la sobrecarga de DiRCoD se genera en el CCH, ya que agrega el *connectivity field* a mensajes CAM. Al contrario, la sobrecarga de IFTIS está repartida entre el CCH (transmisiones de SAs y transmisión *geobroadcast* del paquete CDP en la intersección I1) y el SCH1 (transmisiones *multi-hop geounicast* de paquetes CDP a lo largo de la calle). Es importante además destacar que, para los rangos de comunicaciones más cortos, el tamaño del CDP aumenta, ya que es necesario un número más alto de celdas para cubrir la calle. Los resultados obtenidos muestran claramente que la sobrecarga de comunicaciones generada por DiRCoD es menor que la generada por IFTIS. Sin embargo, dado que DiRCoD actualiza con más frecuencia que IFTIS la información de conectividad (ver la Figura 3), es necesario analizar la sobrecarga no solo para cada transmisión de información de conectividad desde I2 a I1, sino también para un intervalo temporal definido. En este contexto, la Figura 5 muestra la sobrecarga de comunicaciones media generada por ambas técnicas para un intervalo temporal de un segundo. En este caso, la diferencia entre DiRCoD e IFTIS se reduce. Sin embargo, como se ha explicado anteriormente, la sobrecarga generada por DiRCoD puede ser disminuida reduciendo la frecuencia con la que se agrega el *connectivity field* a los mensajes CAM. Como se puede observar en la Figura 3, esta ganancia en términos de menor sobrecarga es obtenida sin afectar significativamente a la probabilidad de que un mensaje de conectividad sea recibido en la intersección I1.

Finalmente, la Figura 6 presenta el ratio entre la sobrecarga de comunicaciones media por segundo introducida por cada técnica en el CCH y la probabilidad de recibir por lo menos un mensaje de conectividad en I1[1]. Esta métrica es muy importante ya que representa la eficiencia en proporcionar datos actualizados sobre la conectividad *multi-hop* de la calle a los vehículos que entran en la intersección I1, sin incurrir en una gran sobrecarga de comunicaciones. En este contexto, los resultados obtenidos han mostrado que DiRCoD es capaz de proveer de forma dinámica y eficaz información de conectividad *multi-hop* con una mínima sobrecarga y con un bajo coste de implementación.

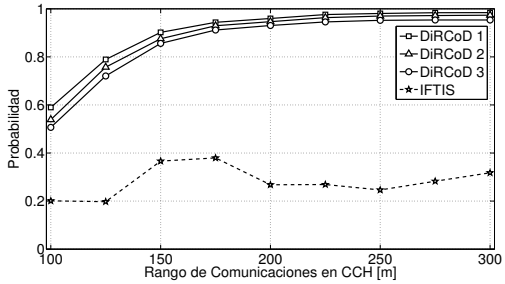


Figura 3. Probabilidad de recibir por lo menos un mensaje de conectividad en la intersección I1.

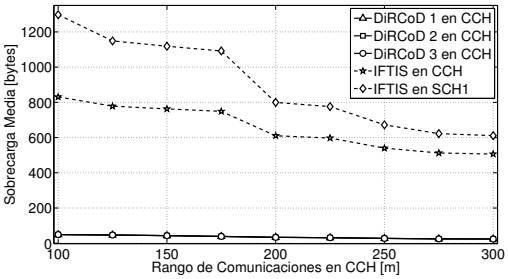


Figura 4. Sobrecarga de comunicaciones media.

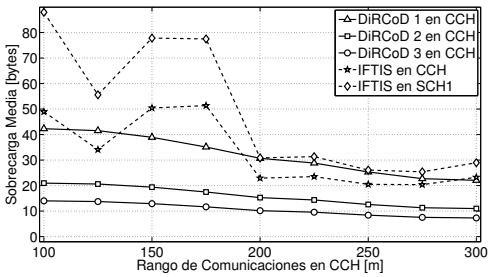


Figura 5. Sobrecarga de comunicaciones media en un segundo.

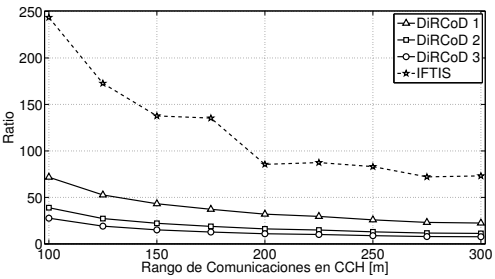


Figura 6. Eficiencia de la sobrecarga de comunicaciones en términos de conectividad *multi-hop*.

V. CONCLUSIONES Y TRABAJOS FUTUROS

Los protocolos de enrutamiento *multi-hop* que utilizan una selección dinámica del camino de enrutamiento basándose en las condiciones actuales del tráfico mejoran los esquemas convencionales de enrutamiento en VANETs. Para utilizar técnicas eficaces y dinámicas de selección de caminos *multi-hop* es necesario desarrollar herramientas de apoyo que computen y actualicen la capacidad de retransmisión *multi-*

[1] Es importante destacar que la sobrecarga de IFTIS en el SCH1 no es considerada en este caso.

hop de estos caminos. Con este propósito, este artículo ha presentado DiRCoD, un mecanismo eficiente que, utilizando mensajes vehiculares *beacon* estándar, permite estimar de forma distribuida la capacidad de enrutamiento de los segmentos de carretera en términos de conectividad *multi-hop*. Como se ha mostrado en este trabajo, DiRCoD es capaz de estimar dinámicamente esta conectividad *multi-hop* con una baja sobrecarga de comunicaciones y con un coste de implementación mínimo.

Los autores de este trabajo están actualmente desarrollando un protocolo de enrutamiento para VANETs que utiliza DiRCoD como herramienta de apoyo. Siguiendo la filosofía de tomar decisiones de enrutamiento en las intersecciones en base al estado de conectividad de las distintas calles, la finalidad de dicho protocolo será la de garantizar la correcta entrega de los paquetes, independientemente de las variaciones de la distribución del tráfico de vehículos en la red de carreteras considerada. En este contexto, se aprovechará la capacidad de DiRCoD para medir la conectividad con un bajo consumo de recursos radio, garantizando el funcionamiento en escenarios de elevada utilización del canal provocada por una alta densidad de vehículos. Además, se implementarán las funcionalidades necesarias para mantener las prestaciones de encaminamiento en aquellos casos en que una baja densidad de vehículos dificulte el enrutamiento de los paquetes hasta el destino.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por la Comisión Europea a través del proyecto FP7 iTETRIS: An Integrated Wireless and Traffic Platform for Real-Time Road Traffic Management Solutions (No. FP7 224644). Los autores desean agradecer a la Comisión el apoyo recibido.

REFERENCIAS

[1] B. Karp and H. T. Kung, “GPSR: greedy perimeter stateless routing for wireless networks,” en Libro de Actas ACM/IEEE MOBICOM’00, Boston, Massachusetts, USA, 2000, pgs. 243–254

[2] H. Fussler, J. Widmer, M. Kasemann, M. Mauve, and H. Hartenstein “Contention-based forwarding for mobile ad hoc networks”, en Ad Hoc Networks, vol. 1, no. 4, pgs.351-369, Nov. 2003.

[3] R. Bauza, J. Gozálvez and M. Sepulcre, “Operation and Performance of Vehicular Ad-hoc Routing Protocols in Realistic Environments”, en Libro de Actas IEEE 68th Vehicular Technology Conference, 2008, VTC 2008-Fall, pgs.1-5, 21-24 Sept. 2008

[4] Jing Tian, Lu Han, K. Rothermel, “Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks”, en Libro de Actas IEEE Intelligent Transportation Systems 2003, vol.2, pgs. 1546- 1551, 12-15 Oct. 2003

[5] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve , “A routing strategy for vehicular ad hoc networks in city environments,” en Libro de Actas IEEE Intelligent Vehicles Symposium 2003, pgs. 156- 161, 9-11 Junio 2003

[6] Jing Zhao, Guohong Cao, “VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks,” IEEE Transactions on Vehicular Technology , vol.57, no.3, pgs.1910-1922, Mayo 2008

[7] Jaehoon Jeong, Shuo Guo, Yu Gu, Tian He, D. Du, “TBD: Trajectory-Based Data Forwarding for Light-Traffic Vehicular Networks,” en Libro de Actas 29th IEEE International Conference on Distributed Computing Systems ICDCS '09, 2009, pgs.231-238, 22-26 June 2009

[8] K.C. Lee, M. Le, J. Harri, M. Gerla, “LOUVRE: Landmark Overlays for Urban Vehicular Routing Environments,” en Libro de Actas IEEE 68th Vehicular Technology Conference VTC 2008-Fall, 2008, pgs.1-5, 21-24 Sept. 2008

[9] J. Nzouonta, N. Rajgure, Guiling Wang, C. Borcea, “VANET Routing on City Roads Using Real-Time Vehicular Traffic Information,” IEEE Transactions on Vehicular Technology, vol.58, no.7, pp.3609-3626, Sept. 2009

[10] M. Jerbi, S.-M. Senouci, T. Rasheed, Y. Ghamri-Doudane, “Towards Efficient Geographic Routing in Urban Vehicular Networks,” IEEE Transactions on Vehicular Technology, vol.58, no.9, pp.5048-5059, Nov. 2009

[11] M. Jerbi, S.-M. Senouci, T. Rasheed, Y. Ghamri-Doudane, “An Infrastructure-Free Traffic Information System for Vehicular Networks,” en Libro de Actas IEEE 66th Vehicular Technology Conference, 2007, VTC-2007 Fall, pgs.2086-2090, 30 Sept. 2007-3 Oct. 2007

[12] COMeSafety consortium, “D31: European ITS Communication Architecture: Overall Framework Proof of Concept Implementation”, COMeSafety European Specific Support Action Public Deliverable, Dic. 2009

[13] ETSI TC ITS, “Intelligent Transport Systems (ITS); Communications; Architecture; Vehicular Communication, Basic Set of Applications, Part 4: Operational Requirements”, Draft ETSI DTS 102 637-4, Marzo 2010

[14] ETSI TC ITS, “Intelligent Transport Systems (ITS); Communications; Architecture; Vehicular Communications, Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 1: Media-Independent Functionality”, Draft ETSI TS 102 636-4-1 v0.0.5, Enero 2010

[15] Simulation of Urban MObility (SUMO) http://sourceforge.net/apps/mediawiki/sumo/

Consolidación de redes Fiber Channel y Ethernet en centros de datos con Fiber Channel sobre Ethernet (FCoE)

Jesús Menéndez Reyes
Cisco Systems España
Avenida de la Vega, 5
28100 Alcobendas (Madrid)
jmenende@cisco.com

***Resumen*: Fiber Channel over Ethernet (FCoE) es un estándar aprobado en junio de 2009 por el International Commitee for Information Technology Standards para el transporte de Fiber Channel (FC) sobre Ethernet a 10 Gbps. El estándar se complementa con extensiones a Ethernet para que transporte tráfico crítico como FC sin pérdidas. El objetivo es simplificar equipamiento y operaciones en los centros de datos consolidando las redes de datos y de almacenamiento en una única red. Este artículo pretende presentar y evaluar el nuevo estándar, con una perspectiva de evolución tecnológica, desde el almacenamiento local hasta FCoE.**

1. INTRODUCCIÓN

Los centros de procesamiento de datos (CPDs) actuales se encuentran sometidos a grandes presiones. Por un lado, deben de crecer para dar respuesta a las necesidades del negocio; por otro, deben de mantener o incluso reducir los costes de operación (espacio físico, consumo eléctrico, ventilación, horas de trabajo) y de capital (cableado, sistemas de computación, almacenamiento y red)

Actualmente los CPDs suelen mantener varias redes separadas y aisladas, cada una de ellas con su equipamiento, cableado y adaptadores propios. Existen redes Ethernet para la conexión de datos entre los servidores del CPD y los clientes; redes de almacenamiento SAN (Storage Area Networks) para interconectar los servidores con los sistemas de discos de almacenamiento; y con mucha menor frecuencia pueden existir redes de alta computación (HPC o High Performance Computing) sobre tecnología Infiniband para servidores que trabajan de forma conjunta.

Consolidar estas redes en una sola es una oportunidad para reducir costes: menos conmutadores de red, cables y adaptadores de red con los consiguientes ahorros en espacio físico, consumo energético y simplificación en las operaciones.

La multiplicación del ancho de banda en los enlaces Ethernet de los servidores de 1 Gbps a 10 Gbps reduce cables y conexiones en la LAN, pero se consigue una simplificación aun mayor si se aprovecha ese caudal para transportar también el tráfico de la SAN.

FCoE es una tecnología que posibilita esta consolidación de manera gradual y compatible con tecnologías SAN ya existentes y en las que empresas y organizaciones han realizado grandes inversiones, como es FC. Más aun, FCoE aprovecha y mantiene las inversiones realizadas en FC.

2. ALMACENAMIENTO: UNA APROXIMACIÓN HISTÓRICA

La aproximación más sencilla al almacenamiento es utilizar los propios discos duros corresidentes de ordenadores y servidores. Surgieron así las interfaces IDE/ATA-1 (Integrated Device Electronics/Advanced Technology Adapter) y SCSI (Small Computer System Interface) en 1986, para la interconexión del ordenador con discos de almacenamiento masivo locales

Actualmente IDE/ATA y sus evoluciones se utilizan en PCs, mientras que SCSI, dada su mayor complejidad y capacidad está posicionado en servidores y estaciones de trabajo.

SCSI inicialmente se definió como un protocolo en paralelo, aunque desde 2003 existe una implementación en serie (SAS o Serial Attached SCSI, tercera versión del estándar), que ofrece mayor velocidad de transferencia y se puede transportar en red. [1] [2]

2.1 DIRECT ATTACH STORAGE (DAS)

En una arquitectura cliente-servidor, todas las transacciones con una aplicación pasan por el servidor, luego son éstos los equipos en los que es más importante hacer copias de seguridad o a los que proveer con mayores capacidades de almacenamiento.

Superada la capacidad local, el siguiente paso es utilizar almacenamiento externo en los servidores.

La forma más sencilla es conectar el almacenamiento externo directamente a los servidores. Es lo que se conoce como DAS (Direct Attach Storage) (Figura 1) El almacenamiento externo se realiza en cabinas de discos, conectadas a los servidores. Las cabinas no son actualmente un mero contenedor de discos, sino un sistema inteligente de almacenamiento tolerante a fallos que ofrece servicios avanzados como RAID (Redundant Array of Independent Disks) y virtualización. El SO (sistema operativo) del servidor ve los discos externos como propios.

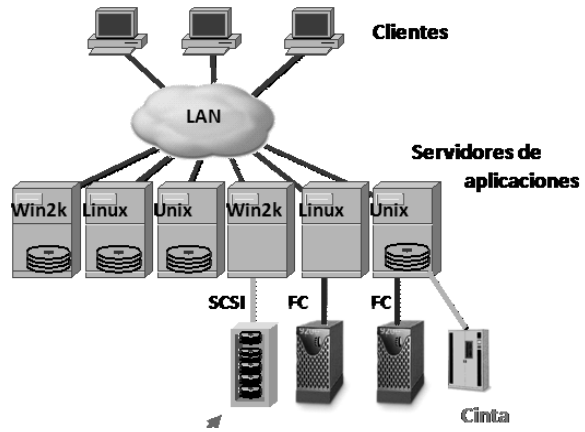


Fig. 1 Arquitectura DAS (Direct Attached Storage)

Este modelo es sencillo, pero tiene varios inconvenientes. Conforme el número de servidores que necesitan almacenamiento crece, la complejidad de operación aumenta. No existe una visibilidad compartida de los datos, ya que están asociados a cada servidor concreto, y por tanto la movilidad del almacenamiento está limitada. Además, se pueden producir ineficiencias, donde unos servidores tengan sus cabinas infrautilizadas, mientras otros tengan sus discos llenos y no puedan crecer más.

Colocar el almacenamiento en red, como un recurso compartido al que pueden acceder los servidores conforme lo necesiten, simplifica la operación y gestión, incrementa la movilidad y permite utilizar las cabinas de una manera más eficiente.

Necesidades técnicas y económicas llevaron a las impresoras a conectarse en red como recurso compartido, e igual ha ocurrido con las cabinas de almacenamiento, sólo que en este caso, la red que conecta a ellas debe de cumplir con requisitos muy estrictos de rendimiento, latencia, y sobre todo de garantía de que no se pierdan paquetes. Por estas razones suele ser una red dedicada, separada de la de datos. Además, la administración de esa red suele recaer bajo la responsabilidad de los administradores del almacenamiento y/o los servidores. Con una red separada se consigue una administración independiente de la de comunicaciones. [2]

2.2. SAN: STORAGE AREA NETWORKS O REDES DE ÁREA DE ALMACENAMIENTO

Existen dos formas de almacenar los datos en discos, a nivel de bloque o de fichero. Hablamos de bloque cuando se copian posiciones de memoria física (que es como funciona SCSI) y se deja que el SO las organice en ficheros. Si en la copia consideramos la estructura de ficheros, entonces hablamos de un sistema de almacenamiento NAS (Network Attached Storage)

En el almacenamiento NAS, la transmisión de datos se realiza a través de un protocolo de transferencia de ficheros: NFS (Network File System), para sistemas Unix y Linux, o CIFS (Common Internet File System) para sistemas Microsoft. En realidad un sistema NAS no deja de ser un servidor compartido que se utiliza como repositorio de ficheros en red. [2]

SCSI en serie, al contrario que las versiones en paralelo, puede ser transportado por un protocolo de red. Cuando conectamos servidores con cabinas de almacenamiento a través de SCSI en red, hablamos de redes de área de almacenamiento (o por su nombre en inglés SAN o Storage Area Networks) (Figura 2)

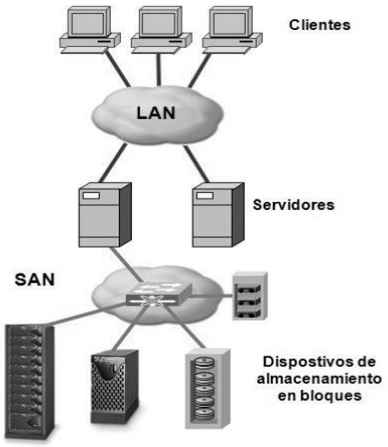


Fig. 2 Arquitectura de red SAN

En la actualidad se emplean dos maneras de transportar SCSI en red: sobre el protocolo IP (iSCSI) o sobre un protocolo específico denominado Fiber Channel (FC)

2.2.1. iSCSI (INTERNET SCSI)

iSCSI es el transporte de SCSI sobre IP. Impulsado por IBM y Cisco, en 2003 fue aprobado como estándar por el IETF con el nombre de RFC 3790. Dado que al almacenar en discos no se deben perder paquetes, el transporte se realiza sobre TCP (Transmission Control Protocol), el nivel 4 de la pila TCP/IP orientado a la conexión, que transmite de manera confiable los datagramas, retransmitiéndolos en caso de pérdida.

En principio iSCSI, como cualquier otra aplicación IP, debería de poder transportarse sobre la red Ethernet de datos habitual. Sin embargo, por latencia, rendimiento y administración, suele ser una red Ethernet dedicada, independiente de la que comunica a los servidores con los clientes. En aquellos casos en que una red dedicada no sea posible, se recomienda utilizar una VLAN (Virtual LAN) dedicada sobre la infraestructura Ethernet existente. [3]

iSCSI puede funcionar con tarjetas de red Ethernet NIC (Network Interface Card) comunes, pero iSCSI es un proceso que carga mucho a los servidores (tanto por el propio SCSI como por el TCP asociado). Existen tarjetas de red específicas que realizan el procesamiento en hardware, aliviando al SO de esa carga. Pero siempre tendrá más rendimiento un sistema que impide las pérdidas de tramas, como es FC, que otro que las retransmite, como iSCSI.

Se puede afirmar que iSCSI no ha alcanzado la popularidad y uso de otras tecnologías SAN como Fiber Channel, en gran parte debido a un rendimiento insuficiente y a sobrecargar la CPU del servidor. [4] [5]

2.2.2 FIBER CHANNEL

Fiber Channel es un protocolo de red que transporta tráfico de almacenamiento en formato SCSI para interconectar servidores con equipos de almacenamiento. Fue definido por el comité T11, del INCITS, que a su vez depende del instituto estadounidense de estándares ANSI.

El estándar define una pila completa de 5 capas (numeradas de 0 a 4) similar al modelo OSI.

La capa FC-0 define la interfaz física. En la práctica sólo se utiliza fibra (multimodo, monomodo o WDM). Los servidores se conectan a la red FC a través de una tarjeta HBA (Host Bus Adapter) específica.

La capa FC-1 define la codificación de línea. Actualmente se utilizan dos codificaciones: 8B/10B, para los anchos de banda 1/2/4/8 Gbps; y la 64B/66B, para ancho de banda de 10 Gbps (incluído FCoE)

La capa FC-2 es equivalente a la capa de enlace en el modelo OSI. Define la trama, las direcciones FC; el funcionamiento de “hubs”, que se conocen como “arbitrated loops” (FC-AL) y “switches” (FC-SW-2); el mecanismo de registro/baja en la red (“login”/”logout”); los servicios de red, que se ofrecen como servidores (de login, de nombres y zonas, de notificaciones o “fabric controller”) que residen en la infraestructura de red; los filtros o zonas; y los mecanismos de selección de ruta como FSPF (First Shortest Path First)

La capa FC-3 no ha llegado a implementarse, y su objetivo es definir servicios comunes como cifrado o compresión.

La capa FC-4 define el mapeo de protocolos superiores sobre FC. El más habitual es SCSI-3, pero también existen especificaciones para transportar sobre FC otros protocolos como IP (definido como RFC-2526) o ATM.

El estándar define varios tipos de tráfico, pero en la práctica sólo se utilizan dos: clase 3 (que es FC no orientado a la conexión y sin mecanismo de confirmación) y clase F, que se utiliza como señalización entre switches. Los switches se identifican dentro de una red SAN a través de un número único de 8 bits denominado Domain ID. Esto limita el número máximo de switches en una SAN a 256, aunque en la práctica el límite está muy por debajo.

Una diferencia entre FC y Ethernet es que si en éste todos los puertos de red son iguales, FC muy estricto en la definición de los puertos. Así, cuando servidores y cabinas conectan a la red, su lado del enlace se denomina N_Port (puerto N), mientras que el lado de red se denomina F_Port (puerto F) Los enlaces entre switches, conocidos como ISL (Inter-Switch Link) se forman entre E_Ports (puertos E)

FC utiliza dos tipos de direcciones, WWN (World Wide Names) y FCID (Fiber Channel IDs). WWN son direcciones únicas de 64 bits que definen unívocamente los puertos de un switch o de una tarjeta HBA. Las direcciones FCID tienen 24 bits, y las entrega la red a los servidores. La red FC utiliza ambas direcciones, las FCID para conmutar las tramas, y las WWN para filtrar el

tráfico por zonas. WWN y FCID son similares a las direcciones MAC e IP, respectivamente.

En FC los servidores tienen que registrarse en la red para poder conectarse. Es lo que se conoce como FLOGI. Una vez realizado, la red entrega al servidor una dirección FCID. A continuación el servidor se registra a través de transacciones PLOGI en el "Name Server", y en los equipos de almacenamiento en los que está autorizado por las zonas activas. El servidor se registra también en el servidor "Fabric controller" a través de un mensaje SCR (Status Change Registration). El "fabric controller" mantendrá informado a los servidores de cualquier cambio en la topología de la red a través de mensajes RSCN (Registered State Change Notification). Este mecanismo centralizado de notificaciones hace de FC un protocolo que hace poco uso de la difusión, en contraste con Ethernet. Otras transacciones como PRLOGI, conectan con los discos SCSI concretos dentro de los dispositivos de almacenamiento.

El servidor de nombres o "name server" mantiene el registro de las direcciones WWN y de las FCID correspondientes. Además, se ocupa del control de zonas, que son un filtro de seguridad en el que se especifican qué conexiones entre servidores y cabinas están autorizadas. Es responsabilidad de los dispositivos de red hacer que el tráfico cumpla con las zonas. Las zonas pretenden evitar que servidores con sistemas operativos diferentes se interfieran, escribiendo sobre el mismo espacio en disco.

Otra diferencia crítica entre Ethernet y FC es que en el primero se puede perder paquetes, mientras que en el segundo no está permitido. Por ello FC tiene un mecanismo de control de flujo, por el cual los dos lados del enlace se informan de su capacidad de almacenar tramas, y sólo en caso de que el otro extremo garantice la recepción de la trama, ésta se transmite. La capacidad de almacenar tramas se denomina créditos buffer a buffer ("buffer to buffer credits") y las dos partes de un enlace FC llevan una contabilidad de los créditos disponibles en el otro extremo.

En los últimos años han cobrado especial importancia las tecnologías de recuperación ante desastre y continuidad de negocio. Una práctica recomendada por diferentes reglamentaciones es disponer de un centro de datos de respaldo, y FC puede replicar los datos del CPD principal al de respaldo (lo que se conoce como replicación) a través de una SAN extendida. [5]

3. LIMITACIONES DE FIBER CHANNEL

En la actualidad los servidores que soportan aplicaciones importantes mantienen conexiones separadas a FC y a Ethernet, para conectar a las cabinas de almacenamiento y a los clientes respectivamente. Para ello, se tiene dos redes separadas, con sus switches, tarjetas de red (HBAs y NICs), cables y procesos de administración independientes (Figura 3)

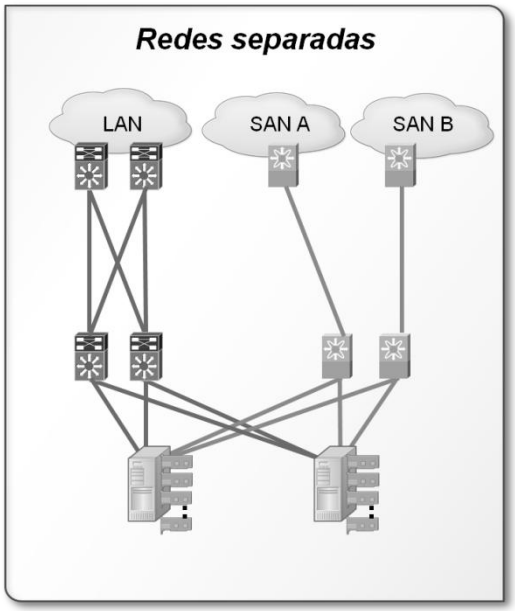


Fig. 3 Servidores conectados a redes Ethernet y FC separadas

Si ambas redes se pudieran consolidar en una sola, que permitiera FC y Ethernet a la vez, con las mismas tarjetas y los mismos cables, se ahorraría en espacio en los centros de datos (y con ello en consumo eléctrico y refrigeración), en equipamiento (tarjetas, switches) y cableado, y en operaciones simplificadas. Además se aprovecharía la inversión realizada en FC. Es lo que en la industria se conoce como "fabric unificada".

Pero hay otro catalizador que empuja muy fuerte hacia la consolidación de redes, y es la virtualización de los servidores. Y ello por dos razones: por universalizar el acceso al almacenamiento, y por limitar la multiplicación del número de tarjetas de red en los servidores.

La virtualización de servidores es la posibilidad de definir múltiples servidores virtuales o lógicos sobre un único servidor físico. Con la virtualización de servidores se ahorran costes, por la utilización más intensiva del hardware físico subyacente; igualmente se gana en flexibilidad operativa, al poder aprovisionar, activar y desactivar servidores más rápidamente y con independencia del hardware. No es de extrañar que se uso se haya popularizado enormemente en los últimos años.

Las soluciones de virtualización incluyen funcionalidades que permiten que los servidores (o máquinas) virtuales se

puedan mover de unos servidores físicos a otros, incluso de manera automática. De esta manera, la máquina virtual se convierte en un elemento "fluido" que se puede activar y desactivar bajo demanda y que se mueve por la red migrando de un servidor a otro. La "identidad" (básicamente su sistema de ficheros) del servidor virtual reside en un disco de almacenamiento compartido, al que tienen acceso todos los servidores físicos sobre los que puede migrar el servidor virtual. La movilidad de los servidores virtuales ha extendido aun más el uso de las redes de almacenamiento, haciendo que los datos almacenados en discos externos sean accedidos frecuentemente (Figura 4) [6]

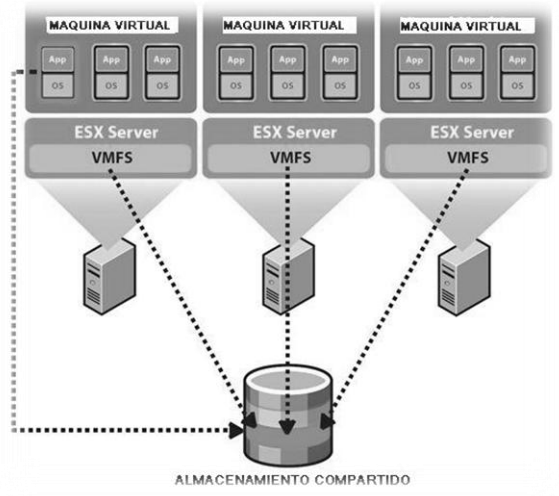


Fig. 4 Servidores virtuales con almacenamiento compartido

Por ello, cada servidor físico virtualizado debe de tener conexión a una SAN. Las opciones son extender FC (con el consiguiente coste) a todos los servidores físicos; o limitar la movilidad y con ello la virtualización a servidores concretos, lo que también complica las operaciones.

Unificar FC y Ethernet simplificaría enormemente la operativa en entornos virtuales, sin disparar el coste.

Si con la virtualización se aumenta la utilización de los servidores físicos, también hace falta más ancho de banda de E/S, para aprovechar ese incremento de rendimiento. Además del tráfico cliente-servidor propio de las aplicaciones ahora sobre sistemas operativos virtualizados, la propia virtualización produce tráfico de uso interno (para la gestión, o el movimiento de máquinas virtuales, por ejemplo) lo que se traduce en más necesidad de E/S.

La manera de dar más E/S en los servidores ha sido añadir tarjetas de red (NICs) de un 1 Gbps. La profusión de múltiples tarjetas NIC más las tarjetas HBA para el almacenamiento en los servidores virtualizados supone un entorno de operación muy complicado.

Recientemente han aparecido tarjetas Ethernet a 10 Gbps, que pueden consolidar muchos enlaces de 1 Gbps. Pero tendríamos una consolidación y simplificación aun mayores si esas tarjetas sirvieran también para el almacenamiento.

iSCSI cumple técnicamente con esos requerimientos, pero su uso no se ha generalizado, al contrario que FC. La realidad es que FC es un protocolo ampliamente implantado, y cualquier solución de consolidación debe de contemplar este hecho.

Y aquí es donde hace su aparición FCoE (Fiber Channel over Ethernet).

4. FIBER CHANNEL SOBRE ETHERNET (FCoE)

FCoE es el transporte de FC sobre redes Ethernet. Es estándar desde junio de 2009, definido como FC-BB-5 por el grupo técnico T.11 del INCITS.

La idea detrás de FCoE es mantener FC y sus ventajas, pero transportándolo sobre Ethernet sin perder tramas. Así se mantiene la inversión realizada en FC: las cabinas, el conocimiento del personal de operaciones, el software de gestión de las tarjetas HBA,…

FCoE asume que la red Ethernet no pierde tramas en caso de congestión, pero deja este detalle a los organismos normativos de Ethernet (concretamente al IEEE) Dentro de la pila FC, FCoE se corresponde con FC-2, mientras que FC-0 y FC-1 corresponderían ahora a Ethernet sin pérdidas. FC-3 y FC-4 no sufren ninguna modificación respecto del estándar FC original. Dado que Ethernet por definición pierde paquetes en caso de congestión, se ha definido un Ethernet especial sin pérdidas para FCoE. Se denomina DCB (Data Center Bridging) y hablaremos de él más adelante.

FC-BB-5 distingue entre ENodes que son los servidores y cabinas de almacenamiento y FCF (FCoE Forwarders) que son los switches FCoE. El FCF realiza el encapsulado y desencapsulado de FCoE. El FCF es un switch FC en el sentido de que necesita un Domain ID, y sobre él se registran ("login") los ENodes. En el FCF se definen y aplican las zonas FC.

En una red FCoE puede haber también switches "FCoE passthrough", con capacidad DCB, que pueden transportar FCoE sin pérdidas, pero que no tienen inteligencia FC: sólo ven tramas DCB sin visibilidad del FC que cargan. Esos switches no necesitan Domain ID, su papel es meramente de transporte o tránsito.

El estándar define dos protocolos: FCoE propiamente dicho, que transporta los datos de almacenamiento, y FIP (FCoE Initialization Protocol) que es el protocolo de señalización. Se distinguen en la trama Ethernet por tener valores diferentes en el campo Ethertype (35078 y 35092 respectivamente)

FIP se ocupa de descubrir las VLANs que transportan FCoE, descubrir los switches FCoE sobre esas VLANs, hacer el "fabric login" con ellos e inicializar, mantener y terminar los enlaces FCoE. Recordemos que FC define básicamente dos tipos de enlaces: entre nodos y switches (entre N_Ports y F_Ports) y entre switches (entre E_Ports). FCoE define estos mismos enlaces ahora sobre transporte Ethernet, pero les añade el prefijo "virtual", y así existen VN_Port, VF_Port, y VE_Port.

La señalización FIP se iniciaría en el momento en que el ENode se conecta a la red, y seguiría este orden:

1/ Descubrimiento de las VLANs (Virtual LANs) FCoE.

El tráfico FCoE debe de estar separado del que no es FCoE en VLANs distintas. El descubrimiento se realiza a través de un mensaje multidifusión a una dirección MAC a la que responden todos los FCFs con un mensaje unidifusión. El descubrimiento se hace sobre la VLAN nativa (la define 802.1q), y por tanto no se debe utilizar para el transporte de datos.

2/ Descubrimiento de los FCFs

Sobre las VLANs de FCoE, el ENode inicia el descubrimiento de los FCFs. Nuevamente con un mensaje de multidifusión a una dirección MAC a la que respondan todos los FCFs. Los FCFs que reciben el mensaje responden directamente al ENode con sus datos. Entre todos los recibidos, el ENode selecciona uno basándose en un valor de prioridad.

3/ Registro en la red ("Fabric login")

Igual que se haría en FC, el ENode hace FLOGI con el FCF. A continuación el FCF entrega al servidor una dirección MAC que utilizará para todo el tráfico FCoE como dirección de origen. Se denomina FPMA (Fabric Provided MAC Address) y sus últimos 24 bits coinciden con el FCID de ese VN_Port (con lo que sería su dirección FC)

4/ Mantenimiento del enlace

FIP define unos mensajes de mantenimiento ("keepalives") entre el ENode y el FCF al que está conectado. En caso de perderse 2 mensajes consecutivos el enlace se da de baja.

5/ Finalización del enlace ("logout")

Cualquiera de los dos extremos del enlace puede señalizar su terminación a través de mensajes FIP similares a los FLOGO de FC.

En la figura 5 se puede seguir el proceso de señalización.

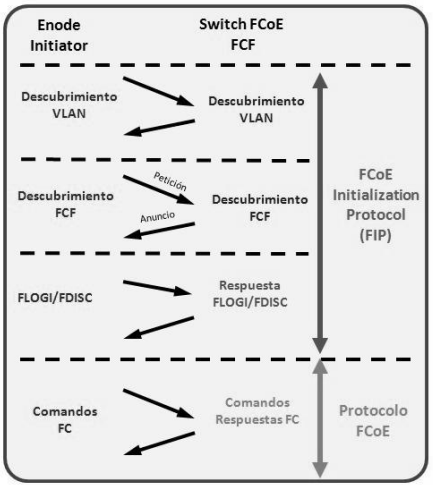


Fig. 5 Señalización FIP / FCoE

Aunque el estándar define FCoE como un protocolo extremo a extremo, desde los servidores a las cabinas, pasando por toda la SAN [7], en la actualidad sólo existen implementaciones de los servidores a los switches de acceso (VN_Ports y VF_Ports); Algunos fabricantes ya han anunciado el soporte de FCoE sobre sus cabinas de manera nativa (Netapp y EMC), pero sólo existen implementaciones de FCoE en el acceso, entre los servidores y el switch de acceso, donde se separa el tráfico puramente Ethernet del FC, y se entregan a sus respectivas redes. Este entorno mixto (redes unificadas en el acceso, redes FC y Ethernet separadas más allá del acceso) se denomina "E/S consolidado." (Figura 6)

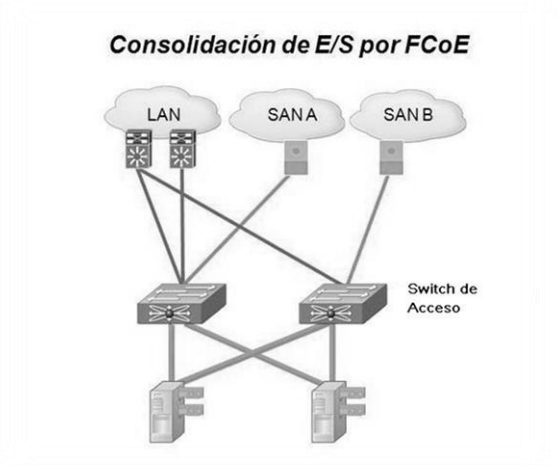


Fig. 6 FCoE en el acceso

Si en el escenario de FC y Ethernet clásico existen tarjetas separadas, HBAs y NICs respectivamente, con FCoE se unifica tarjetas. Las nuevas tarjetas de E/S se denominan CNA (Converged Network Adapters) Son tarjetas Ethernet a 10 Gbps, con capacidad de DCB y con las funciones típicas de una HBA.

La tarjeta CNA se presenta ante el SO del servidor sobre el que está instalada como dos tarjetas diferentes: NIC y HBA. De esta manera, su parte HBA puede ser gestionada de la forma tradicional, a través del software de gestión de tarjetas. Los dos principales fabricantes de adaptadores FC, Emulex y Qlogic tienen disponibles tarjetas CNA, que pueden ser gestionadas con el mismo software que utilizan para sus HBAs. [8]

FC puede funcionar a 4 Gbps y hasta a 8 Gbps (muy poco habitual en servidores, algo más en cabinas). Ethernet a 10 Gbps tiene el ancho de banda suficiente para transportar FC y agregar además varias tarjetas de red Ethernet a 1 Gbps.

4.1. DATA CENTER BRIDGING (DCB)

Uno de los principales retos de FCoE es que FC no permite que se pierdan tramas, mientras que Ethernet puede perder tramas sin problemas en caso de congestión, esperando que los protocolos de capa superior se encarguen de la retransmisión. El IEEE ha definido una serie de extensiones a Ethernet para que pueda transportar FC sin perder tramas. Esas extensiones se conocen con los nombres de 802.1Qbb y 802.1Qaz.

802.1Qbb o Priority-Based Flow Control (PFC) emula el mecanismo de control de flujo de FC. 802.3x es el mecanismo de control de flujo de Ethernet, pero funciona a nivel de todo el enlace, y en la práctica se utiliza muy poco. 802.1Qbb aplica el control de flujo de una manera más granular. No en todo el enlace, sino sobre un tipo de tráfico concreto, que se identifica por el valor del campo clase de servicio (CoS) de la cabecera Ethernet. El mecanismo funcionaría así: el tráfico FC se identifica y marca con un valor de CoS, y PFC aplica control de flujo ("sólo se transmite si hay memoria para recibir") sólo a las tramas con ese valor de CoS, mientras que para el resto de tramas (las que no son FCoE) Ethernet tiene el comportamiento habitual. Recordemos que el campo CoS tiene 3 bits, con lo que podríamos definir hasta 8 tipos de tráfico, cada uno con un mecanismo de control de flujo diferente.

802.1Qaz cumple dos funciones, denominadas Enhanced Transmission Selection (ETS) y DCBX (Data Center Bridging Exchange). ETS optimiza los 10 Gbps del enlace: garantiza un ancho de banda mínimo a cada tipo de tráfico (por ejemplo, 4 Gbps a FC) pero si en un momento dado no lo está utilizando, otro tipo de tráfico puede hacerlo en su lugar. ETS garantiza el ancho de banda a cada clase de servicio, pero no lo reserva, para que no se pierda si no se ocupa. DCBX es un protocolo de negociación por el que el servidor y el puerto de red confirman que tienen capacidades de DCB. Si no lo confirman (esto es, si alguno de los dos extremos no soporta ETS o PFC), formarían un enlace Ethernet convencional. DCBX se ocupa también de notificar si la capa de enlace está activa o no para FC y Ethernet. [8]

4.2. CONVIVENCIA FCoE Y ETHERNET

Hemos visto que FCoE preserva los mecanismos de FC (sus aplicaciones de gestión, por ejemplo en las tarjetas; el mecanismo de registro en la red; el control de flujo; las zonas y la asignación de direcciones) Por otro lado, DCB puede transportar FC sin pérdidas.

Una cuestión a resolver en FCoE es la diferencia en la facilidad de interoperabilidad entre Ethernet y FC. Si en el primero la interoperabilidad entre estaciones (PCs y servidores), SO, tarjetas de red y switches se da por supuesta (todo funciona, salvo que la experiencia demuestre lo contrario), en el segundo se tiene que confirmar y documentar por los fabricantes en extensas matrices públicas (se asume que sólo funciona aquello que se ha probado). Actualmente en los sistemas FCoE se certifica la interoperabilidad, al igual que en FC, pero es posible que con el tiempo la "cultura de interoperabilidad" de Ethernet se termine imponiendo.

Ethernet y FC se suelen desplegar en dos arquitecturas de red diferentes. En Ethernet se utiliza el modelo jerárquico, que consiste en la ordenación de los switches en tres capas: acceso, distribución y núcleo. Por el contrario, en FC prima la redundancia, y se suele desplegar en redes duplicadas aisladas, con servidores y cabinas que conectan a esas dos redes simultáneamente.

Actualmente FCoE se limita a la capa de acceso y mantiene las dos redes LAN y SAN paralelas (Figura 6).

Conforme FCoE se extienda hasta las cabinas de almacenamiento, habrá que consensuar una arquitectura de red que cumpla con los requisitos de Ethernet y FC, y sobre todo con las expectativas que los administradores de ambos dominios tienen respecto de los sistemas a su cargo. Es muy posible que en una primera fase se mantengan redes DCB separadas para el almacenamiento y los datos (Figura 7), para más adelante, conforme la tecnología FCoE demuestre su madurez y fiabilidad, consolidar en una única arquitectura.

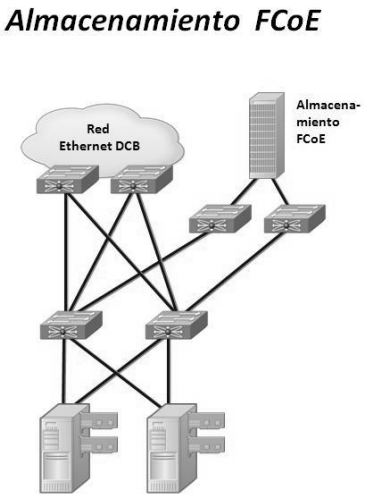


Fig. 7 FCoE extremo a extremo con infraestructura separada

Una limitación actual de la tecnología FCoE es que no se puede utilizar para conectar cabinas entre centros de datos. No es posible extender la SAN a través de FCoE, sino que su uso es local en un CPD. [8]

5. CONCLUSIONES

El mantenimiento de dos redes separadas en centros de datos, una para los PCs, otra para el almacenamiento, es ineficiente, costoso y dificulta la virtualización de servidores. Por otro lado, los centros de datos han hecho grandes inversiones en FC, que es una tecnología probada y madura en un entorno tan crítico como el del almacenamiento y las copias de seguridad.

FCoE es un estándar del INCITS, el mismo organismo reglamentador de FC, que responde a la necesidad de consolidar redes separadas bajo una misma infraestructura, pero manteniendo todas las funcionalidades de FC. Dado que Ethernet puede perder tramas, pero FC no, el IEEE ha definido DCB para el transporte conjunto de FC y datos sobre una misma red Ethernet, esta vez sin pérdidas.

Los servidores acceden a la red unificada FCoE a través de unas tarjetas de red nuevas denominadas CNA, con capacidad DCB a 10 Gbps. Estas tarjetas de 10 Gbps pueden reducir el número de NICs de 1 Gbps y de HBAs, que en los servidores se han multiplicado por la virtualización.

Actualmente FCoE puede desplegarse como tecnología de acceso: de los servidores a unos switches de acceso en los que luego se separa el tráfico a las redes LAN y SAN. En la siguiente fase FCoE se extenderá a una única red, de los servidores hasta las cabinas. Queda para más adelante el uso de FCoE de un centro de datos a otro secundario de respaldo como solución de continuidad de negocio.

REFERENCIAS

[1] Andrei Khurshudov, “The Essential Guide to Data Computer Storage: from floppy to DVD”, Prentice Hall, 2001.

[2] Marc Farley: “Storage Networking Fundamentals: An Introduction to Storage Devices, Subsystems, Applications, Management, and File Systems”. Cisco Press, diciembre 2004.

[3] “IP SAN Best Practices”, Dell, junio de 2010.

[4] IDC: “Worldwide Disk Storage Systems 2008 Vendor Shares: Year in Review”, diciembre de 2009

[5] Meeta Gupta: “Storage Area Networks Fundamentals”. Cisco Press, abril 2002

[6] D. Marshal, W. Reynolds, D. McCrory:“Advanced Server Virtualization: VMware and Microsoft Platforms in the Virtual Data Center”. Auerbach Publications, 2006

[7] T-11 INCITS: “Fiber Channel Backbone 5 (FC-BB-5) Rev 2.0”, junio 2009. Estándar que se encuentra en línea en: http://www.fcoe.com/09-056v5.pdf

[8] Silvano Gai, Claudio DeSanti: “I/O Consolidation in the Data Center”. Cisco Press, septiembre 2009

AUTOMATIZACIÓN DEL DESPLIEGUE DE RECURSOS EN BASE DE DATOS

Francisco Javier Blanco, Rubén Jiménez, Carlos A. Iglesias
Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid
28040
fcojavibr@dit.upm.es, jimmy399@hotmail.com, cif@gsi.dit.upm.es

***Resumen*—En una arquitectura SOA, los servicios presentan dependencias con otros servicios y recursos ya desplegados, necesitando comunicarse con la base de datos para que les provea de información y donde almacenen los datos obtenidos. Una arquitectura telemática que gestione la configuración y el despliegue de tales servicios se hace esencial y dentro de esta, un sistema que gestione los recursos de bases de datos. Las tareas relacionadas con base de datos suponen una actividad ardua y compleja que es realizada de forma manual por administradores especializados. Rompiendo con esta idea y siguiendo la línea de investigación actual, el sistema desarrollado pretende gestionar automáticamente los recursos en el proceso de despliegue dando un soporte integral al DBA, facilitando considerablemente su trabajo y colocándole a un nivel superior de validación y optimización. El sistema se puede separar en dos: una herramienta de generación de unidades de despliegue y otra para realizar el despliegue en base de datos.**

I. INTRODUCCIÓN

Una de las actividades a llevar a cabo durante el desarrollo de aplicaciones empresariales es el despliegue de unidades software funcionales denominados comúnmente servicios. Este despliegue consiste en realizar todas las acciones necesarias para poder poner dichos servicios en funcionamiento. Es habitual que los servicios cooperen entre sí y necesiten de una serie de recursos previamente instalados y disponibles, existiendo dependencias entre estos servicios y otras unidades software en función de los recursos ofertados y los requisitos demandados. Siguiendo esta línea, unos de los recursos más demandados son los relacionados con base de datos ya que pocos servicios ejecutan su función de forma ajena a la información almacenada en el sistema o sin necesitar hacer persistentes los datos computados u obtenidos.

Los recursos de base de datos son unidades software que no realizan ninguna función ni operativa visible al usuario pero son los encargados de manipular la base de datos en dos vertientes: aquellos que tocan la estructura de la base de datos y aquellos que contienen la información y los datos a ser almacenados. Más técnicamente, los primeros se implementan siguiendo el lenguaje DDL, del inglés *Data Definition Language*, permitiendo llevar a cabo tareas de definición de las estructuras que almacenarán los datos. Por lo tanto, estos recursos, llamados a partir de ahora recursos DDL, son desplegados para construir la estructura y el esquema de la base de datos. Los segundos son definidos usando al lenguaje DML, *Data Manipulation Language*, llevando a cabo tareas de manipulación de los datos, organizados por la estructura correspondiente. Estos recursos serán llamados recursos DML a partir de ahora. En este artículo, se va a tratar mayormente el manejo de los recursos DDL pues estos son los recursos más complejos y los más propensos a errores y conflictos sobre la base de datos. El despliegue de los recursos de base de datos sería el proceso íntegro para poner dichos recursos en funcionamiento, es decir, que estén disponibles para los servicios y el resto de unidades software en general. El despliegue supone un procedimiento para situar los recursos en las base de datos correspondientes.

Los recursos de base de datos y más concretamente su despliegue son piezas clave para el funcionamiento de los servicios ya que definen la estructura requerida para el modelado de datos y manipulan los datos que son requerridos por estos. El manejo y gestión de bases de datos, incluyendo el despliegue de recursos, en sistemas de cierto volumen es una tarea ardua y complicada, que requiere que en los proyectos existan personas especializadas únicamente en esta tarea conocidos como administradores de base de datos (DBA). Durante el despliegue, un mínimo fallo, una inserción de datos incoherentes, una ejecución inadecuada puede dejar parte de la base de datos, sino toda, en un estado de error haciendo que servicios dejen de funcionar e incluso provocando que el sistema entero falle. Debido a la importancia de las bases de datos, la cantidad de factores y riesgos a tener en cuenta y la cantidad de actividades primarias y secundarias involucradas hace que el despliegue de los recursos de bases de datos sea una actividad compleja, costosa y realizada desde siempre de forma manual por los DBAs presentando en total un alto coste asociado.

En los últimos años se está investigando en propuestas para que la gestión de la configuración y el despliegue de recursos en base de datos esté más automatizada [1]. El desarrollo de herramientas que faciliten la labor de gestión de base de datos y el manejo de modelos y datos, incluido migración, control, abstracción, transformación, extracción y carga que representan las actividades existentes en los procesos de despliegue, han crecido de gran forma en los últimos años, tal y como se expone en la siguiente sección. El objetivo principal del sistema desarrollado es seguir este nuevo punto de vista de automatización y dar soporte automático al administrador de una forma integral, implementando el proceso completo de despliegue de recursos en bases de datos facilitando el trabajo al DBA y colocándole en un nivel superior de validación y optimización donde sólo ejerza su participación en tareas muy específicas.

ITECBAN (Infraestructura Tecnológica y Metodológica de Soporte para un Core Bancario) es un proyecto de inves-

tigación del programa nacional I+D CENIT cuyo principal objetivo es el desarrollo de una plataforma que sirva como base para la creación de sistemas de gestión destinados al sector bancario, eliminándose las actuales limitaciones de los sistemas de información empleados en entornos financieros. Las aplicaciones empresariales empleadas en este área se caracterizan por presentar en la mayor parte de los casos una arquitectura orientada a servicios [2], lo que las permite adaptarse de manera continua y flexible a los cambios que se producen en su alrededor, en respuesta a la demanda del mercado. Esta arquitectura facilita la interoperabilidad entre sistemas, al definir una manera estándar de anunciar e invocar servicios que pueden actuar de manera independiente. La heterogeneidad y dinamismo de estos servicios hace esencial la creación de un sistema telemático que los gestione incluido su adecuación y estado. Así, surge la necesidad de una solución que facilite el despliegue de los servicios, adecuándolos a las necesidades y características de cada entorno en concreto, lo que ha llevado al desarrollo dentro de un sistema de gestión al objetivo de dar soporte a las operaciones de despliegue y configuración de unidades software sobre los distintos entornos gestionados. Es, dentro de este sistema, donde se incluye el gestor de despliegue específico de los recursos de base de datos.

El resto del artículo se estructura de la siguiente manera. En el capítulo II se realiza un breve estado del arte sobre la gestión automática de los recursos de base de datos incluyendo un análisis de las herramientas existentes de despliegue y migración sobre base de datos exponiendo antes los requisitos del sistema implementado. A continuación, en III se describe en detalle el sistema implementado, centrándose en las dos herramientas que lo componen. En el capítulo IV se explica brevemente implementación final de las dos herramientas en la arquitectura global con sus pruebas finales. Por último, en V se muestran las conclusiones.

II. Gestión automática del despliegue en base de datos

En los últimos años han surgido muchas propuestas y un número considerable de herramientas que conllevan una automatización, o al menos la inclusión de tareas bastante más automatizadas, de gestión y configuración de las bases de datos y del despliegue de los recursos en estas. Según Mateen [3] la escasez de DBA cualificados ha motivado que la industria de las bases de datos desarrolle sistemas de gestión de base de datos automáticos, SGBDA o en inglés ADBMS.

Ahora que la complejidad de los sistemas está alcanzando un nivel que supera las capacidades humanas, con el desarrollo de las tecnologías las personas pueden gestionar tales sistemas complejos de una manera más fiable y eficiente. Con la inclusión de capacidades automáticas, incluso con ideas que parten de la *autonomic computing*, los sistemas crecen en rapidez, eficacia, fiabilidad y precisión con menos o sin interacción humana. Tales capacidades automáticas se pueden implementar en los sistemas de gestión, configuración y despliegue sobre base de datos [4]. La importancia de tales sistemas ha ido creciendo sustancialmente y actualmente existen bastantes herramientas que contemplan actividades sobre base de datos de forma automática o con un nivel de autonomía elevado.

Nuevas capacidades automáticas se están investigando en la gestión de base de datos que la dotarían, en el mayor de los casos, con suficiente inteligencia para ser autosuficientes [5] [6]. Tales características se pueden agrupar en seis áreas: auto-optimización (mejoras del rendimiento, manejo eficiente de recursos, configuración y carga de trabajo), auto-configuración (reconocer los cambios del entorno y reconfigurarse dinámicamente ante ellos), auto-reparación (mantenerse en un estado consistente todo el tiempo), auto-protección (seguridad, mecanismo de auditoría, capacidades de encriptamiento), auto-inspección (realizar decisiones inteligentes basadas en la consciencia que tiene la base de datos de ella misma: recursos, limitaciones, estado, entorno...) y auto-organización (reorganizar y reestructurar dinámicamente el modelo de datos e incluso los índices). Sin embargo, estás capacidades todavia distan de llevarse a cabo en plenitud y se encuentran pocas herramientas que integren de forma completa alguna de estas tareas.

Desde otro punto de vista más real, desde los últimos años existe un amplio abanico de herramientas, que aún siguiendo parte de esas capacidades automáticas, plantean actividades más claras y objetivas. La gran mayoría de las herramientas basan sus tareas automáticas en la gestión, el tratamiento y manejo de los recursos de bases de datos más que en la propia base de datos, refiriéndose a procesos de extracción, transformación y carga (ETL) como herramientas de ayuda a la migración [7] [8] [9]. Las herramientas abarcan áreas como el despliegue [10], la configuración [11], la recuperación [12], la monitorización [13] o el diagnosis de problemas de rendimiento [14]. Estas herramientas desarrollan la perspectiva de las capacidades automáticas pero sobre tareas concretas realizando actividades específicas de valor, dando soporte y facilitando de gran forma el trabajo de los DBA. Es bajo este punto de vista menos teórico donde la industria de las bases de datos ha decidido revolucionar el mercado, sacando una variedad de herramientas que llevan la gestión automática a muchas de las tareas de base de datos.

A. Marco impuesto para el sistema

La arquitectura de configuración y despliegue de ITECBAN debe gestionar correctamente los servicios, en el sentido en el que éstos necesitan recursos de base de datos, estos recursos deben ser gestionados también. Si la arquitectura pretende dar gestión de la forma más automática posible, el despliegue de los recursos debe realizarse siguiendo esta línea y, por lo tanto, siguiendo la línea actual de investigación. Esta actividad de despliegue contiene características automáticas de auto-configuración y de auto-organización, el resto de capacidades se alejan más del sistema implementado.

Según el modelo de configuración y depliegue [15], los recursos de base de datos se tratan como unidades software. Cada unidad software representa una entidad que exporta por sí sola uno o varios recursos, esta unidad es posible que necesite de los recursos exportados por otras unidades como ya se ha dicho. Además, una unidad software es desplegada, o replegada, de una única vez y de forma independiente a las otras, aunque se sigue para salvaguardar las posibles dependencias. Para que las unidades software sean manejadas por la arquitectura global y puedan desplegarse según un mismo patrón, estas deben estar contenidas en una estructura

estandarizada. Esta estructura estandarizada, definida en el modelo citado, se le aplica a una unidad software para ser desplegada pasando a llamarse el conjunto unidad de despliegue. Así, los recursos de bases de datos son paquetizados en una unidad de despliegue, conteniendo los archivos organizados, que será utilizada para desplegar la unidad software, en este caso el modelo de datos o los propios datos, sobre un contenedor software, en este caso una base de datos.

Los componentes desarrollados para la arquitectura siguen un diseño multicapa, con el objetivo de separar en la medida de lo posible las distintas responsabilidades. En concreto, cuenta con un diseño típico de tres capas: capa de presentación que utiliza la capa de lógica de negocio que a su vez se apoya en la capa de persistencia. Para esta interacción se emplea el patrón DAO (Data Access Object), que permite independizar las capas de la tecnología de implementación de la persistencia. Siguiendo este patron, la arquitectura impone la solución ORM (Object-Relational Mapping) que realiza la persistencia apoyándose en una base de datos relacional. De las soluciones ORM, la arquitectura permite utilizar dos tecnologías: JPA, anotaciones directamente en las clases Java, o Hibernate con el uso de archivos de mapeo específicos.

La arquitectura implementa el tratamiento de versiones sobre los servicios. El uso de versiones en los recursos de base de datos se hace necesaria ya que diferentes versiones de aplicaciones pueden necesitar diferentes modelos o datos de la base de datos. Así, aparecen dos conceptos asociados a las versiones que son únicos de base de datos: la desinstalación o vuelta atrás de una versión y la actualización entre versiones. La vuelta atrás, o rollback, necesita del conjunto de sentencias inversas al proceso de instalación para llevar a la base de datos al estado previo antes de la instalación. Es decir, para desinstalar un recurso de base de datos se necesita explícitamente las sentencias inversas a las sentencias que realizan la instalación. La actualización representa el conjunto de sentencias diferencia, es decir, las que llevan de un modelo de datos existente en la base de datos a otro de una versión posterior a ser desplegado con los menores cambios posibles. Lógicamente el conjunto de cambios de la actualización debe ser más reducido que si se eliminara completamente la versión anterior y se instalara de cero la nueva. A nivel DDL, esto también contribuye a que los datos existentes en la base de datos permanezcan tras la actualización de la versión ya que el proceso de destrucción de la versión anterior también elimina todos los datos existentes, si bien es cierto que la existencia de datos puede generar ciertos errores en el proceso de actualización. A través de la Fig. 1 se puede ver de forma fácil el uso de versiones en los recursos.

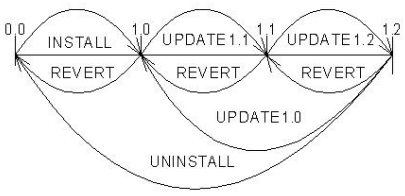


Figura 1: Uso de versiones en los recursos de base de datos

El sistema debe operar sobre un amplio espectro de bases de datos, así como el uso de tecnologías que permitan abstraerse del tipo de base de datos al definir el modelo de esquema. Es decir, el sistema debe dar soporte a múltiples SGBD. Algunas de las razones para tal motivación son que las empresas constantemente están buscando formas de mejorar y de obtener ventajas competitivas. A menudo, estas nuevas oportunidades de mejora pueden repercutir potencialmente en la infraestructura de TI básica de la empresa y requerir la migración de aplicaciones y bases de datos vitales a un entorno nuevo. La capacidad de desplegar un entorno nuevo con rapidez puede reportar considerables beneficios y ventajas a la empresa. La motivación de estas acciones puede ser debida a factores como la pérdida de fe en el proveedor actual, el bajo rendimiento de la plataforma o los elevados gastos de soporte. Ya que la arquitectura implementa el uso de versiones, otro de los objetivos es dotar al sistema de capacidades de control de versiones para poder realizar una navegación sobre ellas, incluido la posibilidad de regresar a una versión anterior conocida en caso de error.

Las actividades que demanda el marco impuesto para realizar el proceso íntegro de despliegue automático de recursos de base de datos encajan en un primer proceso que genere la unidad de despliegue y otro que realice el despliegue. Estos dos procesos se adecuan a las herramientas de ETL, extracción-carga-transformación, como procesos responsables del transporte, control e integración de datos de uno o más sistemas fuentes a uno o más sistemas destino, que contienen actividades de migración y de ejecución sobre bases de datos. La idea es que una aplicación ETL lea los datos primarios, realice su transformación o migración sobre un procesamiento cualitativo, abstrayéndose lo máximo posible de las bases de datos específicas, y al final cargue estos datos tratados en el almacén para que estén disponibles por los servicios.

B. Análisis de herramientas de despliegue y migración

Se ha hecho un análisis de las herramientas existentes que ofrecen procesos ETL y de migración de base de datos. Estas son las herramientas más importantes:

- Ruby on Rails[1]: para facilitar la administración de la DB, Rails pone a disposición las migraciones, que se pueden definir como clases de Ruby destinadas a la modificación del esquema de la base de datos. Rails contiene clases de migración que realizan operaciones de creación o de destrucción, permitiendo además mantener un control de versiones.
- CloverETL[2]: framework Java que puede ser utilizado para la transformación de datos estructurados. Las transformaciones están definidas en forma de gráfico que contiene descripciones metadata, secuencias, conexiones, componentes de transformación... Los metadatos pueden ser definidos, entre otras, automáticamente basándose en la estructura de una base de datos o con consultas SQL. El usuario selecciona de una paleta de componentes existentes y los coloca en una hoja de trabajo, luego los conecta a través de un gráfico de transformación. La representación gráfica es entonces traducida automáticamente por cloverGUI en código

[1] http://www.rubyonrails.org.es/
[2] http://www.cloveretl.com/

XML que posteriormente es ejecutado por el motor cloverETL.

- Enhydra Octopus[3]: herramienta basada en Java. Se puede conectar a cualquier fuente de datos JDBC y realizar transformaciones que se definen en un archivo XML. El modelo de datos DODS (Data Object Design Studio) es soportado generando identificadores para los nuevos objetos. Este modelo de datos es utilizado por Enhydra DODS, herramienta ligera de mapeo que soporta objetos relacionales persistentes para diferentes bases de datos. Se proporciona un generador de esquemas, e incluso archivos DODS, de una base de datos existente.
- Liquibase[4]: herramienta de software libre que se puede emplear para refactorizar bases de datos, es decir, resuelve el problema habitual de cómo sincronizar la información que se encuentra en diferentes bases de datos. Su funcionamiento se basa en crear un archivo XML que define los cambios que se han producido en la estructura y en la información de una base de datos respecto de otra. Liquibase proporciona una serie de funcionalidades: actualización de la base de datos, generación de rollback automático, validación base de datos, generación de documentación de BD...
- Pentaho Data Integration[5]: componente responsable de los procesos de ETL. Es la herramienta ETL más popular de código abierto disponible. PDI soporta una amplia gama de entrada y salida de formatos, incluyendo archivos de texto, hojas de datos y motores de bases de datos comerciales y libres. La capacidad de transformación de PDI le permite manipular los datos con muy pocas limitaciones. PDI es fácil de usar, cada proceso es creado con una herramienta gráfica donde se especifica qué hacer sin tener que escribir código. Posee una arquitectura escalable basada en plugins. PDI realiza además migración de datos entre bases de datos, exportación de datos a archivos planos, carga de datos de forma masiva, limpieza de datos, integración de aplicaciones y permite la definición de conjuntos de procesos referidos como ETTL.
- Talend Open Studio[6]: una potente solución que proporciona las capacidades de integración de datos avanzados. Su interfaz gráfica cuenta con numerosos componentes para el modelado del proceso de negocio, así como implementaciones técnicas para extraer, transformar y mapear flujos de datos. Posee una amplia escalabilidad al poderse realizar nuevos componentes para integrarlos con el sistema. Incluye funcionalidades interesantes como estar totalmente integrado con Eclipse, hacer transformaciones y mappings complejos, tener mecanismos de debugging y control sobre los procesos realizados, varios wizards para ayudar en todo el proceso, etc.
- Glashfish ESB: servidor de aplicaciones que implementa las tecnologías definidas en la plataforma Java EE. Posee dos subproyectos con capacidades de ETL, el más importante es:
  - OpenESB (ETLSE)[7]: dentro de esta plataforma existe una herramienta de integración de datos (ETLSE) que pueden utilizarse en los procesos ETL ya sea para construir almacenes de datos o migrarlos. ETLSE está diseñado para organizar y gestionar grandes volúmenes de datos, con transformaciones de alto rendimiento dentro de los niveles de SOA. Es un módulo empresarial optimizado para los procesos de ETL entre archivos y bases de datos. Soporta operadores de limpieza de datos para mantener la integridad de los datos. Para garantizar la calidad de los datos, ETL Integrator permite al usuario configurar la lógica de validación de datos. Su capacidad de procesamiento concurrente/paralelo permite manejar diferentes flujos de datos.
- Otras herramientas analizadas, que se omiten en la comparativa posterior debido a que sus características son englobadas en las anteriores, son Migrate4j (herramienta flexible de migración Java que pueden aplicarse a diferentes motores a la vez), Scriptella (herramienta ligera ETL con ejecución de scripts que se utilizan para actualizarse entre versiones), OpenDBCopy (utilidad de base de datos universal destinada a la migración basado en plugins que pueden encadenarse), KETL (plataforma de integración en Java como servidor multi-threaded que gestiona diversas tareas), Jitterbit (poderosa herramienta de ETL basado en operaciones sobre una GUI, incluido *drag and drop*), JasperETL (plataforma Open Source de Business Intelligence que incluye herramienta ETL con interfaz), Pentaho Data Integration (herramienta ETL más popular de código abierto disponible, cada proceso es creado con una herramienta gráfica sin tener que escribir código, poseyendo una arquitectura escalable basada en plugins), Apatar (innovadora y potente suite de herramientas de software diseñado para proporcionar beneficios de productividad a las organizaciones que necesitan mover datos de diferentes fuentes) y Mural (comunidad de código abierto con el fin de desarrollar un "ecosistema" de productos que solucionen los problemas de *Master Data Management*).

C. Comparativa

En la Fig. 2 se representa una tabla en la que se exponen las características más esenciales de las herramientas ETL. Se puede observar en las tablas características tales como los diversos modos de ejecución, control de versiones, el lenguaje de transformación, seguridad, si poseen interfaz gráfico, capacidad de generar documentación y monitorización. Se omiten datos referentes a la conectividad ofrecida pues todas las herramientas, aun con alguna diferencia, soportan las principales bases de datos.

D. Selección

La selección se realizó pensando en una herramienta de migración de bases de datos que debía integrarse en la arquitectura de configuración y despliegue. Además se deseaba que las migraciones o cambios realizados estuvieran gestionados

[3] http://www.enhydra.org/tech/octopus/index.html
[4] http://www.liquibase.org/
[5] http://kettle.pentaho.org/
[6] http://es.talend.com/index.php
[7] http://wiki.open-esb.java.net/Wiki.jsp?page=ETLSE

	Herramientas				Suites		
Nombre del producto	*Ruby*	*Octopus*	*CloverETL*	*Liquibase*	*TOS*	*KETTLE*	*Open ESB*
Control de Versiones							
• Por TAG	No	No	No	Si	No	No	No
• Por hora/fecha	No	No	No	Si	No	No	No
• Por últimos x cambios	No	No	No	Si	No	No	No
• Por nº de migración	Si	No	No	No	No	No	No
Lenguaje de Transformación							
• Java	No	No	Si	No	Si	No	No
• JavaScript	No	Si	No	No	No	No	No
• Ruby	Si	No	No	No	No	No	No
• XML	No	Si	Si	Si	No	No	No
• SQL	No	No	No	Si	No	No	No
• Perl	No	No	No	No	Si	No	No
• Gráfico. Librería de transformaciones	No	No	No	No	Si	Si	Si
Seguridad							
• Apache Commons logging	No	No	Si	No	No	No	No
GUI	No	No	Si. Clover.GUI	Si	Si	Si. Spoon	Si
Genera Documentación	No	No	No	Si	No	No	No
Validación de BD	No	No	No	No	Si. Mediante operaciones	Si. Mediante operaciones	Si. Mediante operaciones
Monitorización	No	No	No	No	No	Si. Herramienta Carte, remoto.	Si. ETL monitor

Figura 2: Tabla características herramientas ETL

de forma eficiente. Los motivos de ello eran mantener el control sobre las acciones llevadas a cabo y para poder deshacer de una forma sencilla las acciones realizadas. Teniendo en cuenta la tabla anterior y los requisitos brevemente descritos se seleccionó la herramienta Liquibase por sus capacidades de rastreo, gestión y aplicación de cambios en la base de datos. Otros motivos de la elección fueron principalmente:

- Su gran capacidad de integración con otros frameworks y entornos de desarrollo.
- Una amplia capacidad de gestión de versiones, que supera a la de Rails, con funciones adicionales.
- Es capaz de generar documentación asociada a los cambios a realizar, teniendo control sobre las acciones que se han tomado.
- Conexión con una amplia variedad de fuentes.
- Utiliza las capacidades de Hibernate para validar bases de datos, así como recrear el esquema de una base de datos.
- Retroceso de los cambios realizados, automáticamente genera las sentencias inversas necesarias.
- Realizar cambios que no han sido realizados con Liquibase. Genera automáticamente un informe para actualizar la base de datos, comparando una base de datos existente con archivos de mapeo Hibernate.
- Proporciona gran capacidad de acoplamiento en sistemas de despliegue. Con un único fichero de cambio puede generar los cambios en múltiples bases de datos.

III. Sistema implementado

El sistema implementado gestiona todo el proceso de manipulación y despliegue de los recursos de base de datos en la arquitectura. Los desarrolladores basan el funcionamiento de los servicios a desarrollar en la existencia de información almacenada en la base de datos. Dicha información está estructurada según un modelo de datos que es definido por el propio desarrollador o un analista siguiendo una serie de requisitos impuestos. Este modelo de datos representa un recurso DDL que será desplegado en las bases de datos para que los servicios correspondientes funcionen. Los servicios frecuentemente necesitan de datos existentes en la base de datos por lo que el despliegue de recursos DML es también parte del sistema.

El despliegue de estos recursos de base de datos en toda la arquitectura ITECBAN sigue siempre el mismo procedimiento. Este procedimiento es definido con una metología sencilla de dos pasos que se ejecutan de forma consecuente. Cada uno de los pasos define una tarea a realizar, que de forma general son explicadas en esta misma sección. Es decir, que estas dos tareas componen la metodología para desplegar los recursos de base de datos en la arquitectura de una forma automatizada.

Los recursos DDL suelen definirse, para mayor facilidad para el desarrollador, en un nivel más abstracto del que entiende el manejador de base de datos que, como se ha dicho, por requisitos de la arquitectura son las tecnologías JPA e Hibernate. Así, la primera tarea del sistema es la de traducir ese lenguaje abstracto en el que el desarrollador ha definido el modelo a un lenguaje entendible por la base de datos; además, toda la información, tanto la traducida como la previa, es encapsulada en una unidad de despliegue, paquete con una estructura estandarizada, para que sea entendida por la arquitectura global.

La siguiente tarea es, de forma consecuente, el despliegue de los recursos en la base de datos. Se ha implementado una herramienta encargada de coger la unidad de despliegue adecuada, analizarla y coger las sentencias en un lenguaje entendible por la base de datos y ejecutarlas sobre esta en función de una serie de propiedades o parámetros dados. Debido al dinamismo existente de los servicios Web, la arquitectura permite el desarrollo de los recursos en versiones asociadas a las unidades aumentando con ello la complejidad de los sucesivos despliegues.

El sistema se compone, por lo tanto, de dos herramientas que realizan respectivamente cada una de las dos tareas secuenciales. La primera consiste en la generación de la información sobre un paquete estructurado y la segunda es la que se encarga de desplegar los paquetes en la base de datos. Estas herramientas están implementadas sobre scripts Ant como consecución de múltiples tareas, entre ellas cabe

destacar las tareas que utilizan la herramienta Liquibase.

A. Herramienta de creación de unidades de despliegue

Liquibase no soporta directamente la transformación de clases anotadas por lo que se debe incluir para este caso una tarea intermedia proporcionada por Hibernate para traducir el conjunto de clases anotadas a un conjunto de archivos de mapeo. Sobre estos archivos de mapeo, Liquibase los traduce a su lenguaje específico, independiente del SGBD.

Debido a la importancia de las bases de datos es necesario tener asegurado que todo lo que se ejecute contra una base de datos esté validado. Además puede ser necesaria la modificación de algunos atributos del modelo de datos obtenido del desarrollo de la aplicación. Esto también puede venir impuesto por las limitaciones del SGBD concreto, por ejemplo, existen diferencia en la longitud máxima del nombre de las tablas entre diferentes SGBD y algunos nombres pueden resultar excesivamente largos. Por ello es necesario que el DBA se encargue de validar las unidades de despliegue. Además, las sentencias generadas pueden ser optimizadas debido a la experiencia del propio DBA y a su conocimiento específico de toda la arquitectura y de la base de datos en concreto, siendo este un proceso clave cuando el volumen de información sea muy elevado.

El problema surge en que, en un principio, Liquibase ha creado un fichero con su lenguaje específico, este lenguaje no supone ningún estándar y no suele ser entendido por los DBA, además de que se queda a un nivel de abstracción superior al que entiende el SGBD y por lo tanto si un DBA validara el archivo en ese lenguaje no estaría 100 % seguro de que se fuera a ejecutar todo correctamente ni optimizado. Así, Liquibase presenta la funcionalidad de traducir las sentencias a lenguaje SQL, que es el lenguaje por antonomasia que domina las bases de datos. El problema de SQL es que tiene sentencias que son específicas de cada SGBD. En el presente sistema, se almacenarán las sentencias en lenguaje Liquibase y en los scripts SQL para los SGBD que se necesiten (generalmente sólo uno), si más adelante se requieren otros SGBD se traducirán desde el lenguaje Liquibase. El DBA necesita validar cada script SQL creado para cada SGBD.

La herramienta genera de forma automática desde los archivos de persistencia una unidad de despliegue que contiene una estructura formalizada con el archivo en lenguaje Liquibase y los scripts SQL para cada uno de los SGBD. Liquibase generara no sólo el script SQL con las sentencias a ejecutar en la base de datos, script de instalación, sino el script SQL de rollback que contiene las sentencias inversas para eliminar esas acciones una vez ejecutadas en la base de datos.

Liquibase es capaz de generar el script SQL de actualización que supone la diferencia entre los archivos de persistencia de la nueva versión (del que surge el script de instalación) y la estructura de datos existente en la base de datos que supone una versión anterior. También es capaz de generar el script SQL de rollback de dicha actualización conteniendo las sentencias inversas que llevarán desde la nueva versión a la anterior.

Además, la herramienta es capaz de generar la documentación asociada a dichos scripts conteniendo información referente al estado actual de la base de datos y a los cambios que realizarán estos scripts. En la Fig. 3 muestra el funcionamiento más específico de esta herramienta con los archivos que genera.

La herramienta también debe generar un descriptor de la unidad de despliegue que corresponde con un archivo XML que sigue un formato entendible por la arquitectura de configuración y despliegue. Este descriptor define un modelo estándar con información relativa a la propia unidad: tipo de unidad, nombre, versión...

Por último, la herramienta presenta un proceso de modificación de los archivos generados por Liquibase debido a que éste algunas veces genera errores fácilmente detectables y modificables por un patrón. Así, este proceso permite definir un patrón de coincidencia para borrar o reemplazar dichos errores de una forma automática y cómoda. El proceso es representado en la Fig. 3 por el nombre Sql transform.

B. Herramienta de despliegue en base de datos

La arquitectura de configuración y despliegue ha de presentar las herramientas suficientes para desplegar cualquier tipo de unidad sobre cualquier tipo de contenedor. Específicamente, la herramienta implementada ejecuta las instrucciones necesarias para realizar las operaciones demandadas sobre los recursos DDL o DML en un contenedor del tipo base de datos. La arquitectura define para realizar el despliegue de unidades un plan de despliegue [16] que contiene una serie de actividades. Cada actividad representa una operación a realizar sobre una unidad de despliegue. Las operaciones permitidas sobre los recursos de bases de datos son: instalación (se instala un recurso con la versión indicada en la base de datos), desinstalación (se elimina completamente un recurso de la base de datos), actualización (se despliega un recurso con cierta versión basándose en una versión anterior ya desplegada) y desactualización (se lleva un recurso con cierta versión ya desplegado a una versión anterior).

Cada una de estas cuatro operaciones presentan scripts diferentes creados a lo largo del proceso de generación de la unidad de despliegue. La arquitectura mira cada actividad del plan de despliegue y coge la unidad de despliegue específica. Si la unidad es de base de datos, entonces llama a esta herramienta pasándole el contenido de la unidad, la operación a realizar y el contenedor de base de datos donde se ha de desplegar. Esta herramienta, de forma básica, establece la comunicación con la base de datos y ejecuta los scripts SQL contenidos en la unidad que representan la operación indicada.

La herramienta apoyándose en Liquibase es capaz de llevar un control de versiones de unidades desplegadas en base de datos. Cada vez que realiza una operación en base de datos añade una línea indicando la unidad desplegada, la operación, la versión en la que queda dicho recurso, el cheksum (hashing de los scripts ejecutados) y la fecha en la que se ejecutó. Si una operación se vuelve a repetir, la fecha se actualizará en la tabla de control.

La herramienta necesita de una serie de parámetros para realizar el despliegue en la base de datos: usuario y contraseña, url, tipo de SGDB... Estos parámetros son recogidos bien del archivo de propiedades que es definido en el modelo asociado al contenedor de base de datos o del descriptor existente en la unidad de despliegue. Como parámetros específicos

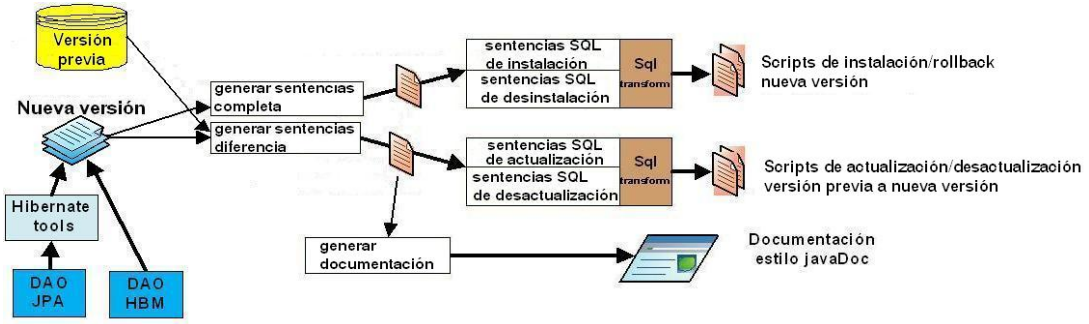


Figura 3: Funcionamiento de la herramienta de generación de unidades de despliegue

de la herramienta que configuran nuevas funcionalidades se encuentran dos. La primera, es la posibilidad de no ejecución de scripts modificados, si los scripts de una unidad de despliegue son modificados y cierta operación sobre esa unidad de despliegue ha sido realizada con anterioridad, al querer realizar el despliegue se comprueba la tabla de control de versiones, y al comparar los cheksums podrá impedir la ejecución de la operación. La segunda funcionalidad, es la elección del despliegue en modo transaccional o no, entendiendo una transacción como la capacidad que tiene la base de datos de hacer rollback automático si ocurre un error. A veces, las sentencias que se han ejecutado no tiene sentido darles vuelta atrás simplemente porque uno de las sentencias falle ya que la base de datos permanece en un estado correcto y es una pérdida de tiempo tener que hacer rollback automático de las sentencias ya ejecutadas para volverlos a ejecutar.

C. Mejoras en Liquibase

Liquibase aporta una gran funcionalidad a la gestión automática de tareas en base de datos y es una herramienta excelente para manejar muchos de los procesos a llevar a cabo. Pero como cualquier herramienta que no tenga demasiado tiempo de vida presenta fallos y errores, y más si se trata de software libre, por lo que para dar pleno rendimiento, ajustarse a la arquitectura y realizar las tareas previstas ha sido necesario solucionar errores y solventar ciertas deficiencias que presentaba esta herramienta. Todos estos cambios están en proceso de análisis dentro de la comunidad Liquibase para ser implementados de forma oficial. Siendo una herramienta de software libre, la obtención de todo su código es inmediata y siendo una comunidad muy abierta cualquier duda o problema que surgió era contestada de una forma eficaz por los desarrolladores más expertos.

Tres son las aportaciones principales al código:

- Mejora de los tipos de datos predeterminados desde Hibernate. Los archivos de persistencia presentan el modelo de datos siendo para ello necesario especificar el tipo de datos de cada elemento a representar. Para que quede bien definido el modelo, el correcto manejo de los tipos de datos es un punto clave. Uno de los problemas que tiene Liquibase es que la conversión de ciertos tipos de datos expuestos en los archivos de persistencia eran transformados incorrectamente a formato SQL y otros que aún transformándose correctamente a formato SQL entendible por el SGBD lo hacía con una precisión y escala en desacorde a lo que realmente representaba ese tipo de datos. Por este motivo, se ha decidido modificar el código para solucionar estos problemas de conversión.
- Cambios inversos a operaciones eliminatorias. Liquibase no es capaz de generar las sentencias SQL a cambios destructivos en la base de datos (acciones drop, alter drop/modify) en los scripts. Se añade esta funcionalidad, sacando la información del modelo de datos de la foto actual de la base de datos con lo que se pueden llenar los campos necesarios para generar las operaciones aditivas, es decir, las inversas a las destructivas.
- Soporte a modificación en los tipos de datos. La funcionalidad de modificar las columnas de las tablas se incluye en el cambio anterior pero hay que hacer más cambios para soportar las modificaciones en los tipos de datos. Primero se ha de definir la comparación entre los datos obtenidos desde el controlador de la base de datos y los datos generados desde los archivos de persistencia. Una vez se crea una tabla de sinónimos se extiende la comparación a la escala, longitud y precisión.

IV. Implementación y pruebas finales

La herramienta de generación de unidades de despliegue queda con un script Ant al que se le pasa los archivos de persistencia y crea la unidad de despliegue en la ruta elegida. Dicha unidad de despliegue es subida al repositorio de unidades.

La herramienta de despliegue en base de datos ha sido empaquetada en un bundle de OSGi. En el archivo de configuración se indica que exporta un servicio OSGi para ser utilizado por cualquier otro módulo de la arquitectura ITECBAN. El servicio exportado lanza las tareas Ant de la herramienta tras pasarle la operación a realizar, la unidad de despliegue y las propiedades de la base de datos. Para la integración en la arquitectura de despliegue, se añade un servlet configurado en Spring MVC que contiene el controlador que, tras mirar el plan de despliegue seleccionado y para las actividades de despliegue en base de datos, enlaza con el servicio implementado para que se encargue del despliegue una vez le pase los datos necesarios y permitiendo la visualización del proceso en la consecución de sucesivas páginas web. La Fig. 4 visualiza el resultado del despliegue de uno de los escenarios.

Las pruebas en esta parte han sido las correspondientes a cinco escenarios. La idea era crear un recurso DDL con dos versiones consecutivas y un recurso DML. Los recursos DDL fueron creados a partir de archivos de persistencia necesarios para llevar a cabo una aplicación financiera relacionada con

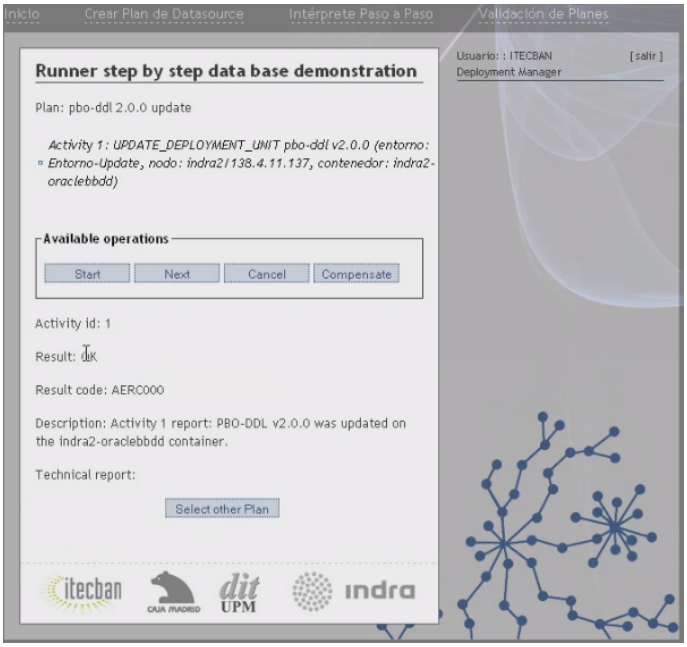


Figura 4: resultado del despliegue de un recurso sobre un contenedor de base de datos

la gestión de hipotecas. Las unidades de despliegue generadas fueron almacenadas en el repositorio real utilizado en la arquitectura. Las operaciones de despliegue, una por escenario, fueron instalación de un recurso DDL, carga de datos (DML), actualización de un recurso DDL, desactualización de un recurso DDL y desinstalación de un recurso DDL.

V. Conclusiones

Una actividad fundamental en una arquitectura SOA es el despliegue de servicios siendo conscientes de que para su funcionamiento existen dependencias con otros servicios y una serie de recursos ya desplegados. En el sentido de que todos los servicios necesitan comunicarse con la base de datos para coger y hacer persistente información del entorno, los recursos más demandados son los de bases de datos. Estos recursos son, por tanto, una pieza clave y su despliegue es una actividad compleja, costosa y realizada de forma manual por gente especializada presentando un alto coste asociado.

Dentro del proyecto ITECBAN surge la necesidad de facilitar el despliegue de sistemas del sector bancario. El proyecto implementa una arquitectura de configuración y despliegue, dentro de la cual se encuentra nuestro gestor específico de base de datos cuyo objetivo es gestionar de una forma automatizada todo el proceso de manipulación de los recursos de base de datos.

Siguiendo las líneas actuales que intentan encontrar métodos automáticos para las tareas en bases de datos, el sistema se basa en dos herramientas principales que intentan automatizar lo máximo posible las operaciones a realizar sobre la arquitectura de configuración y despliegue, ayudando en gran medida al DBA. La primera herramienta consiste en la generación de unidades de despliegue de base de datos desde archivos de persistencia conteniendo los scripts SQL a ser validados por el DBA y que serán desplegados, según la operación definida en la actividad planificada, por la segunda herramienta, añadiendo ésta un control de versiones.

Realizando un extenso análisis de las herramientas existentes de migración y de ETL, el sistema desarrollado se ha basado en Liquibase, solucionando ciertos errores y añadiendo cierta funcionalidad de tal forma que se ha adaptado el software libre existente y los cambios han sido ofrecidos de vuelta a la comunidad.

El sistema, conformado por las dos herramientas, se adecua a los objetivos de la arquitectura de configuración y despliegue que, a través de una metodología sencilla de dos pasos, realiza las tareas secuenciales para desplegar los recursos de base de datos en un ambiente automático.

Agradecimientos

Nos gustaría mostrar nuestro agradecimiento al Gobierno de España, por la financiación del proyecto ITECBAN (MITYC CDTI-CENIT 2005) a través del Ministerio de Industria, Turismo y Comercio.

Referencias

[1] S. Elnaffar, W. Powley, D. G. Benoit, and T. P. Martin, "Today's DBMSs: How autonomic are they?" in *DEXA Workshops*. IEEE Computer Society, 2003, pp. 651–655.

[2] S. Hashimi, "Service-Oriented Architecture Explained," O'Reilly Media, Inc., 2003. [Online]. Available: {http://ondotnet.com/pub/a/dotnet/2003/08/18/soaexplained.html}

[3] A. Mateen, B. Raza, T. Hussain, and M. Awais, "Autonomic computing in sql server," in *ICIS '08*. Washington, DC: IEEE Computer Society, 2008, pp. 113–118.

[4] B. Raza, A. Mateen, T. Hussain, and M. Awais, "Autonomic success in database management systems," *Computer and Information Science, ACIS*, vol. 0, pp. 439–444, 2009.

[5] M. Parashar and S. Hariri, "Autonomic computing: An overview," in *Unconventional Programming Paradigms*. Springer Verlag, 2005, pp. 247–259.

[6] IBM White Paper, "Practical Autonomic Computing: Roadmap to Self Managing Technology," 2006.

[7] X. Zhang, W. Sun, W. Wang, Y. Feng, and B. Shi, "Generating Incremental ETL Processes Automatically," in *IMSCCS '06*, vol. 2, june 2006, pp. 516 –521.

[8] T. Jörg and S. Dessloch, "Towards generating etl processes for incremental loading," in *IDEAS '08*. New York, NY, USA: ACM, 2008, pp. 101–110.

[9] M. Hernandez, L. Popa, H. Ho, and F. Naumann, "Clio: A schema mapping tool for information integration," in *ISPAN '05*. Washington, DC, USA: IEEE Computer Society, 2005, p. 11.

[10] Y. Wang, "DB2 query parallelism: Staging and implementation," in *21st VLDB Conference*, 1995, pp. 686–691. [Online]. Available: http://www.vldb.org/dblp/db/conf/vldb/Wang95.html

[11] K. Eva, L. Sam, S. Berni, S. Adam, W. Leanne, "Automatic Database Configuration for DB2 Universal Database: Compressing Years of Performance Expertise into Seconds of Execution," IBM Journal Paper, 2002.

[12] S. S. Lightstone, G. Lohman, and D. Zilio, "Toward autonomic computing with DB2 universal database," *SIGMOD Rec.*, vol. 31, no. 3, pp. 55–61, 2002.

[13] Steven Warren, "SQL Server Performance Monitor," Database Journal, 2005.

[14] D. G. Benoit, "Automatic diagnosis of performance problems in database management systems," in *ICAC '05*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 326–327.

[15] F. Cuadrado and J.C. Dueñas and R. García and J.L. Ruiz, "A Model for Enabling Context-Adapted Deployment and Configuration Operations for the Banking Environment," *Networking and Services Conference*, vol. 0, pp. 13–18, 2009.

[16] F. J. Blanco, L. D. Casillas, and M. Garijo, "A Knowledge-based System for the Validation of the Deployment of Software Units," in *ICAART (1)*, 2010, pp. 305–310.

Videoconferencia con Isabel en la Web 2.0

Fernando Escribano, Javier Cerviño, Pedro Rodríguez, Joaquín Salvachúa
Departamento de Ingeniería de Sistemas Telemáticos,
Universidad Politécnica de Madrid
Avda. Complutense, Ciudad Universitaria s/n, 28040 - Madrid, España.
{fec, jcervino, prodriguez, jsalvachua}@dit.upm.es

***Resumen*- Este artículo presenta una arquitectura que transforma una aplicación tradicional de videoconferencia en un servicio Web accesible desde cualquier navegador, de tal forma que cambia el modelo de uso y propone un nuevo sistema de colaboración en tiempo real que cuenta con las ventajas intrínsecas de cualquier servicio de la web 2.0. Además esta solución facilita la transición hacia un servicio típico de Cloud Computing en el que se utilizan y se liberan recursos de videoconferencia dependiendo de la demanda en cada momento.**

***Palabras Clave*- Videoconferencia, Colaboración, Web, Cloud Computing.**

I. INTRODUCCIÓN

En los últimos años se ha cambiado la filosofía de las aplicaciones que los usuarios utilizan. De tener aplicaciones instaladas en su ordenador se utilizan aplicaciones basadas en el navegador. Este nuevo escenario tiene algunas ventajas, como eliminar problemas de instalación, versionado y configuración. Por otra parte abstrae a los desarrolladores de características del sistema operativo y plataforma sobre la que se ejecuta.

Este tipo de aplicaciones web altamente interactivas se han venido a llamar RIA (*Rich Internet Applications [1]*). Este paradigma está creciendo en uso y aceptación por parte de los usuarios ya que acceden a estas aplicaciones desde cualquier dispositivo con la necesaria conexión a la red. Uno de sus principales problemas es qué hacer cuando no hay conexión. Se está trabajando en esta línea, pero estamos habituados a la conexión permanente.

En nuestro caso nos plantamos como se puede realizar un sistema de comunicación multimedia altamente interactivo dentro de una plataforma RIA. Anteriores experiencias, como Marte [2], nos había permitido conocer que algunas tecnologías tales como Adobe Flash [3] permite un acceso a los diversos recursos multimedia del ordenador desde el navegador.

En este artículo presentamos la arquitectura híbrida que permite la integración entre múltiples tecnologías de una forma flexible que da una visión perfectamente integrada. Es necesario destacar que la mayor complejidad está en la interoperabilidad a nivel de control, ya que la interoperabilidad de los códecs de audio y video es un problema técnico resuelto con relativamente poca complejidad conceptual.

La mayor dificultad está en ver qué modelo de uso existe detrás de dichas aplicaciones multimedia distribuidas; o como en el caso de Isabel dicho modelo es reprogramable al vuelo. Las arquitecturas basadas en diversas pasarelas no sólo de multimedia sino incluso de paradigma de uso aislando y adaptando cada metáfora y caso de uso en las diversas plataformas integradas. No tiene ningún sentido el forzar que dichos casos de uso se implementen donde no son adecuados, como puede ser los teléfonos SIP.

Por otra parte la arquitectura aquí presentada nos abre la puerta a sistemas de tipo *Cloud Computing* [4] donde la videoconferencia sea un servicio disponible que los usuarios son capaces de usar de manera totalmente transparente permitiendo la *Collaboration as a Service*.

Creemos que la solución arquitectónica, usando el patrón del mediador y de las *facade*, es lo suficientemente general como para ser aplicada a cualquier arquitectura multimedia actual. Creemos que es una contribución importante, no existente anteriormente, para la evolución de la actual Web 2.0 a un internet de tiempo real y de las cosas.

A lo largo del artículo vamos a ver por este orden la aplicación Isabel [5], que es sobre la que creamos una pasarela que permite la evolución hacia un servicio Web. A partir de ahí empezaremos a describir las piezas básicas de la pasarela, desde las librerías en las que se basa (GAPI) hasta la arquitectura de los diferentes componentes y sus funciones. En el siguiente apartado explicaremos las pruebas y los principales problemas a los que nos enfrentamos durante el desarrollo y terminaremos comentando diversas conclusiones del trabajo.

II. LA APLICACIÓN ISABEL

Isabel es una herramienta de colaboración multimedia y multipunto que, mediante un innovador concepto de servicio denominado escenario flexible, permite que la colaboración remota sea los más parecida posible a la presencial. Esto se consigue basándose en dos ideas básicas:

- Protocolos sociales: La gestión del escenario de colaboración se realiza de acuerdo a las convenciones que rigen una determinada actividad presencial. Por tanto si en una clase es el profesor el que controla las actividades en el aula, también será el profesor el que determine la interacción durante una clase distribuida con Isabel.
- Producción multimedia distribuida: La vista de todos los participantes es la misma para todos e integra tanto los videos activos en ese momento como las herramientas de colaboración correspondientes a la actividad que se desarrolle. Por ejemplo durante una clase se podría mostrar el video del profesor en una posición principal, los videos de los alumnos en segundo plano, una presentación de transparencias y un panel que indica si algún alumno ha "levantado la mano" para hacer una pregunta.

En el escenario flexible de Isabel se han introducido tres servicios diferentes que permiten realizar tres clases de reuniones tal y como se detalla a continuación:

• Congresos distribuidos: realizados con varios auditorios interconectados con Isabel, donde los ponentes, presidentes de mesa o asistentes pueden participar desde cualquiera de ellos. En este servicio el control está centralizado y los modos de interacción son seleccionados desde una sala de control de acuerdo al programa de la conferencia.

• Clases distribuidas: realizadas con profesores y alumnos que participan desde diferentes sedes. Este servicio está diseñado para mantener un control estricto por parte del profesor, permitiéndole hacer presentaciones, charlas, etc... El educador también puede dar la palabra a cualquier sitio en cualquier momento.

• Reuniones de trabajo distribuidas: para la coordinación de proyectos u otras actividades interconectando personas o salas pequeñas mediante Isabel. En este servicio no hay control centralizado, sino que todos los participantes pueden tomar el control.

III. ISABEL GAPI

La pasarela genérica de Isabel, también conocida como GAPI (Gateway API), es un módulo de pasarela genérico desarrollado con el fin dar servicio a pasarelas hacia protocolos específicos (SIP, H323,...), de manera que la parte común a todas las pasarelas se encuentre en un único paquete y pueda ser reutilizado de manera simple y rápida. GAPI ha sido desarrollada como paquete Java [6] y ofrece las funcionalidades más comunes que puede necesitar una pasarela mediante un API simple y bien definido. La Fig. 1 muestra esta arquitectura.

La función principal del GAPI es el manejo del protocolo de señalización de Isabel que se ofrece al programador de pasarelas a través de una serie de interfaces sencillas en Java. De esta forma se permite la conexión y desconexión de usuarios a la sesión, el control de los modos de interacción y la solicitud de turno de preguntas en los modos en los que está disponible. Así mismo el GAPI informa mediante callbacks a los GAPIListeners de conexiones y desconexiones de usuarios, cambios de modo de interacción y de los flujos multimedia activos.

Por otro lado, para la gestión de los flujos multimedia, el GAPI controla una MCU que distribuye los diferentes flujos RTP de los clientes de la pasarela hacia el componente de multicast a nivel de aplicación de Isabel y de éste hacia los clientes de la pasarela.

IV. PASARELA WEB

A. Arquitectura General

El objetivo de este apartado es dar una visión general de cada una de las partes que servirá como introducción a la siguiente parte del artículo donde se entrará en detalle sobre cada una de los componentes.

En primer lugar tenemos el mundo Isabel. Como se ha explicado anteriormente, Isabel es una aplicación de videoconferencia que utiliza su propio protocolo de control sobre UDP mientras que los diferentes flujos se transmiten utilizando el protocolo RTP [7]. Por otro lado, tenemos el mundo Flash en el que la transmisión tanto de mensajes de control como de flujos multimedia se realiza mediante el protocolo RTMP [8].

Es, por tanto, labor de la pasarela traducir los tanto el control de la videoconferencia como los datos de audio y vídeo en ambos sentidos para que la comunicación entre los dos sistemas sea posible.

Además, Isabel tiene su propio mecanismo de redistribución de flujos entre pares, en el mundo Flash, para una comunicación multipunto es necesario disponer de un servidor central que se encargará de distribuir los diferentes mensajes y flujos entre los clientes. Para este desarrollo se ha decidido utilizar Red5 [9].

Finalmente, se considera parte del desarrollo de la pasarela el diseño e implementación de la aplicación Flash que correrá en los navegadores de los clientes. Como veremos, esta aplicación tiene que cumplir ciertos requisitos impuestos por Isabel, así como tratar correctamente los flujos según su proveniencia (pasarela o resto de los clientes).

Todo esto queda de manifiesto en la Fig. 2, donde vemos cada uno de los grandes componentes de la pasarela y su comunicación con Isabel a nivel de protocolos.

B. Arquitectura de la pasarela Isabel

En Fig. 3 se muestra la arquitectura de la pasarela en mayor detalle. En ella se muestran elementos de la capa de control y de la capa de distribución de los flujos multimedia.
Gracias al GAPI, la pasarela Flash minimiza la complejidad del código destinado al control proveniente y hacia la sesión de Isabel, limitándose a traducir determinadas órdenes que son necesarias de cara a los clientes.
A continuación se describen superficialmente cada uno de los componentes que aparecen en la figura:

• Flash Gateway: Es la capa superior, como se puede apreciar en la figura. Es responsable de la comunicación entre el GAPI y el Flash Manager. Escucha los eventos generados en ambas partes propagándolos de manera que el estado quede sincronizado.

• GAPI: Es el componente explicado anteriormente que facilita en gran medida la conversión del protocolo de control de Isabel.

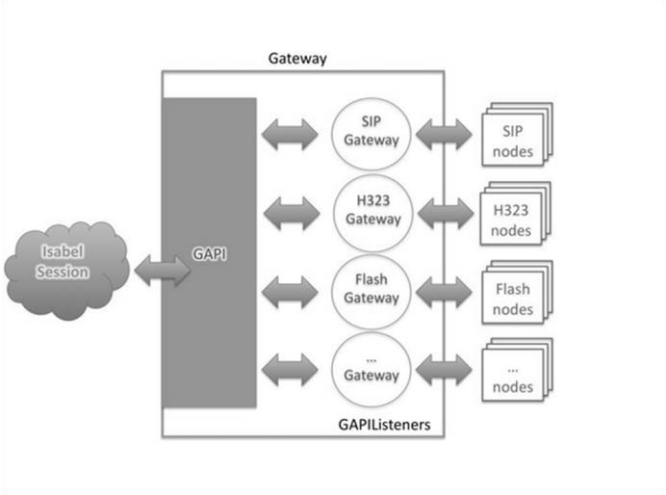


Fig. 1 Arquitecturas de utilización del GAPI

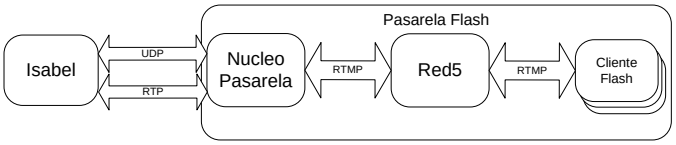


Fig. 2 Componentes que forma la pasarela.

• Flash Manager: Esta pieza junto con su principal módulo llamado Red5UserManager, se encarga de toda la comunicación con el servidor Flash.
• MCU: La MCU de Isabel es un desarrollo de software capaz de transcodificar vídeo y audio así como de sumar flujos de audio y formar mosaicos de vídeo. La pasarela utiliza principalmente la MCU para manejar audios y vídeos según sea conveniente de cara al envío de estos a la sesión de Isabel o al servidor Flash.
• Servidor VNC: En la pasarela, el servidor VNC es necesario para obtener de una manera sencilla la composición del escritorio de la sesión de Isabel para poder mandárselo a los clientes Flash sin que éstos tengan que componer su propia imagen a partir de vídeos separados. Además se asegura que lo que ve cada cliente es lo mismo, siguiendo el modelo de Isabel.
• Transcoder: Este módulo se encarga de realizar las transcodificaciones tanto de audio como de vídeo necesarias para que los dos sistemas se entiendan.
• Conexión RTMP: Este componente emula a un cliente RTMP (que normalmente es un Flash Player). Este cliente simulado es el que, de cara al servidor Flash, publica y recibe los vídeos y audios correspondientes a la sesión.

Hasta aquí el repaso de los diferentes componentes. En las siguientes secciones del artículo se detalla el funcionamiento de los mismos.

C. Arquitectura del Red5 y Clientes Web

Tal y como se puede ver en la Fig. 4 la pasarela Flash envía el video de Isabel al servidor Red5 utilizando el protocolo RTMP de Adobe. Para ello utiliza un cliente RTMP que se conecta directamente a este servidor. Por otro lado aquellos usuarios que quieran acceder al video de Isabel tendrán que conectarse también a este servidor, de forma que el servidor además les permite interactuar en la sesión Isabel de forma activa. En el momento en el que un usuario con un cliente Flash se conecta al servidor Red5, podrá enviar el video captura de su webcam, el audio de su micrófono, podrá realizar preguntas durante un evento de Isabel e incluso controlar un escritorio remoto. Todo esto se consigue gracias a que el servidor Red5 reencaminará estos flujos multimedia y los eventos generados en los clientes Flash hacia la pasarela Flash, y viceversa.

En la misma figura podemos ver como se reencaminan los flujos entre las máquinas Isabel y los clientes Flash. La línea continua representa los flujos de video de los clientes Flash. La línea con puntos representa el audio de éstos y la línea discontinua representa el video y el audio mezclados en un único flujo que Isabel a través de la pasarela Flash envía al Red5. Este flujo es la suma de todos los audios de los terminales Isabel, no de los clientes Flash, ya que así se evitan ecos y realimentación del sonido. La suma de videos de todos los participantes (incluyendo Isabel y clientes Flash) se hace con la composición que realiza Isabel mismo con el modo de interacción elegida incluyendo, si se escoge, cualquier video de los clientes Flash que están conectados a la sesión a través de dicha pasarela.

El flujo de audio de cada cliente Flash se envía al servidor Red5, que lo transmite a Isabel a través de la pasarela. Es Isabel mismo el que toma la decisión de presentar o no cualquier flujo de video por pantalla dependiendo del modo de interacción elegido por el operador de Isabel. Dependiendo del modo de interacción el operador puede controlar la sesión incluso utilizando un cliente Flash.

El servidor Red5 puede servir diferentes sesiones de Isabel simultáneamente ya que se pueden arrancar múltiples instancias de la misma aplicación que se ejecuta sobre éste, cada una para una sesión de Isabel. Por lo que los diferentes clientes Flash se podrían conectar a diferentes sesiones de Isabel al mismo tiempo y utilizando el mismo Red5. Se pueden distinguir las sesiones de Isabel a través de la URL por la que se conectan estos clientes: `rtmp://servername/IsabelWebGWApp/isabelSessionID`.

D. Librerías Utilizadas

Para transcodificar el video y el audio que se obtiene de los terminales Isabel para después incluirlo en una conexión RTMP se utiliza la librería de código abierto llamada Xuggler [10]. Esta librería está pensada para poder codificar, decodificar y manipular video y audio en tiempo real desde aplicaciones Java. Para ello utiliza la librería FFMpeg [11] por debajo para conseguir codificar y decodificar el video y el audio. En nuestro caso lo que hacemos por una parte es obtener el audio de Isabel a partir de una suma de todos los audios que obtenemos de la sesión de Isabel, es decir, del audio de todos los terminales que están emitiendo. En cuanto al video lo que hacemos es representar el video en una pantalla que después capturamos a través de un cliente VNC especial, de esta forma obtenemos las imágenes que se mostrarían por éste VNC y las codificamos utilizando el Xuggler.

Para realizar este cliente VNC especial nos basamos en la librería Java creada por TightVNC [12] con la que se implementa un visor VNC completamente en Java. Esta librería es también de código abierto y se distribuye con el servidor VNC del mismo nombre. En nuestro caso modificamos el código del cliente Java para, simplemente, quedarnos con las imágenes que este cliente recompone para formar la vista del escritorio.

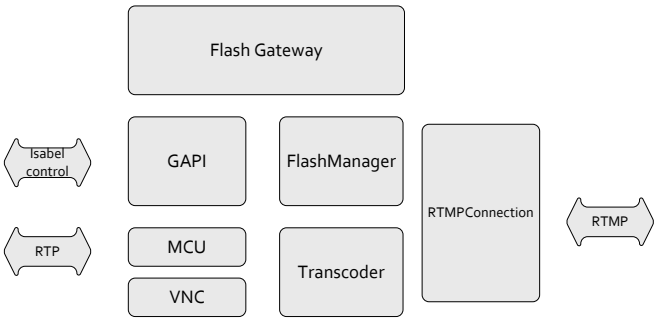


Fig. 3 Arquitectura detallada de la pasarela

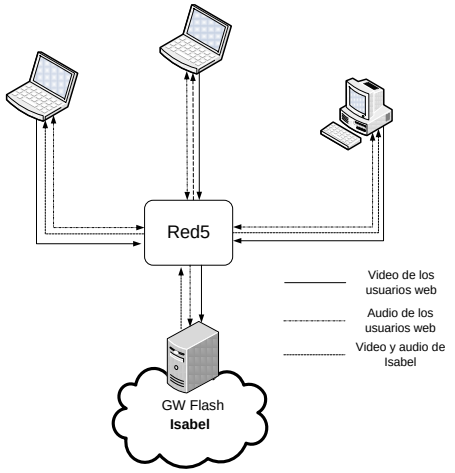


Fig. 4 Arquitectura de la aplicación Red5

Los flujos de video y audio generados por el Xuggler se empaquetan dentro de conexiones RTMP utilizando la librería que se incluye en Red5 para implementar clientes RTMP en Java. De nuevo utilizamos esta librería por ser de código abierto, y porque en este caso era la única librería que conocíamos, ya que la parte del servidor también está implementada sobre los mismos APIs, ya que se ejecuta con el servidor que lleva su nombre: Red5.

Los clientes Flash se implementaron utilizando el framework de código abierto Flex [13], creado por Adobe, y que permite crear aplicaciones que se ejecutan sobre el reproductor Flash Player, que hoy en día se puede instalar sobre muchos navegadores web. Estos clientes son los que se conectan al Red5 para interactuar en la sesión de Isabel. Como ya hemos dicho anteriormente estos clientes enviarán audio y video hacía Isabel, por lo que de nuevo se hará uso de la librería Xuggler para que desde la pasarela se obtengan estos flujos multimedia y poderlos transcodificar a códecs y formatos que conoce Isabel.

E. Configuraciones de la pasarela

Debido a las posibilidades que ofrece tanto las librerías de Xuggler como de Red5 la pasarela se ha implementado de forma que a través de ciertas variables de configuración permita ofrecer unos servicios bien diferenciados.

De esta forma es posible configurar la URL del servidor a donde se va a realizar la conexión RTMP y el nombre principal del flujo de video y audio. También es posible separar los flujos de video y audio para tener una pasarela que únicamente envíe audio, al igual que cambiar el ancho de banda utilizado en ambos sentidos: uno en cuanto al video y al audio que se recoge de Isabel, y otro en cuanto al audio y al video que se recoge de los clientes Flash.

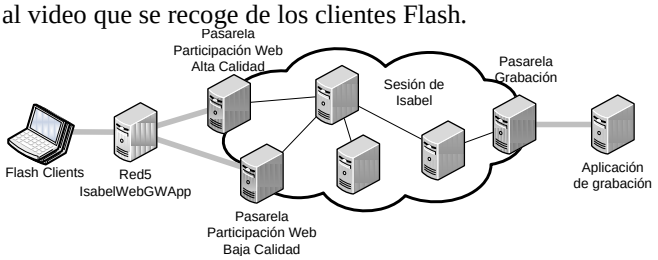


Fig. 5 Escenario real de una sesión Isabel con pasarelas

Además permite la utilización del códec H.264 en vez del códec por defecto, que es Sorenson Spark. Y otros parámetros adicionales como la configuración del servidor VNC al que controlaran los clientes Flash cuando activen el modo de compartición de escritorio de Isabel.

Todo esto permite que la pasarela tenga dos funcionalidades clave:

- La primera de ellas es la función de participación Web, que es la que hemos comentado a lo largo del artículo, que a su vez se puede dividir en diferentes pasarelas con diferentes anchos de banda y calidades de video para dar servicio a una mayor variedad de usuarios (teniendo en cuenta simplemente el ancho de banda del que pueda disponer cada uno). Como resultado tendríamos que en una sesión de Isabel podrían estar conectadas dos o más pasarelas apuntando al mismo Red5 (pero a diferentes instancias del servidor), por lo que los clientes Flash a través del mismo cliente podrían conectarse a la sesión de Isabel a mayor o menor calidad dependiendo del ancho de banda disponible en su conexión hacia el Red5.
- La segunda es la aplicación de la pasarela como centro de streaming y grabación de la sesión de Isabel en formato FLV [14], para poder ser reproducido tanto en tiempo real como en diferido por parte de reproductores Flash, los mismos que permiten hoy en día ver videos en YouTube, por ejemplo. A su vez podríamos tener streaming y grabación a distintas calidades.

El resultado es que en una misma sesión de Isabel podremos ver conectadas (como en Fig. 5) varias pasarelas equivalentes que tienen objetivos diferentes: unas podrían dedicarse a dar servicio a usuarios que quieren participar en una sesión (permitiendo incluso varias calidades de video) y otras a ofrecer el video para que otros usuarios puedan visualizarlo (también con varias calidades).

F. Audio y Video

Una de las principales labores de la pasarela es traducir los flujos de audio y vídeo entre el mundo Isabel y el mundo Flash. En este proceso intervienen cuatro componentes: el servidor VNC, MCU, RTMPConnection y Transcoder.

Como se ha adelantado anteriormente, el servidor VNC va a proporcionar el vídeo que se destina a los clientes Flash. Para ello, se ejecuta una sesión Isabel en su interior para obtener la composición de la pantalla propia de la aplicación. A partir de ahí, el servidor VNC pasa las imágenes al Transcoder que se encarga de codificarlas al formato necesario pasándolo finalmente al RTMPConnection que encapsulará el flujo en paquetes RTMP enviándolos finalmente al servidor Flash. En cuanto a los formatos de vídeo, las mayores restricciones las encontramos, como vemos en la tabla, en la plataforma Flash que, además de hacer necesario el uso de RTMP, impone restricciones en cuanto a los codecs que permite utilizar.

Formatos	Reproducción	Captura
Sorenson Spark	SI	SI
On2 VP6	SI	NO
H.264	SI	NO

Tabla 1 Codecs aceptados por el reproductor Flash.

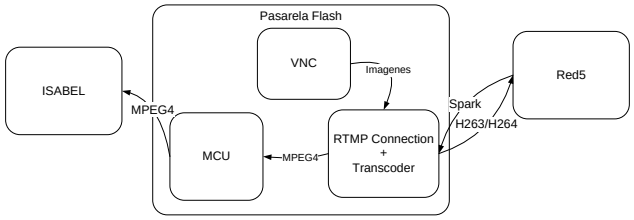


Fig. 6 Transcodificación del video

En el otro lado, Isabel permite utilizar (tanto en reproducción como capturando de una cámara) una gran variedad de códecs, siendo MPEG4 el más habitual. Así, normalmente es necesaria una transcodificación de los vídeos provenientes de los clientes Flash antes de que estos puedan ser vistos por Isabel.

En ese caso, los datos recibidos mediante RTMPConnection en Sorenson Spark se pasan al transcoder que se encarga de pasarle el vídeo en formato MPEG4 y en paquetes RTP. Finalmente, la MCU retransmite estos paquetes hacia Isabel. El proceso en ambos sentidos puede verse en la Fig. 6.

El caso del audio es más sencillo ya que en ningún caso hace falta transcodificación debido a que tanto Isabel como los clientes Flash son capaces de operar con Speex. En este caso, la única labor del Transcoder es introducir los datos en paquetes RTP cuando la comunicación es en el sentido hacia el mundo Isabel. Además, para ahorrar ancho de banda se utilizan las capacidades de la MCU como sumador de audios uniendo todos los flujos provenientes de Isabel en uno único que será el que se transmita a todos los clientes Flash.

G. Control de los Modos de Interacción

Para controlar los modos de interacción de Isabel desde los clientes de la pasarela web así como la solicitud del turno de preguntas, se ha implementado un mecanismo que permite presentar al usuario distintos botones dependiendo de la actividad de colaboración que se está desarrollando. Por ejemplo durante una conferencia distribuida en la que el control está fuertemente centralizado a los usuarios de la pasarela solo se les permite pedir turno de pregunta, mientras que si la actividad es una reunión de trabajo distribuida en la que cualquiera puede tomar el control de la reunión, el usuario de la pasarela tiene una serie de botones que le permiten cambiar el modo de interacción entre los disponibles.

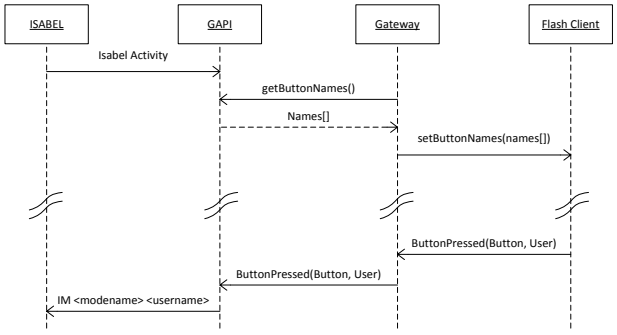


Fig. 7 Mecanismo de control de los modos de interacción.

El mecanismo implementado tiene los siguientes pasos tal y como se muestran en Fig. 7:

1. Al conectar un cliente de la pasarela se le da una lista con los nombres de los botones que tiene que presentar al usuario. Desde el punto de vista del software de la pasarela todos estos botones son idénticos en funcionamiento.
2. Cuando el usuario pulsa uno de estos botones, la misma función es llamada en el servidor Red5, que en respuesta avisa a la pasarela Web de que un botón ha sido pulsado por un usuario.
3. La pasarela, mediante una llamada al GAPI, envía el mensaje pertinente a Isabel mediante su protocolo de señalización interna.

H. Control de Escritorio Remoto

Para permitir el control del escritorio remoto por parte de un usuario de la pasarela web que lo que está viendo es un flujo de vídeo, hemos implementado un mecanismo que recoge eventos de ratón y teclado en los clientes flash sobre el video y los envía hacia la pasarela. Puesto que cada cliente puede estar viendo el vídeo a una resolución diferente es necesario escalar las coordenadas de la posición del ratón a una resolución estandarizada. En la pasarela estos eventos se reproducen programáticamente sobre el cliente VNC que corre en la pasarela. Esto nos permite controlar todos los elementos interactivos que aparecen en una sesión de colaboración Isabel: escritorio remoto, panel de preguntas, pizarra, etc…

Este mecanismo solo se activa cuando el modo de Isabel lo permite y para los usuarios que indica el modo de interacción. Para ello el GAPI avisa del cambio de modo de interacción a la pasarela mediante un evento que contiene la lista de escritorios activos. Esta lista se pasa al servidor red 5 que avisa a los clientes flash de si deben activar o no su escritorio.

V. PRUEBAS DEL SISTEMA

A. Ancho de banda consumido

Uno de los objetivos fundamentales de la pasarela es que pueda ser usada por el mayor abanico posible de sistemas. Esto incluye tanto sistema operativo y CPU como calidad de la conexión disponible. En este contexto, la disponibilidad de la plataforma Flash en los sistemas operativos más populares asegura el primer punto aunque, como veremos más adelante, plantea algunos problemas en cuanto a CPU.

En el apartado de los requisitos en cuanto a la conexión se han realizado numerosas pruebas durante el desarrollo de la pasarela para intentar identificar los principales problemas que puedan surgir. La principal conclusión obtenida de estas pruebas es la necesidad de que coexistan más de una pasarela con diferentes parámetros de calidad para poder ofrecer mejor servicio a conexiones de mayor y menor ancho de banda.

Por otro lado, en casos específicos como redes inalámbricas o redes con pérdidas nos encontramos con el problema de que TCP sea el protocolo sobre el que se apoya RTMP. Como sabemos [15], TCP no está pensado para estos escenarios e interpreta la pérdida de paquetes como congestión de red disminuyendo el tamaño de la ventana de congestión lo que reduce la velocidad de transmisión. Esta

situación afecta gravemente a los flujos de video y audio hacia los clientes de la pasarela haciendo que obtengan un rendimiento sensiblemente peor al esperado llegando incluso a cortarse la comunicación.

Este efecto negativo empeora aún más en escenarios en los que aparte de las pérdidas de paquetes coexisten grandes retardos en la red, como es el caso de los enlaces por satélite, por lo que en estos casos no serviría una solución basada en TCP.

B. Problemas de Eco

Durante las pruebas uno de los problemas que surgieron desde un comienzo fue el eco existente al conectar un cliente Flash. Esto surge principalmente por el nuevo tipo de usuarios que se conectan a la pasarela Web y su peor conocimiento de aspectos técnicos de los sistemas. Así como Isabel está más enfocada a su utilización por parte de un operador que se encarga de configurar el sistema la pasarela se caracteriza por su configuración más simple. Para ello abordamos diferentes soluciones que pasaran por que los usuarios no tuvieran que hacer pruebas de eco, ni tener por qué conocer detalles de cómo viaja el flujo de audio entre sus ordenadores y las sesiones de videoconferencia.

La primera solución que utilizamos fue la de activar el cancelador de eco que viene de por sí en el reproductor Flash, este cancelador intenta eliminar el eco producido cuando un usuario está escuchando la videoconferencia a través de altavoces y utilizando un micrófono de baja calidad como son muchos de los que vienen en las mismas Webcams. Este escenario no es el correcto para establecer una videoconferencia ya que los micrófonos de este tipo recogerán todo el sonido ambiente incluido aquel que es emitido por los altavoces, por lo que el nivel de eco es muy alto. En estos casos el reproductor de Flash funciona correctamente siempre que el único audio emitido y capturado sea a través de él. Es decir, no vale si a la vez están haciendo uso de la E/S de audio otras aplicaciones. Además hay casos en los que el resultado no es el esperado. De hecho Adobe en el propio API de Flash avisa de que este cancelador de eco no quita todo el eco en todos los escenarios posibles.

La segunda posibilidad, aparte de utilizar este cancelador de eco, fue la de implementar en la aplicación otro adicional que controlara la ganancia del micrófono a partir del nivel de audio que llegaba desde la videoconferencia. Esta supresión de eco, que está basada en sistemas antiguos de supresión de eco, supone que todo el audio que hay en una videoconferencia está producido por una sola persona en un momento dado, que es la persona que en ese momento está hablando, por lo que en realidad lo que hace es que si recibes audio desde la videoconferencia corta el audio de tu micrófono (si es que hay) porque supone que sólo puede ser eco. Lógicamente este no es el sistema de reducción de eco más eficaz, de hecho hoy en día se utilizan muchos otros que responden mejor a situaciones reales, pero sería el único que nosotros podríamos utilizar debido a que el API de Flash no nos permite procesar la señal de audio que llega de la videoconferencia ni la que capturamos de los micrófonos. Aún así decidimos que no era la mejor solución ya que hay situaciones en las que si alguien a través de su micrófono está emitiendo ruido hacia la videoconferencia los demás usuarios no podrán hablar correctamente.

Fig. 8 Capturas de pantalla de la pasarela Web

La tercera posibilidad fue la de implementar un sistema de Push-to-talk de forma que aquel usuario que quisiera hablar a través de la videoconferencia debería mantener presionado un botón mientras durara su intervención. Así se eliminaría el eco producido por este tipo de usuarios y sólo se introduciría eco cuando aquel que tuviera un mal ajuste de su micrófono y altavoces interviniera a la vez que otros usuarios. Este sistema está muy extendido en los terminales móviles (PoC [16]). Por lo que por su sencillez de desarrollo y uso pensamos que sería la mejor solución y la implementamos.

VI. CONCLUSIONES

En la figura anterior podemos ver una captura de pantalla de una sesión de videoconferencia con Isabel y la pasarela Web.

La solución planteada cumple todas las expectativas que teníamos en un principio. Se han incluido y permitido la interoperación de una compleja aplicación multimedia distribuida, como es Isabel, con aplicaciones tipo RIA. Las principales ventajas la disponibilidad inmediata desde cualquier terminal que disponga de un navegador con el plugin Flash instalado para participar en cualquier conferencia que se esté realizando, superados los debidos controles de seguridad.

Esto permitiría, por una parte, una integración con otras aplicaciones sociales tales como Facebook o Twitter permitiendo una mayor interactividad y una mayor facilidad de colaboración para usuarios nómadas. Por otra parte elimina algunas barreras de entrada para muchos usuarios tales como la instalación y configuración de dichas aplicaciones. Por ello el trabajo presentado aquí es un gran avance de usabilidad para la realización ubicua de complejas sesiones distribuidas.

Actualmente los trabajos futuros se están centrando en la evolución de la arquitectura aquí presentada a un esquema de SaaS (*Software as a a Service*), lo que permitiría eliminar problemas de escalabilidad y configuración a usuarios finales.

Por otra parte se considera el portarlo a tecnologías HTML5-JavaScript si bien estas aún adolecen de las capacidades de captura de audio y video (cámara y micrófono) de los diversos terminales existentes, siendo perfectamente adaptable a cualquier dispositivo (tablet o móvil) en cuanto dichas capacidades estén disponibles.

REFERENCIAS

[1] T. Noda and S. Helwig. “Rich internet applications”. Technical report, http://www.uwebc.org, 2005.
[2] J. Cerviño, P. Rodriguez, G. Huecas, J. Salvachúa, F. Escribano, “Marte 3.0: Una videoconferencia 2.0”, VII jornadas de JITEL, septiembre 2008.
[3] Adobe Flash: www.adobe.com/go/gntray_prod_flash_home_es
[4] B. Hayes, “Cloud computing”, Communications of the ACM, 2008.
[5] J. Quemada, G. Huecas, S. Pavón, J. Salvachúa, “La Aplicación Isabel: Actividades Educativas interactivas a través de Internet”, COIT, Jun-Jul 2008.
[6] Java: www.java.com
[7] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, RFC 1889, Jan. 1996.
[8] Real Time Messaging Protocol: http://www.adobe.com/go/tn_16631
[9] Red5: www.red5.org.
[10] Xuggler: www.xuggle.com/xuggler/
[11] FFMpeg: www.ffmpeg.org/
[12] TightVNC: www.tightvnc.com/
[13] Flex SDK: www.adobe.com/es/products/flex/
[14] Adobe, “Video File Format Specification Version 9”.
[15] “Impact of mobility on TCP/IP: an integratedperformance study”, IEEE Journal on Selected Areas in Communications, 1995.
[16] Manzoni, P.; Ghosal, D.; Serazzi, G. “Push to talk over Cellular (PoC) – Architecture”, Open Mobile Alliance, Feb. 2008.

Análisis de QoS para una Plataforma Distribuida de Telefonía IP

Jenifer Murillo, José Mª Saldaña, Julián Fernández-Navajas, José Ruiz-Mas, Eduardo Viruete, José I. Aznar
Grupo de Tecnologías de las Comunicaciones (GTC) Instituto de Investigación en Ingeniería de Aragón (I3A)
Dpto. IEC. Edificio Ada Byron. CPS Univ. Zaragoza
50018 Zaragoza, España
e-mail: {jenifer.murillo, jsaldana, navajas, jruiz, eviruete, jiaznar}@unizar.es

***Resumen*—En los últimos años, muchas empresas están cambiando sus soluciones de telefonía tradicionales por otras nuevas que utilizan centralitas *software*, en las que un único PC actúa como nodo central en un sistema completo de telefonía IP, utilizando Internet para realizar llamadas. Las soluciones propietarias suelen utilizar elementos locales que implementan esquemas de control de admisión, pero las centralitas *software* a menudo carecen de mecanismos para proporcionar Calidad de Servicio (QoS, *Quality of Service*) al tráfico de voz. En este artículo se presenta un Control de Admisión de Llamadas (CAC, *Call Admission Control*) para este tipo de sistemas. Para ello se incluye un agente local en cada sucursal de la empresa, que sólo acepta nuevas llamadas si estima para ellas una calidad aceptable. La primera evaluación del sistema ha sido realizada en una plataforma de pruebas basada en virtualización. En un primer paso las llamadas son simuladas, y posteriormente se realizan con tráfico real.**

***Palabras Clave*—CAC; centralita *software*; QoS; virtualización; VoIP**

I. Introducción

En los últimos años, muchas empresas están cambiando sus viejos sistemas de telefonía por otros que utilizan Voz sobre IP (VoIP, *Voice over IP*), que permite realizar llamadas telefónicas utilizando redes de datos. Este cambio ha impulsado la aparición de centralitas *software* que utilizan un simple PC para actuar como nodo central en un sistema completo de telefonía IP, ofreciendo los servicios propios de una centralita. Este PC puede utilizar también algunas tarjetas especiales para conectarse a la RTC. Las soluciones de centralita *software* están popularizándose en Pequeñas y Medianas Empresas (PYMES), para evitar el coste de un sistema propietario.

VoIP es un servicio en tiempo real que tiene que funcionar sobre una red que inicialmente fue diseñada para servicios *best-effort*. Pero los usuarios demandan una Calidad de Servicio (QoS, *Quality of Service*) similar a la de los sistemas telefónicos tradicionales. Esto ha propiciado la búsqueda de soluciones que permitan añadir control de calidad a las redes IP. El sobredimensionado de las redes se usa a menudo para resolver este problema, pero el continuo crecimiento del tráfico y el desarrollo de nuevos servicios hacen que sea una propuesta demasiado simple, y también muy cara. Existen soluciones más inteligentes que pueden ser aplicadas tanto en el plano de datos como en el de control [1]. Entre estas últimas se utiliza mucho el Control de Admisión de Llamadas (CAC, *Call Admission Control*), un sistema que puede rechazar nuevas llamadas que no van a recibir una QoS mínima o que van a disminuir la de las que ya están en curso, evitando así la degradación del servicio de todas las llamadas del sistema.

A menudo, las empresas tienen más de una sucursal y pueden utilizar los sistemas de telefonía IP para evitar el alto coste de las líneas dedicadas. Así, parte del tráfico VoIP ha de ser soportado por una red *best-effort*. Algunos sistemas propietarios de telefonía IP utilizan un elemento en cada sucursal para proporcionar QoS a las comunicaciones. Pero con frecuencia las soluciones de centralita *software* carecen de garantías de calidad para las comunicaciones.

En este artículo se presenta un CAC para un sistema de telefonía IP basado en una centralita *software* (Fig. 1). Se ha añadido un agente local en cada sucursal para interceptar los mensajes de señalización y, dependiendo de la decisión de admisión, reenviar el mensaje al destino o enviar un mensaje de no disponibilidad a la centralita. Así, el CAC se integra con facilidad en el sistema de telefonía, sin que la centralita ni los terminales VoIP necesiten modificación alguna. La introducción de un nuevo agente en cada sucursal puede verse como una desventaja, pero como veremos, es un elemento simple que no requiere gran capacidad de procesado, así que puede ser fácilmente incluido como un proceso dentro de un servidor ya existente. De todos modos, se estudiará el agente local como un elemento diferenciado.

Antes de implementar el sistema en entornos reales, es muy recomendable validar primero la solución en un entorno controlado, como una plataforma de pruebas, donde pueda ser instalado y evaluado. Las plataformas basadas en virtualización permiten desplegar un escenario de red completo en una única máquina física. Además, de este modo las aplicaciones multimedia y las pilas de protocolos pueden ser implementaciones reales. Por otra parte se pueden ahorrar costes, ya que es posible ejecutar muchas máquinas virtuales dentro de una única máquina física. La técnica de virtualización se ha utilizado para construir diversas plataformas: algunas son grandes infraestructuras como *PlanetLab* [2], mientras que otras son pequeñas [3], [4]. El simulador de red *ns-3* [5] permite integrar máquinas virtuales, que pueden ejecutarse sobre sus dispositivos y canales.

La organización del artículo es la siguiente: la sección II habla sobre trabajos relacionados y el uso del control de admisión. La arquitectura del sistema se presenta en la sección III. La siguiente sección se centra en la plataforma de pruebas. La sección V presenta los resultados obtenidos. La última sección detalla las conclusiones del presente trabajo.

II. Trabajos relacionados

Existe una amplia variedad de protocolos que se utilizan para la señalización en sistemas de VoIP. H.323, IAX (*Inter-*

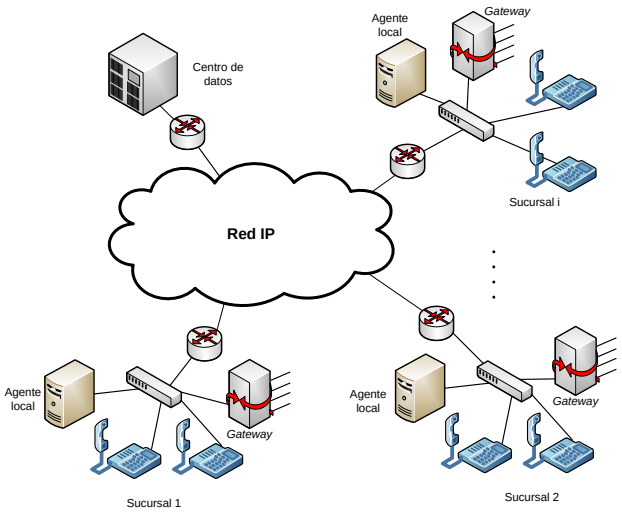


Fig. 1. Sistema de telefonía IP

Asterisk eXchange), MGCP (*Media Gateway Control Protocol*) y SIP (*Session Initiation Protocol*) son algunos de los más utilizados. El análisis realizado en este artículo está basado en SIP, ya que es un protocolo abierto y muy utilizado en redes IP. SIP también ha sido adoptado por el 3GPP como el protocolo de señalización para IMS (*IP Multimedia Subsystem*) [6]. Otra ventaja de SIP es que no sólo puede utilizarse para administrar sesiones VoIP, sino que también puede usarse para otros servicios. Existen centralitas *software* de código abierto y sistemas comerciales de VoIP que utilizan SIP [7] y permiten que el sistema CAC pueda ser fácilmente integrado en ellos.

La recomendación RFC 3261 para SIP incluye el concepto de *proxy* SIP, un elemento que puede concentrar o redirigir tráfico, añadiendo escalabilidad al sistema, ya que transfiere carga computacional del núcleo de la red a los extremos. Entre las soluciones de centralita *software* destaca Asterisk, desarrollada por Digium. Actúa como *back to back user agent*, realizando dos comunicaciones, una desde el origen hasta la centralita y otra desde la centralita hasta el destino y uniendo las dos. Asterisk soporta SIP y otros protocolos de señalización.

Pero actualmente no existe una solución completa para añadir QoS a una centralita *software* [8]. En redes IP se puede utilizar DiffServ (*Differentiated Services*), que modifica el campo ToS (Tipo de Servicio, *Type of Service*) de la cabecera IP para clasificar el tráfico. Pero no existe un acuerdo entre los diferentes proveedores de redes, aplicaciones, etc. para unificar dicha clasificación. De este modo el envío extremo a extremo no tiene garantías de QoS. Otra opción es el uso de IntServ (*Integrated Services*), que reserva recursos para los flujos de datos. Esto conlleva problemas de escalabilidad y requiere que todos los *router* intermedios implementen este protocolo, algo que no es posible en la práctica en muchos casos.

La existencia de un elemento local en cada sucursal es importante porque la centralita no dispone de información acerca del tráfico de cada sucursal. Algunas soluciones propietarias añaden un elemento en cada sucursal, por ejemplo las soluciones de CISCO utilizan un elemento denominado *Call-Manager* que interopera con el *Gatekeeper* que se encuentra en el nodo central [9].

En los últimos años se han estudiado y desarrollado muchos sistemas de control de admisión. En [10] se puede encontrar un estudio sobre diferentes métodos, incluyendo comparativas y clasificaciones. Las soluciones basadas en el almacenamiento de información sobre los recursos reservados en la red presentan problemas de escalabilidad y dificultades de implementación, mientras que las soluciones basadas en medidas de las condiciones de la red son más adecuadas para adaptarse al estado de la red.

Algunos sistemas CAC utilizan el modo basado en parámetros. Para ello, es necesario realizar algunas medidas durante la configuración inicial del sistema. El tráfico interferente debe ser medido para obtener el número máximo de llamadas que podrían establecerse simultáneamente. Los sistemas basados en medidas realizan estimaciones cuando una llamada va a establecerse, pero su desventaja radica en que añaden más retardo, ya que normalmente se implementa una fase de prueba previa al establecimiento de la llamada; las medidas activas añaden sobrecarga al sistema y presentan una alta dependencia de la congestión instantánea de la red.

En [11] se presentó un sistema CAC basado en parámetros. En él se añade QoS en entornos CISCO, siendo H.323 el protocolo inicial, y se incluye un *Integration Component* para interceptar la señalización. Como nuestro sistema está basado en SIP, el uso de *proxy* SIP evita este elemento, interceptando la señalización de las llamadas de una forma natural.

La principal novedad del presente estudio es que el sistema utiliza un protocolo abierto como SIP, y *software* libre para el elemento central y también para los agentes que están a cargo del CAC en cada sucursal. Estas características permitirán el estudio y las medidas, ya que la documentación y el código fuente están disponibles. El sistema evaluado es similar a los esquemas propietarios, pero con muchos parámetros que podrán ser modificados y estudiados para obtener resultados comparativos: diferentes *codec*, esquemas de CAC, influencia de los *buffer* de los *router*, etc.

Nuestro sistema también puede utilizarse para reducir costes en empresas multinacionales, ya que podemos conseguir que las llamadas internacionales tengan un coste local. Para ello, como muestra la Fig. 2, en lugar de realizar estas llamadas directamente desde el *gateway* local, se divide la llamada en dos tramos: el primero utiliza VoIP, vía Internet, hasta la sucursal destino, y un segundo tramo llega hasta el terminal destino con el coste de una llamada local.

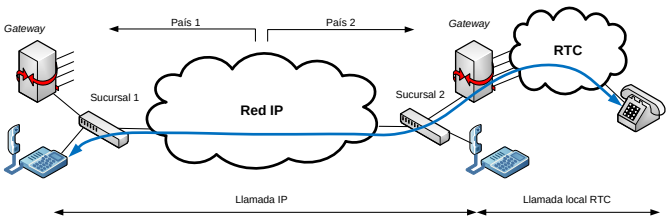


Fig. 2. Llamada internacional

III. Arquitectura del sistema

A. Descripción general del escenario

Como hemos dicho, el sistema de telefonía IP se ha diseñado para una empresa con varias sucursales en distintas localizaciones de diferentes países. Para reducir costes de administración, es deseable tener el plan de numeración sólo en la centralita, y no distribuido en las sucursales. Además, se utiliza Internet para enviar el tráfico telefónico entre las sucursales, en lugar de utilizar líneas dedicadas. Hemos asumido que el sistema no utiliza ningún protocolo de reserva de recursos, y podemos asumir también que el tráfico VoIP es el único tráfico en tiempo real que se trata de forma especial.

En este escenario se utiliza un sistema CAC basado en parámetros, en el que se realizan varias medidas de tráfico al inicio de la configuración, para asignar un número máximo posible de llamadas simultáneas en cada sucursal. El principal objetivo es asegurar un valor mínimo de QoS para las llamadas, al coste de tener que rechazar algunas de ellas.

Se ha introducido un elemento para implementar el sistema CAC en cada sucursal: un agente local. Su arquitectura puede verse en la Fig. 3. Este elemento juega un papel fundamental en la elección de la mejor ruta para realizar las llamadas telefónicas, en base a las medidas de QoS y a las tarifas. A continuación se explican los elementos que lo componen:

1) Un *proxy* SIP procesa la señalización de las llamadas telefónicas para implementar el mecanismo del CAC, basado en información almacenada en la base de datos. La decisión de CAC se basa en el estado actual de las sesiones VoIP, teniendo en cuenta las tarifas y las líneas disponibles en los *gateway*. El *proxy* SIP no requiere una gran capacidad de procesado. En [12] se realizaron algunas medidas del comportamiento del *proxy*, comprobando que un único *proxy* puede administrar 2.000 mensajes SIP por segundo. El tráfico que estamos considerando en este artículo es mucho menor.
2) El módulo contador se encarga del control de líneas libres y ocupadas en el *gateway*. También realiza un conteo del número de llamadas telefónicas cursadas en la sucursal en cada momento. Teniendo en cuenta esta información, las tarifas telefónicas y el número de líneas disponibles en el *gateway*, el agente local rellena la tabla de decisiones en la que se basa el sistema CAC.

B. Funcionamiento del sistema CAC

La señalización SIP se envía desde el teléfono IP al agente local, y posteriormente a la centralita. En ella, de acuerdo al plan de numeración, se establece otra llamada hasta el terminal destino, y las dos llamadas se unen. La comunicación de voz transmite tráfico RTP, y se ha configurado el sistema para que este tráfico se envíe directamente entre los teléfonos, y no a través de la centralita.

Como toda la señalización pasa a través del agente local, éste puede tomar decisiones sobre futuras peticiones de establecimiento y llevar la cuenta del número de líneas ocupadas en el *gateway*. En caso de que no haya que rechazar la llamada, el agente local únicamente retransmite los mensajes de señalización. Las llamadas internas a la sucursal son administradas directamente por el agente local, sin necesidad de intervención de la centralita, de modo que no están afectadas

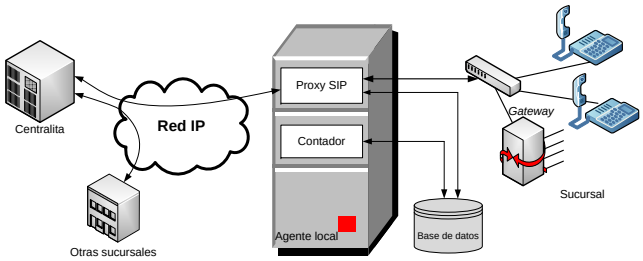


Fig. 3. Arquitectura del agente local

por el sistema CAC. Las llamadas entre terminales de distintas sucursales pueden ser rechazadas por el CAC, por falta de QoS en la ruta entre dichas sucursales o por la indisponibilidad del terminal destino. Cuando se rechaza una llamada, se envía un mensaje SIP a la centralita del tipo *480 Temporarily Unavailable*.

Las llamadas cuyo destino es la RTC que se realizan a través del *gateway* pueden ser redirigidas si no existen líneas disponibles. En este caso el agente actúa como *redirect server*, redirigiendo la llamada a otra sucursal (si es posible del mismo país) que tenga líneas disponibles para establecer la comunicación. El *redirect server* envía un mensaje 3XX informando sobre una ruta alternativa (Fig. 4). El agente que actúa como *redirect server* ya no tomará parte en esta llamada. Para evitar bucles en la señalización hay que elegir un valor adecuado en el campo *MAX_Forwards* de la cabecera.

Veamos un ejemplo simplificado para ilustrar el ahorro en costes y el incremento del grado de servicio de las llamadas a la RTC al utilizar redirecciones. Los teléfonos de cada sucursal generan tráfico hacia la RTC (AP_i) y hacia la otra sucursal a través de la red IP (AI_{ij}). El tráfico de desbordamiento (AO_i) representa las llamadas que no pueden ser cursadas por el *gateway* local. N_i representa el número de líneas del *gateway*, y M_i el máximo número de llamadas que pueden ser aceptadas por el sistema CAC. Para ilustrar las ventajas de compartir los *gateway* se muestra un ejemplo con dos sucursales (Fig. 5). Sea γ(A,N) la probabilidad de bloqueo del sistema con tráfico A y N servidores, P_{bRTC} y P_{bIP} las probabilidades de bloqueo de los *gateway* y del sistema CAC respectivamente. En caso de no compartir los *gateway*, la probabilidad de bloqueo en la sucursal 1 será:

$$P_{bRTC} = \gamma(AP_1, N_1) \tag{1}$$

$$P_{bIP} = \gamma(AI_{12} + AI_{21}, M_1) \tag{2}$$

Si los dos *gateway* se comparten entre las dos sucursales, el número de circuitos que se pueden utilizar para la conexión a la RTC crece a N_1+N_2. Así que las probabilidades de bloqueo que se obtienen son:

$$P_{bRTC} = \gamma(AP_1 + AP_2, N_1 + N_2) \tag{3}$$

$$P_{bIP} = \gamma(AI_{12} + AI_{21} + AO_1 + AO_2, M_1) \tag{4}$$

Podemos hacer una simplificación llamada *Erlang Fixed Point* que se usa para redes grandes con poca probabilidad de pérdidas. Asume que todos los tráficos tienen distribuciones

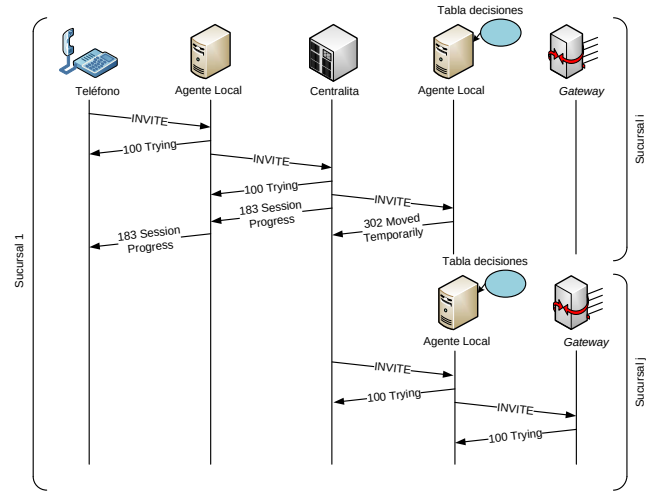


Fig. 4. Llamada redirigida por el sistema CAC

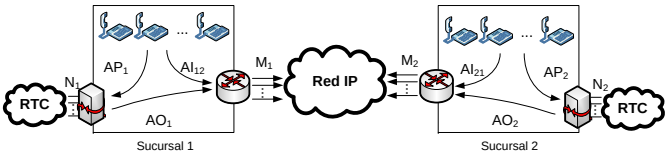


Fig. 5. Líneas de *gateway* compartidas

de probabilidad de Poisson. Así que la fórmula Erlang B (denotada como Er_b) podría utilizarse como la función γ para calcular las probabilidades de bloqueo. Utilizando esta simplificación, la probabilidad de bloqueo de los *gateway* mejora, ya que (3) será menor que (1), si suponemos que las dos sucursales tienen cantidades de tráfico y número de líneas similares. Por otra parte, (4) será mayor que (2), ya que el número de llamadas utilizadas por la red IP crecerá. Como hemos definido un número máximo de llamadas en nuestro sistema, éste rechazará llamadas en más casos. Lógicamente, la simplificación asumida podría ser muy severa, de manera que se necesitarían más cálculos y simulaciones para obtener de manera correcta γ para todos los casos. Hemos utilizado esta simplificación para ilustrar las ventajas de compartir recursos entre diferentes sucursales.

Dejando a un lado el ejemplo, se puede concluir que nuestro sistema permite intercambiar la probabilidad de bloqueo entre los *gateway* y la red IP. Pero si no se desea incrementar la probabilidad de bloqueo, existen dos soluciones: reducir el tráfico interferente o incrementar el ancho de banda, que será probablemente más económico que incrementar el número de líneas del *gateway*.

IV. Plataforma de pruebas

En esta sección se explica resumidamente la plataforma de pruebas [13] en la que se ha implementado el sistema. Se ha buscado un diseño adecuado para el sistema de telefonía IP, que emule condiciones reales y permita pruebas y medidas con flexibilidad.

A. Simulación, entorno real o emulación virtual

A la hora de construir una plataforma de pruebas existen varias opciones. Las herramientas de simulación son una de ellas, y de hecho, ya han sido utilizadas para el estudio de otros sistemas CAC [14], [15]. Su ventaja es que evitan las limitaciones electrónicas reales de los dispositivos, pero su inconveniente radica en que los protocolos tienen unas implementaciones por defecto que no tienen por qué coincidir con las implementaciones reales, de modo que sería necesario desarrollarlas para el simulador. Algunas herramientas disponibles son OPNET, OMNET++ y ns-2.

Por otra parte, la plataforma de pruebas podría implementarse también con máquinas reales. Sin embargo, el coste *hardware* sería elevado debido al gran número de elementos que forman el escenario. La virtualización consiste en ejecutar varias máquinas, cada una con su propio sistema operativo, sobre el *hardware* real de una máquina física. Algunos estudios [16] han utilizado la virtualización para minimizar costes y optimizar el control de la plataforma. Por ejemplo, *User Mode Linux* (UML) se ha utilizado en implementaciones de algunos emuladores, como vBET [17]. Los nodos virtuales se conectan mediante una red emulada que se ejecuta bajo el *driver* de la tarjeta de red. Este concepto encaja con el entorno de pruebas que queremos utilizar, permitiendo usar aplicaciones comerciales para la centralita *software*, *proxy* SIP y *softphone* que proporcionan realismo al escenario.

En lo que se refiere a la escalabilidad, la configuración de la red permite ampliar la plataforma con más máquinas físicas, en caso de que aumente la necesidad de cálculo o si existen más nodos. Además, se garantiza la repetibilidad de las pruebas, ya que utilizando una única máquina física se consigue un entorno aislado y controlable.

B. Selección de la tecnología de virtualización

Considerando todos los esquemas de virtualización existentes, se ha seleccionado la paravirtualización. La ventaja que proporciona es que la velocidad de ejecución conseguida es cercana a la de los esquemas de no virtualización. El único problema que presenta es que requiere modificaciones dentro del sistema operativo del cliente para evitar que ninguna instrucción tenga que ser ejecutada con privilegios, aunque esto no supone un inconveniente en nuestro caso, puesto que al usar Linux el problema queda reducido a una nueva compilación.

La solución escogida ha sido Xen, ya que algunos estudios comparativos de plataformas de virtualización [18] muestran que es una herramienta apropiada en términos de *overhead*, linealidad y aislamiento entre las máquinas virtuales. El rendimiento de las comunicaciones medido para un escenario compuesto por 10 máquinas virtuales fue de 93 MB/s entre pares.

Estas características son muy interesantes para el rendimiento de la plataforma, ya que se desea tener un entorno controlable en el que todas las máquinas virtuales compartan los recursos equitativamente.

C. Emulación de la red

Como el sistema se ha emulado utilizando máquinas virtuales, hemos utilizado el comando de Linux *brctl* para construir *bridge* que conecten las máquinas. Hemos creado dos redes: una de control y otra de pruebas. La red de control utiliza la interfaz *eth0* de cada máquina virtual. Como se puede ver en la Fig. 6, todos los interfaces de control están conectados al *bridge xenbr0*. Esta red se utiliza para controlar,

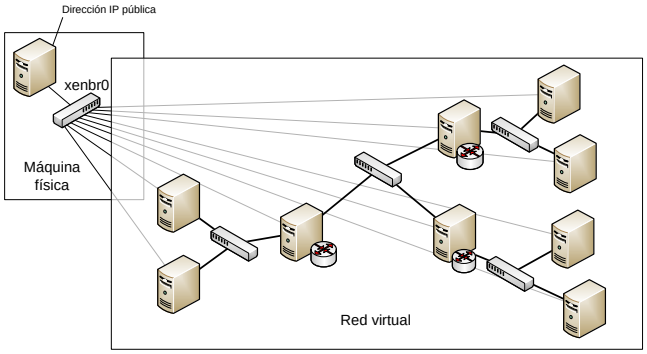


Fig. 6. Máquina física y red virtual de la plataforma

medir y configurar el sistema utilizando el protocolo SSH, evitando interferir con la red de pruebas. La máquina principal tiene una dirección IP pública que permite controlarla de forma remota. La red emulada se implementa utilizando las interfaces de red *eth1* y *eth2*.

El problema del uso de *bridge* emulados es que trabajan a velocidad de procesador, y carecen de los retardos y anchos de banda que tienen habitualmente las redes. Así que se ha utilizado la herramienta de Linux *Traffic Control (tc)* para añadir limitaciones de ancho de banda en los enlaces de acceso a cada sucursal, y la herramienta *Netem* [19] para añadir retardos en la red. *tc* tiene en cuenta las cabeceras de nivel 2, así que el límite del ancho de banda incluye en este caso los bytes de la cabecera ethernet.

Para realizar la sincronización del sistema se ha utilizado NTP, de manera que una de las máquinas virtuales tiene instalado un servidor NTP y en las demás se ha utilizado la opción de Xen *independent_wallclock*. De esta manera se ha conseguido que la sincronización sea muy precisa (aproximadamente 1 ms), permitiendo la obtención del *One Way Delay* (OWD, retardo extremo a extremo en un sentido) y del *Round Trip Time* (RTT).

D. Características de la máquina física

La máquina en la que se ha implementado la plataforma utiliza el Sistema Operativo CentOS 5. La versión del núcleo es la 2.6.18-8.1.15. Dispone de un procesador Core 2 Duo a 2.40 GHz, 2MB de Cache nivel 2, y 4GB de memoria RAM. Las máquinas virtuales también trabajan con CentOS 5. La versión de Xen es la 3.03-25.0.4.

Durante las pruebas se ha monitorizado la utilización de la CPU, para evitar la influencia de la carga del procesador en las medidas. La utilización nunca ha excedido el 10%.

E. Herramientas software

En esta sección se van a explicar las herramientas *software* utilizadas para implementar el sistema CAC en la plataforma. Para ahorrar carga computacional, sólo se han utilizado herramientas de línea de comandos.

En primer lugar, se requiere un *proxy* SIP instalado en el agente local. La herramienta seleccionada debe incluir la opción *redirect server* y la posibilidad de ser adaptable para que las decisiones de CAC puedan ser implementadas. También debe ser capaz de acceder a información externa situada en la base de datos. Se ha seleccionado OpenSIPS 1.4, un proyecto derivado de OpenSER, ya que proporciona funcionalidades de *register server, location server, proxy server y redirect server*. La baja carga computacional y la posibilidad de añadir y eliminar funcionalidades de forma modular son también características interesantes. La configuración del *proxy* SIP se realiza con un lenguaje de programación de alto nivel. También se dispone de acceso a bases de datos MySQL.

La centralita utilizada es Asterisk 1.6, una solución interesante por su flexibilidad, actualizaciones y licencia de distribución GNU-GPL. Por último, se eligió el *softphone* de línea de comandos PJSUA 1.0, también utilizado para emular los *gateway*, ya que no se usan conexiones reales a la RTC .

V. Pruebas y resultados

A. Automatización de realizaciones

Se ha realizado una batería de pruebas para caracterizar el comportamiento del sistema. Se ha construido un escenario que contiene un centro de datos y cuatro sucursales, cada una con una conexión de subida de 1 Mbps, conectadas con una red IP. Para emular la Hora Cargada, en primer lugar se ha generado *offline* con Matlab una hora de llamadas, haciendo uso de distribuciones de probabilidad para generar los instantes de las llamadas y su duración.

Posteriormente se emula dicha realización utilizando una herramienta de automatización de aplicaciones llamada *Expect*, aprovechando que el *softphone* usado es de línea de comandos. Como se utiliza emulación, el tiempo de la ejecución es tiempo real, así que se requiere una hora para cada ejecución. Así, el tráfico del sistema es real, no simulado. El tráfico SIP se genera en los *softphone* PJSUA, mientras que el tráfico RTP se genera con D-ITG [20], por razones prácticas. Durante la ejecución se intenta evitar cualquier cálculo innecesario. Los ficheros *log* del tráfico RTP y parte de la señalización SIP son almacenados en la base de datos, de manera que al finalizar la realización se puedan procesar *offline* para obtener resultados. El procesado del tráfico RTP se realiza con la aplicación ITG-Dec del generador D-ITG, que calcula el OWD, las pérdidas y otros parámetros.

El escenario utilizado para las medidas se puede ver en la Fig. 7. El tráfico interferente tiene la siguiente distribución: el 50% de los paquetes son de 40 bytes, el 10% de 576 bytes y el 40% de 1.500 bytes, todos ellos a nivel IP [21]. Este tráfico se ha generado para saturar el enlace de acceso de cada sucursal. Se ha utilizado UDP en lugar de TCP, para evitar el control de flujo que TCP realiza por defecto. Así, el tráfico interferente siempre es el mismo, y no se adapta al ancho de banda disponible, haciendo que el sistema trabaje siempre en el peor caso.

El tráfico SIP se dirige en primer lugar al *proxy*, después a la centralita y por último al *proxy* destino. El tráfico RTP se envía directamente entre los *softphone*. Cada flujo RTP tiene un ancho de banda de 24 kbps a nivel IP, o 29,6 kbps a nivel ethernet. Se ha utilizado el *codec* G.729, con dos muestras por paquete, que implica un retardo de paquetización de 25 ms, incluyendo un *look-ahead* de 5 ms.

Como se ha dicho, los *router* de cada sucursal tienen una conexión en el enlace de subida de 1 Mbps. Esto se ha conseguido gracias a la herramienta *tc*, utilizando una cola *token bucket* que limita el ancho de banda a nivel 2. El

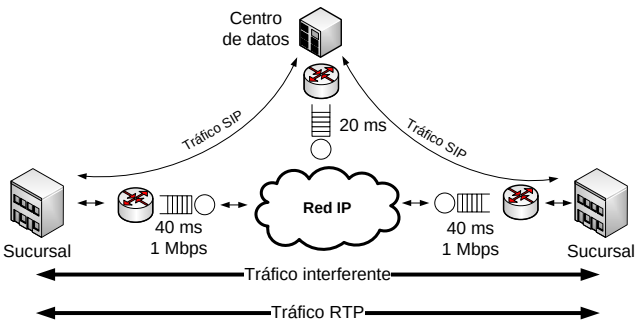


Fig. 7. Esquema de medidas

retardo de los paquetes RTP no debería superar el valor de 150 ms, como recomienda la ITU [22]. Como la red IP emulada introduce un retardo medio de 40 ms, el tamaño del *buffer* se ha calculado para que los paquetes permanezcan encolados un tiempo máximo de 50 ms. En el centro de datos se ha introducido un retardo medio de 20 ms.

B. Resultados

En primer lugar se ha medido el retardo de establecimiento de las llamadas para distintos valores de tráfico interferente. Los resultados se pueden ver en la Tabla V-B. Se compara la situación en la que los *softphone* están directamente registrados en la centralita (sin CAC), con la del comportamiento del sistema CAC, utilizando los *proxy*. Se observa un retardo adicional cuando se introduce el sistema CAC, debido a la presencia de los *proxy* como elementos intermedios, aunque los valores obtenidos no son excesivos y se pueden asumir. Si los enlaces están saturados, el retardo adicional es prácticamente igual para ambos casos, ya que depende mucho del retardo de encolado.

También se han realizado pruebas para obtener los límites de comportamiento del sistema. La existencia de las colas juega un papel muy importante en dicho comportamiento. En [23], los autores sugieren el uso de *buffer* pequeños. En este trabajo hemos supuesto que se puede limitar el tamaño de las colas de los *router*. En la Fig. 8 se observa que cuando el tráfico se acerca al límite del ancho de banda (1 Mbps), los paquetes comienzan a ser descartados, siendo los de mayor tamaño los que se descartan en mayor medida. Esto empieza a ocurrir cuando el número de flujos RTP es 7, ya que tenemos 800 kbps de tráfico interferente y más de 200 kbps de tráfico RTP. La Fig. 9 muestra que los paquetes pequeños mantienen su ancho de banda, mientras que los paquetes grandes son descartados en mayor número, ya que permanecen demasiado tiempo encolados. El hecho de que el tráfico total supere ligeramente el valor de 1 Mbps se debe a la tolerancia de la herramienta *tc*.

Este resultado muestra que el tráfico RTP está protegido frente al descarte debido a su pequeño tamaño. Así que limitar el número máximo de llamadas simultáneas es también importante para evitar la degradación del resto de tráfico de la sucursal. Esto significa que podemos utilizar el sistema CAC no sólo para proteger el tráfico RTP frente al descarte, sino también para evitar la degradación del tráfico interferente.

Las Fig. 10, 11 y 12 muestran el comportamiento del sistema en términos de retardo medio, paquetes perdidos y

Tráfico interferente	850 kbps	900 kbps	950 kbps	1000 kbps
No CAC	83 ms	87 ms	87 ms	199 ms
CAC	175 ms	183 ms	184 ms	205 ms

Tabla I
RETARDO DE ESTABLECIMIENTO DE LAS LLAMADAS

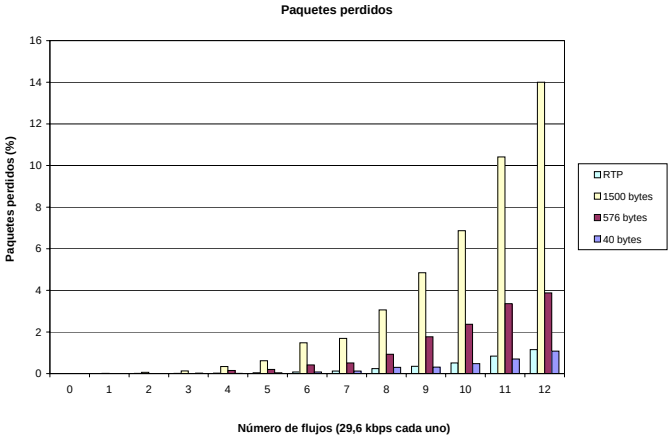


Fig. 8. Paquetes perdidos en el sistema con 800 kbps de tráfico interferente

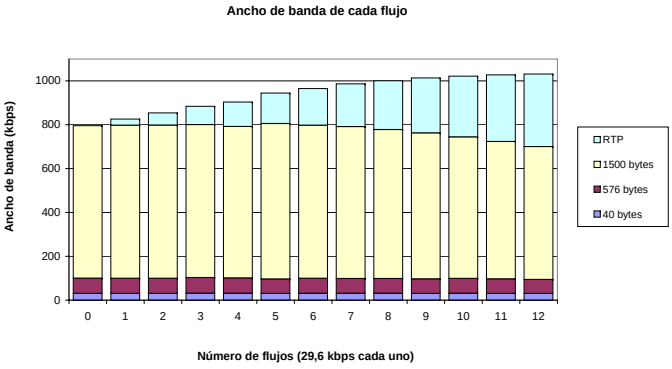


Fig. 9. Anchos de banda en el sistema con 800 kbps de tráfico interferente

jitter. Estas curvas muestran el límite superior para estos parámetros en el caso de tener el máximo número de llamadas posibles con el sistema CAC. Los valores se representan en función del tráfico interferente, de manera que cada gráfica tiene un momento diferente en el cual el tráfico total supera el límite del ancho de banda, y comienza la degradación del sistema. Si representamos estos parámetros en función del tráfico total, las gráficas se acercan entre sí (Fig. 14, 15 y 16). Las Fig. 13 y 17 muestran el comportamiento en términos del MOS. Estos valores se calculan según la recomendación G.107 [24], partiendo de la Relación Señal a Ruido (SNR, *Signal to Noise Ratio*) y teniendo en cuenta diferentes factores que reducen la calidad de la señal. Para obtener estos valores hemos utilizado una aplicación desarrollada por la ITU [25].

En la Fig. 12 observamos el comportamiento del sistema en términos del *jitter*. Para medirlo se ha utilizado el IPDV (*Instantaneous Packet Delay Variation*). Presenta un máximo, y decrece según el acceso se va saturando. La razón es que los paquetes grandes comienzan a ser descartados en mayor porcentaje, y estos paquetes son la principal causa del *jitter*. Los valores de *jitter* se mantienen por debajo de 12 ms.

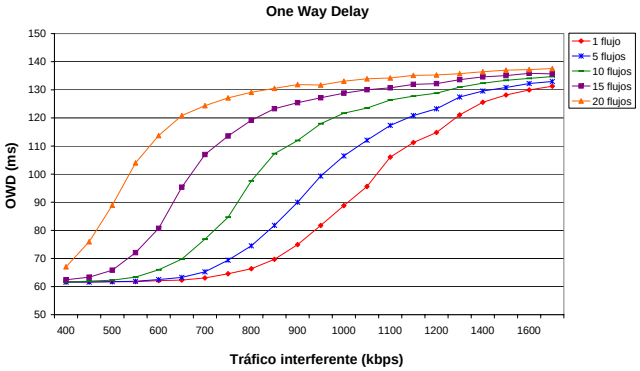


Fig. 10. *One Way Delay* en función del tráfico interferente

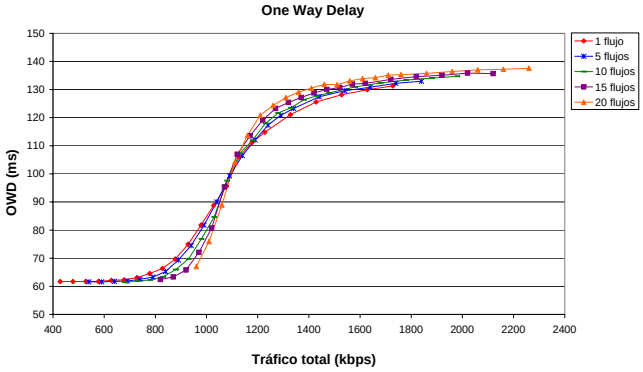


Fig. 14. *One Way Delay* en función del tráfico total

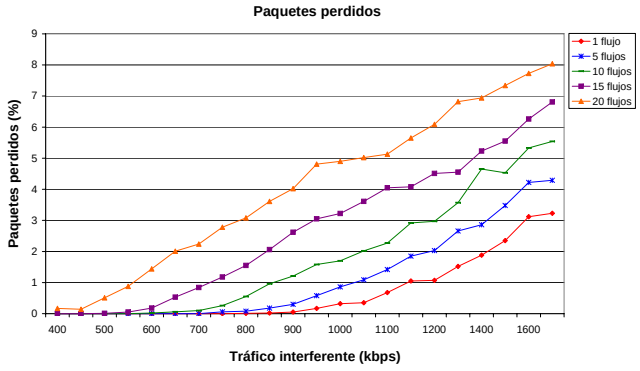


Fig. 11. Paquetes perdidos en función del tráfico interferente

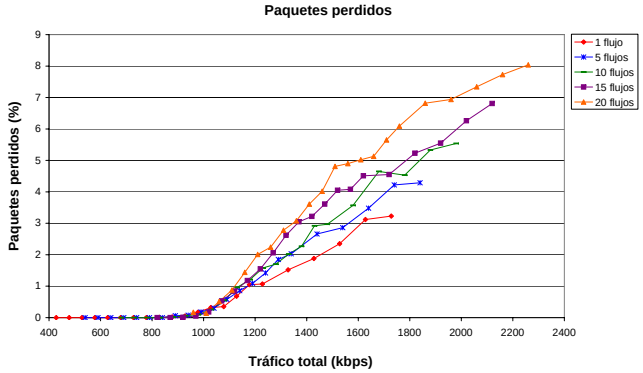


Fig. 15. Paquetes perdidos en función del tráfico total

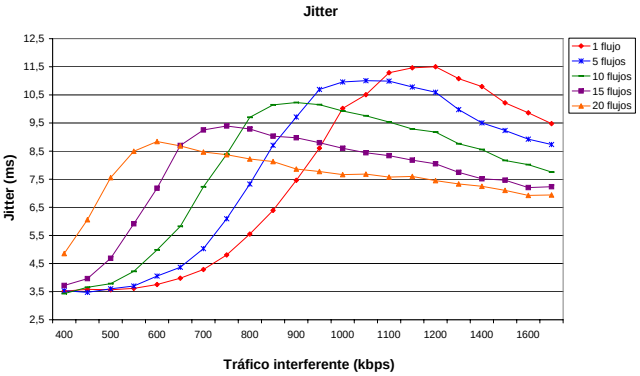


Fig. 12. *Jitter* en función del tráfico interferente

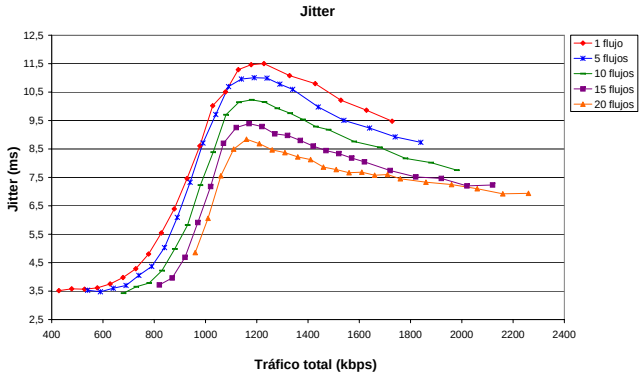


Fig. 16. *Jitter* en función del tráfico total

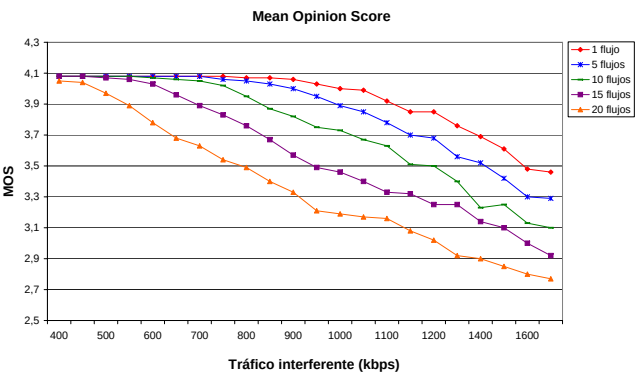


Fig. 13. MOS en función del tráfico interferente

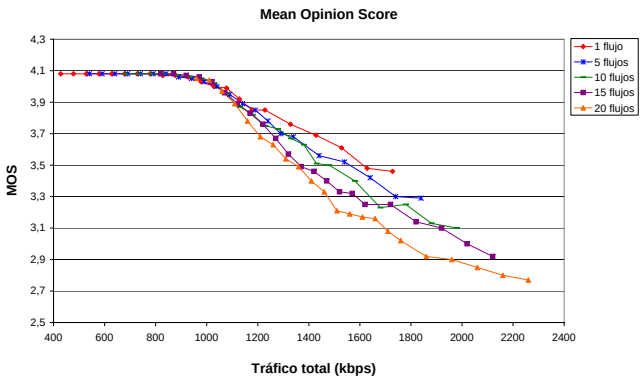


Fig. 17. MOS en función del tráfico total

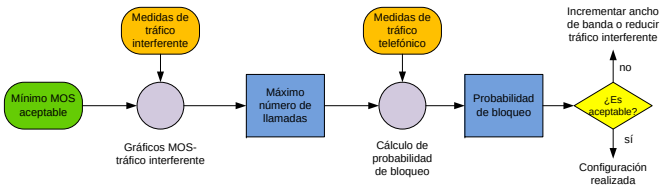


Fig. 18. Diagrama de flujo para configurar el sistema CAC

C. Configuración del sistema CAC

Se ha podido comprobar que existe un compromiso entre la QoS de las llamadas y la probabilidad de admisión del sistema. Por tanto, los pasos para configurar el sistema CAC son (Fig. 18): en primer lugar, se mide el tráfico interferente y el tráfico telefónico de la sucursal en la Hora Cargada; después, se decide un valor mínimo de MOS que sea aceptable para las llamadas y utilizando la Fig. 13 se obtiene el máximo número de llamadas simultáneas. Entonces, usando un método tradicional, como por ejemplo las tablas Erlang, se calcula la probabilidad de rechazo del sistema. Si este valor resulta inaceptable, la solución pasa por reducir el tráfico de fondo o incrementar el ancho de banda.

VI. Conclusiones y líneas futuras

Se ha integrado un sistema CAC con una centralita *software* para añadir QoS a un sistema de telefonía IP que trabaja con SIP. El sistema utiliza un *proxy* SIP para aceptar o rechazar las llamadas dependiendo de unos parámetros establecidos en el tiempo de configuración.

El sistema se ha implementado en una plataforma de pruebas basada en virtualización. Cada elemento del sistema se traslada a una máquina virtual. Se han añadido retardos en la red y anchos de banda para obtener una situación más realista.

Existe una primera fase en la que las llamadas se simulan, realizándose después con tráfico real. Las medidas muestran que el sistema no introduce retardos que podrían afectar la calidad experimentada por los usuarios. Actualmente se está añadiendo al sistema un modo basado en medidas, instalando un subsistema de medidas en el agente local, que modifica el máximo número de llamadas dependiendo de las condiciones de la red.

También se puede concluir que nuestro sistema permite intercambiar la probabilidad de bloqueo entre los *gateway* y la red IP. Pero si no se desea incrementar la probabilidad de bloqueo, existen dos soluciones: reducir el tráfico interferente o incrementar el ancho de banda, que será probablemente más económico que incrementar el número de líneas del *gateway*.

Agradecimientos

Este trabajo está parcialmente financiado por el proyecto RUBENS, del proyecto EUREKA CELTIC (código EU-3187 CP5-020) Europeo, el proyecto TSI-020400-2008-020 del subprograma AVANZA I+D, del Ministerio Español de Industria, Turismo y Comercio, el proyecto Cheque Tecnológico 2009/2010, de la Agencia Aragón I+D, del Gobierno de Aragón, y el proyecto Cátedra Telefónica, de la Universidad de Zaragoza.

Referencias

[1] X. Chen, C. Wang, D. Xuan, Z. Li, Y. Min, W.Zhao, "Survey on QoS Management of VoIP" , *In Proc. of the 2003 International Conference on Computer Networks and Mobile Computing, IEEE Computer Society.*

[2] A. Bavier, M. Bowman, B. Chun, D. Culler, S. Karlin, S. Muir, L. Peterson, T. Roscoe, T. Spalink, M. Wawrzoniak, "Operating System Support for Planetary-Scale Network Services", *in Proc. of the 1st USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI '04)*, San Francisco, CA, 2004.

[3] P. K. Biswas, C.Serban, A. Poylisher, J. Lee, S. Mau, R. Chadha, C. J. Chiang, R. Orlando, K. Jakubowski, "An integrated testbed for Virtual Ad Hoc Networks", *5th International Conference on Testbeds and Research Infrastructures for the Development of Networks Communities and Workshops Tridentcom 2009*, pp.1-10, 2009.

[4] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, Ch. Barb, A. Joglekar, "'An integrated experimental environment for distributed systems and networks"', in Proc. 5th symposium on Operating systems design and implementations, Boston, 2002.

[5] T. R. Henderson, M. Lacage, G. F. Riley, "Network Simulations with the ns-3 Simulator", *demo paper at ACM SIGCOMM'08*, ago. 2008.

[6] 3GPP TS 24.228 v5.15.0, Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), Stage 3, R5, sep. 2006.

[7] SIP: Measurement-Based Call Admission Control for SIP, http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftcacsip.pdf.

[8] M. Ahmed and A. Malik Mansor, "CPU dimensioning on performance of Asterisk VoIP PBX", 11th Communications and Networking Simulation Symposium (CNS 2008), Ottawa, abr. 2008.

[9] VoIP Call Admission Control, http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/CAC.pdf

[10] R. Solange Lima, P. Carvalho and V. Freitas, "Admission Control in Multiservice IP Networks: Architectural Issues and Trends", IEEE Communications, Vol. 45 No. 4, abr. 2007, 114-121.

[11] S. Wang, Z. Mai, D. Xuan, W. Zhao, "Design and implementation of QoS-provisioning system for voice over IP", Parallel and Distributed Systems, IEEE Transactions on, vol.17, no.3, pp. 276-288, mar.2006.

[12] S. Wanke, M. Scharf, S. Kiesel and S. Wahl, "Measurement of the SIP Parsing Performance in the SIP Express Router", Proc. 13th Open Eur. Summer School and IFIP TC6.6Workshop (EUNICE 07) Enschede, Neth., 2007.

[13] J. Saldaña, E. Viruete, J. Fernández-Navajas, J. Ruiz-Mas, J. I. Aznar, "Hybrid Testbed for Network Scenarios". SIMUTools 2010, the Third International Conference on Simulation Tools and Techniques. Torremolinos, Malaga (Spain), mar. 2010.

[14] E. Alipour, K. Mohammadi, "Adaptive Admission Control for Quality of Service Guarantee in Differentiated Services Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, jun. 2008.

[15] H. Tran, T. Ziegler, F. Ricciato, "QoS Provisioning for VoIP Traffic by Deploying Admission Control. Architectures for Quality of Service in the Internet", Springer Berlin/Heidelberg, Vol. 2698/2003, pp. 1084-1085.

[16] J. Zhou, Z. Ji, R. Bagrodia, "TWINE: A Hybrid Emulation Testbed for Wireless Networks and Applications". Proc. IEEE INFOCOM 2006.

[17] X. Jiang, D. Xu, "vBET: a vm-based emulation testbed", Proc. of the ACM SIGCOMM workshop on Models, methods and tools for reproducible network research (MoMeTools03). New York, NY, USA: ACM Press, 2003, pp. 95-104.

[18] B. Quetier,V. Neri, F. Cappello, "Selecting a Virtualization System For Grid/P2P Large Scale Emulation", In Proc. of the Workshop on Experimental Grid testbeds for the assessment of large-scale distributed applications and tools (EXPGRID'06), Paris, France.

[19] S. Hemminger, "'Network Emulation with NetEm", Proc Linux Conference AU, Canberra, 2005.

[20] S. Avallone, S. Guadagno, D. Emma, A. Pescapè, G. Ventre, "D-ITG Distributed Internet Traffic Generator" QEST , IEEE Computer Society, pp. 316-317, 2004.

[21] Cooperative Association for Internet Data Analysis "NASA Ames Internet Exchange Packet Length Distributions".

[22] One-way transmission time (recommendation G.114). International Telecommunication Union (ITU), feb. 1996.

[23] D. Wischik, N. McKeown, "Part I: buffer sizes for core routers". SIGCOMM Comput. Commun. Rev. 35, 3 (jul. 2005), 75-78.

[24] "'The E-model, a computational model for use in a transmission planning"', ITU-T Recommendation G.107, Mar. 2003

[25] http://www.itu.int/ITU-T/studygroups/com12/emodelv1/calcul.php

SISTEMA DE RECOMENDACIÓN EN UNA PLATAFORMA DE DISTRIBUCIÓN DE CONTENIDOS AUDIOVISUALES

José Mª Quinteiro González[1], Ernestina A. Martel Jordán[1], Pablo Hernández Morera[1], Ángelo Santana del Pino[2], Aaron López Rodríguez[1], Leidia Martel Monagas[1]
[1]IUMA Sistemas de Información y Comunicaciones-División Tecnología de la Información- Departamento de Ingeniería Telemática, [2] Departamento de Matemáticas
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira, s/n.
{jquinteiro, emartel,pablo,alopez,lmonagas}@iuma.ulpgc.es, angelo@dma.ulpgc.es

***Resumen*- Una de las tareas principales de los servicios de información es ayudar a los usuarios a que encuentren la información que satisfaga sus preferencias minimizando el esfuerzo de búsqueda. Para este propósito los sistemas de recomendación filtran la información, presentándole al usuario la más acorde con su perfil. Las ontologías, elemento fundamental de la Web Semántica, se han utilizado como mecanismo para generar recomendaciones más seguras y personalizadas mediante la inferencia de las preferencias de usuario no conocidas. En este artículo se presenta un motor de recomendación de contenidos audiovisuales que utiliza el filtrado basado en ontologías para generar recomendaciones a partir del perfil del usuario y su interacción en la plataforma. Este motor también se ha utilizado para conseguir publicidad dirigida al usuario de la plataforma.**

Palabras Clave- Sistemas de recomendación, Ontología, Personalización, Publicidad dirigida

I. INTRODUCCIÓN

Uno de los grandes retos que hoy en día tienen que afrontar los servicios de información es la gestión de grandes volúmenes de información que faciliten a los consumidores el acceso a recursos que satisfagan sus necesidades de una manera rápida, eficaz y transparente. Esta necesidad se vuelve más acuciante en Internet donde los usuarios reciben una gran cantidad de información que deben filtrar para conseguir los contenidos que les resulten de interés. En este punto es donde los sistemas de recomendación juegan un papel importante.

Una de las técnicas de recomendación más extendida es el filtrado colaborativo [1]. Este tipo de filtrado consiste en encontrar usuarios con gustos similares a los de un usuario determinado y recomendar a éste ítems que desconoce pero que gustan a aquellos usuarios con los que mantiene similitud. El filtrado colaborativo obtiene las preferencias de los usuarios a partir de una matriz en la que se almacenan las valoraciones que los usuarios han otorgado a los ítems.

Desafortunadamente los sistemas de recomendación que utilizan el filtrado colaborativo presentan problemas de dispersión (*sparsity*) y arranque en frío (*cold-start*) [2,3]. La *dispersión* hace referencia al pequeño porcentaje que representa la cantidad de ítems valorados frente al número total, lo que disminuye la probabilidad de encontrar usuarios que hayan valorado los mismos ítems, causando un aumento del tiempo de cómputo y dificultades para escalar el sistema. Las técnicas de agrupamiento (*clustering*) solucionan parte de estos problemas a costa de perder exactitud en la recomendación [4]. El *arranque en frío* hace referencia a la imposibilidad de realizar recomendaciones ante la falta de valoraciones, así se distingue entre *cold-start system*, cuando el sistema arranca por primera vez; *cold-start user*, cuando se incorpora un nuevo usuario; y *cold-start ítem*, cuando se incorpora en el sistema un nuevo producto [5].

Otra técnica de recomendación existente, aunque menos utilizada que la anterior, es el filtrado basado en contenido [6]. Éste se centra en localizar productos similares a las preferencias manifestadas por el propio usuario en su perfil. Esta técnica no sufre los problemas de arranque en frío porque permite recomendar un producto antes de que nadie lo haya adquirido. Sin embargo, siempre recomienda productos similares a los ya adquiridos (sobre-especialización), y requiere que los productos se acompañen de una descripción de su contenido, tarea que no resulta fácil de automatizar para ciertos tipos de contenido (video, imagen, música, etc.).

Una propuesta para solucionar los problemas expuestos anteriormente consiste en utilizar la técnica de filtrado basado en ontologías (*ontology filtering*) propuesta en [7]. Esta técnica infiere las valoraciones que un usuario daría a un ítem a partir de una ontología del dominio y de valoraciones realizadas sobre otros ítems. Esta ontología se puede construir de forma automática o manual mediante diferentes técnicas de agrupamiento.

En este artículo aplicamos una versión mejorada de la técnica de filtrado basado en ontologías en una plataforma de distribución de contenidos audiovisuales. En concreto la técnica de filtrado se ha utilizado para recomendar

contenidos audiovisuales a los usuarios de la plataforma en función de su perfil y del uso de la plataforma. En dicha plataforma la personalización de contenidos audiovisuales se acompaña de publicidad dirigida a los intereses del usuario.

El resto del artículo se estructura como sigue: en la sección II presentamos el contexto en el que se ha desarrollado la personalización de contenidos multimedia y la publicidad dirigida, y se introduce la técnica de filtrado basado en ontologías utilizada para la recomendación de contenidos multimedia. Esta recomendación dentro de la plataforma de distribución de contenidos multimedia la realiza el gestor de personalización, que se presenta en la sección III. Este gestor se utiliza para construir el gestor de publicidad de la plataforma que se presenta en la sección IV. A continuación se realizan una serie de experimentos para evaluar el rendimiento del motor de recomendación de la plataforma y, finalmente se presenta el trabajo relacionado y se establecen conclusiones y líneas futuras.

II. ANTECEDENTES

En este apartado se presenta la plataforma de distribución de contenidos audiovisuales, Raudos, en la que se incluye el sistema de recomendación de este artículo. Asimismo en este apartado se comparan diferentes mecanismos de recomendación y se selecciona la técnica de filtrado basado en ontologías como la más adecuada para el motor de recomendación de Raudos.

A. Raudos

Raudos [8] es una red interactiva multiplataforma de contenidos audiovisuales desarrollada en un proyecto del Ministerio de Industria y Comercio a través del Plan Avanza I+D. En este proyecto han colaborado un consorcio de once universidades, centros tecnológicos y empresas.

El principal objetivo de Raudos se centra en la creación de una plataforma que permita aprovechar las potencialidades de las redes para difundir legalmente contenidos audiovisuales generando de esta forma un nuevo modelo de distribución de contenidos audiovisuales.

Un usuario de Raudos se conecta a la plataforma a través de un nombre de usuario y contraseña. Una vez dentro, interactúa con una serie de aplicaciones de carácter lúdico o formativo no reglado, que le permiten ganar puntos e ir incrementando su saldo virtual, con el asesoramiento de personajes virtuales. Se puede interactuar a través de cualquier dispositivo conectado a la red (ordenador, teléfono móvil, PDA, TV, etc.). Con el crédito virtual disponible, el usuario tiene acceso a un catálogo de contenidos audiovisuales desde cualquiera de las plataformas mencionadas para el visionado.

El sistema fomenta así el consumo autorizado de material audiovisual sin coste real para el cliente final y abriendo potenciales modelos innovadores de explotación publicitaria.

En la Fig. 1 se presenta la arquitectura de Raudos que básicamente está formada por repositorios, gestores y un portal de acceso. Esta arquitectura sigue el modelo de arquitectura orientada a servicios en el que cada gestor proporciona su funcionalidad mediante servicios web.

El *gestor de usuarios* se encarga de la autenticación de los usuarios en la plataforma y de mantener la sesión activa de forma transparente para el resto de los gestores. Este gestor constituye la puerta de entrada a la plataforma.

El *gestor de contenidos* proporciona todos los recursos audiovisuales que se ofrecerán a través del portal de Raudos. Estos recursos previamente han sido catalogados y etiquetados de forma que faciliten las búsquedas y el acceso a contenidos específicos por parte del resto de gestores.

El *gestor de actividades* se centra en proporcionar actividades lúdicas o formativas no regladas que estarán disponibles a los usuarios. Estas actividades fomentan el uso de la plataforma proporcionando puntos que incrementan el saldo virtual del usuario dentro de la plataforma. Mediante estas actividades se va completando el perfil inicial que el usuario cumplimentó cuando ingresó por primera vez en la plataforma.

El *gestor de personajes virtuales* controla la aparición y gestión de personajes virtuales que interactúan con el usuario. La información recibida del gestor de personalización permite configurar a los personajes virtuales de forma que se facilite la interacción fluida y agradable entre usuario y sistema.

El *gestor de estadística* se encarga de almacenar los indicadores de funcionamiento de Raudos proporcionando un cuadro de mandos integral para la gestión del sistema.

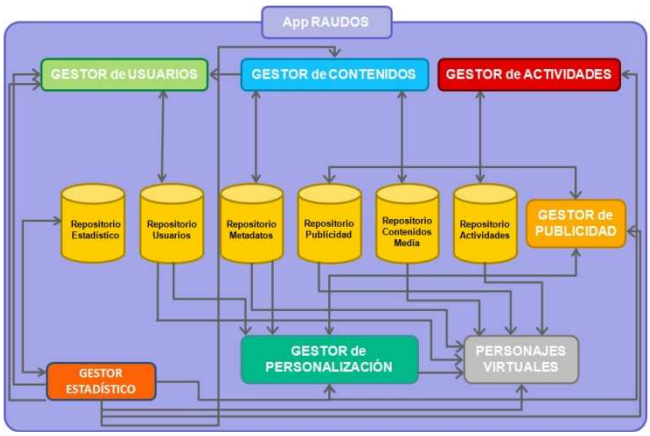


Fig. 1. Arquitectura de Raudos.

Los gestores de personalización y publicidad se presentan en más detalle posteriormente.

B. Análisis de mecanismos de recomendación

Uno de los mecanismos de recomendación más extendidos es el de *filtrado colaborativo* [1], también llamado social. Las recomendaciones proporcionadas por los sistemas colaborativos se calculan en base a las similitudes entre distintos elementos del dominio sobre el que aplicamos el sistema recomendador. Así, el cálculo de las similitudes puede realizarse entre usuarios o entre productos. Mediante el cálculo de similitudes entre usuarios se localiza un grupo de usuarios afín al usuario activo, y en base a las votaciones sobre productos que no conoce el usuario activo se realizan las recomendaciones. Mediante el cálculo de similitudes

entre productos se identifica el grupo de productos más afín a cada uno de los productos de nuestro catálogo. Y en base a los productos valorados positivamente por el usuario activo, elaboramos las recomendaciones sobre los más afines a éstos. En este tipo de filtrado las preferencias de los usuarios no se consideran de forma explícita, sino de forma implícita a partir de las valoraciones que los usuarios otorguen a un conjunto de ítems.

A pesar de la popularidad del filtrado colaborativo, éste presenta el problema de arranque en frío y dispersión. En ambos casos se requiere que existan suficientes valoraciones por parte del usuario cuando el motor de recomendación comience a funcionar. La técnica de *filtrado basado en ontologías* [7] mitiga estos problemas recurriendo a una taxonomía sobre el dominio de los productos, y a un mecanismo de inferencia que permite determinar las preferencias de los usuarios en base a la cercanía taxonómica de otros productos valorados por el usuario.

C. Filtrado basado en ontologías

El *filtrado basado en ontologías* presentado en [7] es una técnica de recomendación que utiliza una ontología para modelar el conjunto de ítems de su catálogo, y para inferir las preferencias de un usuario. Los datos de entrada al sistema son: la matriz de valoraciones usuario-ítem y la ontología del dominio.

La ontología se representa mediante una estructura de árbol donde un nodo representa un concepto, y un arco modela la relación *is_a* entre dos conceptos. Un ítem es un objeto de un concepto, y los arcos representan características que diferencian el conjunto de subconceptos de un mismo padre. Cada concepto puede tener un conjunto de sub-conceptos, pero no todos los objetos de un concepto deben pertenecer a un sub-concepto.

Cada concepto *c* tiene dos propiedades: el *score* (*S*(*c*)) y el *a-priori score* (*APS*(*c*)). La primera representa cuánto le gusta a un usuario determinado un concepto dado, calculado como una media de las valoraciones dadas a los ítems pertenecientes al concepto *c*, mientras la última propiedad determina los parámetros de propagación de las valoraciones entre los sub-conceptos y el concepto *c*, considerando tan sólo la ubicación del concepto *c* en la ontología. Este valor no se utiliza para predecir valoraciones, sino para conocer cómo las valoraciones se propagan por el grafo de la ontología.

El sistema recomendador emplea estas dos propiedades para inferir las valoraciones de un usuario a un concepto no valorado *y*. El sistema utiliza las valoraciones del usuario *S*(*x*) asociadas al concepto más cercano *x*, y el *lowest common ancestor* a los conceptos *x* e *y* en la ontología. Formalmente, la valoración del concepto *y* inferida desde la valoración del concepto *x* es:

$$S(y/x) = \left(\frac{APS(lca)}{APS(x)}\right) S(x) + (APS(y) - APS(lca)) \quad (1)$$

donde *lca* es el *lowest common ancestor* entre los conceptos *x* e *y*.

Las recomendaciones se elaboran buscando ítems no conocidos por el usuario, pertenecientes a conceptos con la más alta valoración y que sean también populares:

$$\rho S(c) + (1-\rho)P(c) \quad (2)$$

donde $P(c)$ es el grado de popularidad del concepto *c*, calculado como la media de las valoraciones de todos los usuarios sobre los ítems del concepto *c*, y ρ es un parámetro en el intervalo [0,1].

Los cambios en el conjunto de ítems son incorporados en el catálogo, gracias al uso de algoritmos de agrupamiento para construir las ontologías a partir de las valoraciones de los usuarios, de forma autónoma sin la intervención de ningún experto. Como algoritmos de agrupamiento se utilizan el aglomerativo y partitivo. La similitud entre ítems se calcula mediante el coseno ajustado y posteriormente se utiliza un *criteria function* para optimizar la construcción de los clusters de ítems. Los *criteria function* utilizados para construir las ontologías son las mostradas en la tabla 1.

Tabla 1. *Criteria functions* utilizados por los algoritmos de agrupamiento

1	$\mathcal{I}_1$	$maximize \sum_{r=1}^{k} \frac{1}{n_r} \left(\sum_{i,j \in C_r} sim(i,j) \right)$
2	$\mathcal{I}_2$	$maximize \sum_{r=1}^{k} \sum_{i \in C_r} sim(i, C_r^t)$
3	$\mathcal{E}_1$	$maximize \sum_{r=1}^{k} n_r \cdot sim(C_r^t, C)$
4	$\mathcal{G}_1$	$maximize \sum_{r=1}^{k} \frac{cut(C_r, C - C_r)}{\sum_{i,j \in C_r} sim(i,j)}$
5	$\mathcal{H}_1$	$maximize \frac{\mathcal{I}_1}{\mathcal{E}_1}$
6	$\mathcal{H}_2$	$maximize \frac{\mathcal{I}_2}{\mathcal{E}_1}$
7	$slink$	$max_{i \in C_i, j \in C_j} sim(i,j)$
8	$clink$	$min_{i \in C_i, j \in C_j} sim(i,j)$
9	$UPGMA$	$maximize \frac{1}{n_i, n_j} \sum_{i \in C_i, j \in C_j} sim(i,j)$

donde *k* es el número de cluster a considerar, C_r representa el cluster *r*, n_r denota el número de elementos en el cluster *r*, C_r^t es el centroide del cluster *r*, y *sim*(*i*,*j*) es la similitud entre los ítems *i* y *j*.

Combinando los *criteria functions* de la tabla 1 y los algoritmos de agrupamiento, el sistema genera 15 diferentes ontologías (aglomerativo con *criteria function* 1 a 9, partitivo con *criteria function* 1 a 6). En vez de utilizar la misma ontología para todos los usuarios, se selecciona la mejor para cada uno de los usuarios, basándose en el perfil de preferencias del usuario con objeto de mejorar la exactitud de las recomendaciones.

Existen tres diferencias fundamentales entre el filtrado colaborativo y el filtrado basado en ontologías. En primer lugar el filtrado basado en ontologías determina la similitud entre ítems mediante una ontología jerárquica frente a la matriz de similitud ítem-ítem utilizada por el filtrado colaborativo. Este razonamiento jerárquico permite reducir el espacio de búsqueda, limitando así el número de valoraciones que el sistema tiene que obtener del usuario.

Los resultados experimentales [9] indican que el filtrado basado en ontologías mejora la seguridad de las predicciones frente al filtrado colaborativo, especialmente cuando se tienen pocos datos del usuario. En segundo lugar el filtrado basado en ontologías infiere las valoraciones a partir del concepto más cercano en lugar de utilizar los vecinos. De esta forma se necesitan menos datos y se consigue que el filtrado basado en ontologías sea más escalable que el filtrado colaborativo. Finalmente, las preferencias de usuario se infieren a partir de la experiencia pasada del usuario en lugar de considerar preferencias de otros usuarios, permitiendo así incrementar la personalización de la lista de recomendaciones.

III. GESTOR DE PERSONALIZACIÓN

Este gestor proporciona la capacidad para seleccionar y presentar a los usuarios los contenidos más adecuados y de mayor interés de acuerdo con sus gustos y preferencias.

A. Descripción

Cuando el usuario entra por primera vez en la plataforma introduce de forma explícita algunos datos de su perfil (edad, sexo, nivel de estudios, etc.). En este instante se recogen aquellos datos más relevantes del perfil del usuario tanto mediante preguntas directas sobre su perfil como mediante una encuesta que permite completar los datos demográficos del usuario.

La primera vez, el gestor utiliza los datos del perfil inicial del usuario para seleccionar aquellos contenidos audiovisuales y actividades que puedan resultar de interés al usuario final. A medida que el usuario utiliza los servicios que le ofrece la plataforma, el motor se va realimentando con sus interacciones con el fin de mejorar las recomendaciones que finalmente presente al usuario. De esta forma el gestor de personalización va completando el perfil del usuario con información extraída de su comportamiento en la plataforma (valoraciones, clicks, etc.).

El gestor de personalización se ha desarrollado de forma que facilite su adaptación para recomendar diferentes tipos de contenidos. En el caso de Raudos el gestor de personalización se ha configurado para que recomiende contenidos audiovisuales, actividades y elementos publicitarios. Esto quiere decir que el motor del gestor de personalización se puede programar fácilmente para otros entornos en los que se precisa recomendar otros tipos de contenidos. Por ejemplo en una plataforma orientada al turismo el tipo de contenido a recomendar sería eventos orientados al turismo. Para este propósito simplemente bastaría con indicarle al gestor de personalización la estructura de datos con la información turística a considerar en las recomendaciones para que el gestor de personalización generase recomendaciones orientadas al turismo.

En definitiva cuántas más valoraciones se realicen acerca de las recomendaciones recibidas, el gestor de personalización de Raudos afinará sus sugerencias, mostrando al usuario sólo aquellos ítems (contenidos, elementos publicitarios, actividades) que le resulten más atractivos.

B. Arquitectura del motor de recomendación

La arquitectura del motor de recomendación se compone de tres capas: capa de presentación, capa de aplicación y capa de datos, tal y como se muestra en la Fig. 2.

La capa de presentación proporciona la interfaz de interacción con el usuario. La capa de aplicación contiene al motor de recomendación. La capa de datos alberga las bases de datos donde se almacenan las valoraciones de los usuarios, el catálogo de productos y la ontología escogida para cada usuario.

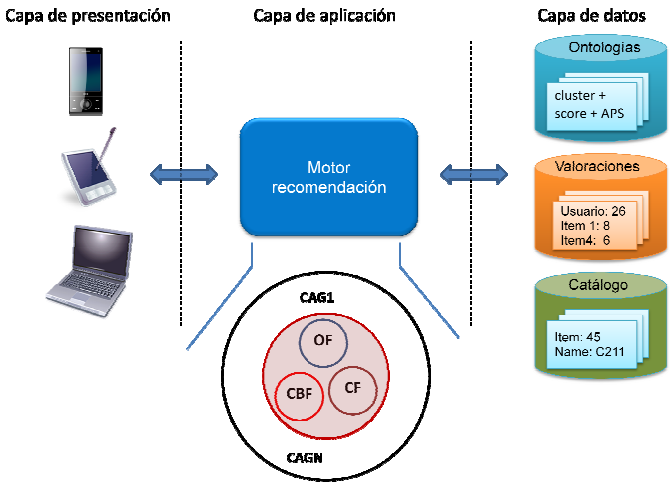


Fig. 2. Arquitectura del motor de recomendación.

El motor de recomendación tiene una arquitectura por capas, donde la capa más interna contiene los agentes que implementan las diversas técnicas de filtrado (colaborativa, basada en contenidos, basada en ontologías, etc.). Por encima de esta capa, se encuentran los controladores de agentes de recomendación (CAG) que permite configurar qué técnicas emplear y cómo combinarlas, así como determinar el conjunto de valoraciones de ítems, catálogo de productos y ontologías utilizar.

De esta forma, el sistema permite incorporar fácilmente nuevas técnicas de filtrado implementando el agente correspondiente.

Actualmente en Raudos se encuentran implementados el controlador para contenidos audiovisuales y el controlador para publicidad, y una única técnica de filtrado, el filtrado basado en ontologías.

Dentro del agente que implementa la técnica de filtrado basado en ontologías cabe distinguir dos componentes: el generador de ontologías y el generador de recomendaciones.

El generador de ontologías realiza, de modo off-line, la labor de construcción del abanico de ontologías indicado en el apartado II.C.; y de modo on-line elige y almacena la ontología más apropiada para cada usuario. Para acometer esta última tarea se divide el perfil de preferencias de cada usuario en un conjunto de entrenamiento y un conjunto de test. El conjunto de entrenamiento se utiliza para particularizar las ontologías a ese usuario, mientras que el conjunto de test se utiliza para evaluar los resultados y escoger la ontología más apropiada.

El generador de recomendaciones lleva a cabo las tareas necesarias para generar las recomendaciones, apoyándose en la ontología seleccionada, las valoraciones del usuario y el catálogo de productos.

IV. GESTOR DE PUBLICIDAD

Este gestor permite manejar toda la información relativa a la publicidad dentro de la plataforma Raudos que se mantiene en el repositorio de publicidad de la plataforma. Su funcionalidad se ha conseguido mediante dos enfoques, uno orientado al anunciante y otro al usuario final.

Desde el *punto de vista del anunciante*, el gestor de publicidad constituye una forma de garantizar que los anuncios alcancen la audiencia adecuada de forma efectiva. Este efecto se ha conseguido mediante un portal en el que los anunciantes definen sus campañas publicitarias como un conjunto de banners o elementos publicitarios, el *target* al que van dirigidas estas campañas y las características que debe reunir el área web en el que se insertará esta publicidad (ver página web mostrada en la Fig. 3).

Fig. 3. Página para inserción de anuncios.

Además, con el fin de asociar los anuncios a las preferencias de los usuarios, se ofrece la posibilidad de que un usuario pueda valorar los elementos publicitarios introducidos por los anunciantes (mediante la página mostrada en la Fig. 4). Esta posibilidad permite completar el perfil del usuario con la información extraída de las valoraciones que realice acerca de un conjunto de elementos publicitarios.

Desde *el punto de vista del usuario final*, el gestor de publicidad se encarga de proporcionar publicidad personalizada de acuerdo con el perfil del usuario y sus preferencias dentro de la plataforma Raudos. Este enfoque permite que la emisión de elementos publicitarios no se realice mediante un envío masivo a todos los usuarios de la plataforma, sino que permitirá difundir anuncios concretos sólo a aquellos usuarios que realmente les pueda interesar.

La publicidad personalizada utiliza el gestor de personalización de la plataforma Raudos para recomendar los anuncios a los usuarios en función de su perfil dentro de la plataforma. El gestor de personalización genera publicidad personalizada utilizando el perfil de usuario y la valoración de los elementos publicitarios.

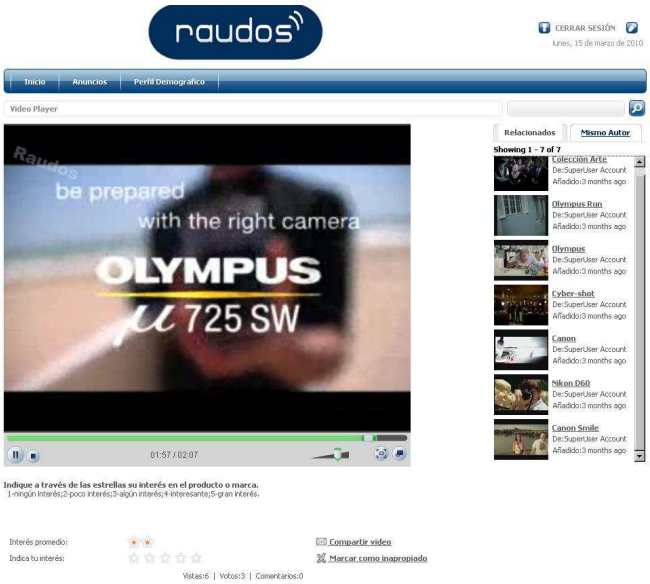


Fig. 4. Página de valoración de anuncios.

V. RESULTADOS EXPERIMENTALES

Se ha experimentado con una versión mejorada del motor de recomendación, consistente en la imputación de valores a la matriz de valoraciones usuario-ítem. El método de imputación utilizado ha sido el algoritmo de los *k* vecinos más cercanos [10].

Para evaluar la mejora obtenida mediante el sistema implementado de imputación de valores *knn* se hace uso del dataset de MovieLens [11], que contiene 100.000 valoraciones que 943 usuarios han realizados de 1.682 películas. De este dataset se ha trabajado con un subconjunto de 250 usuarios seleccionados aleatoriamente.

El conjunto de valoraciones de cada usuario es separado aleatoriamente en un conjunto de entrenamiento y un conjunto de test, de tal manera que el primero contenga el 90% de las valoraciones.

El conjunto de entrenamiento se emplea para generar las ontologías. Así, se han generado las 15 ontologías combinando los métodos aglomerativo y partitivo con cada uno de los *criteria function* indicados en la tabla 1 (aglomerativo con *criteria function* 1 a 9, partitivo con *criteria function* 1 a 6). De igual modo, se han generado otras 15 ontologías pero partiendo de las matrices de valoración usuario-ítem con imputación de datos. Todo esto ha dado lugar a un total de 30 ontologías, como se ilustra en la Fig. 5.

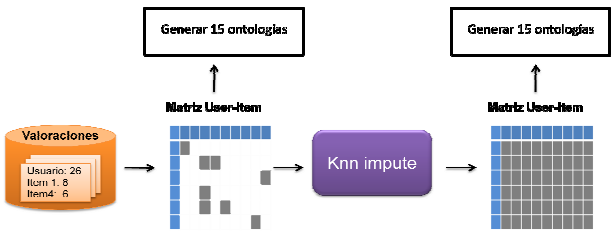


Fig. 5. Generación del conjunto de ontologías.

A continuación y para cada una de las ontologías generadas, se infieren las valoraciones para los conceptos existentes en el conjunto de test, de manera que la exactitud de los valores inferidos se basa en la valoración existente para esos conceptos en el conjunto de test, computándose el NMAE (*Normalized Mean Absolute Error*) [12] entre los conceptos para cada una de las 30 ontologías generadas.

Posteriormente se ha seleccionado la ontología con menor error medio. Los resultados obtenidos para un tamaño de cluster igual 5, se indican en la tabla 2, donde se muestra la cantidad de veces que un método de agrupamiento con un determinado *criteria function* ha sido seleccionado por devolver un error inferior al resto.

Tabla 2. Distribución de la ontología seleccionada para cada usuario.

		Método de agrupamiento			
		aglom.	*aglom-knn*	*part.*	*part-knn*
Criteria function	*1*	13	16	12	0
	2	6	8	4	4
	3	4	9	3	2
	4	9	3	0	11
	5	11	14	9	5
	6	3	8	2	2
	7	22	12	NA	NA
	8	8	25	NA	NA
	9	10	15	NA	NA
Total		86	110	30	24

En la tabla 2 se observa que más de la mitad, concretamente 134 usuarios, se benefician de la utilización de la imputación de valores mediante *knn*. Al mismo tiempo se pone de manifiesto que no existe una única ontología que recoja las particularidades de todos los usuarios.

En la Fig. 6 se muestra la magnitud de la mejora producida en los 134 usuarios.

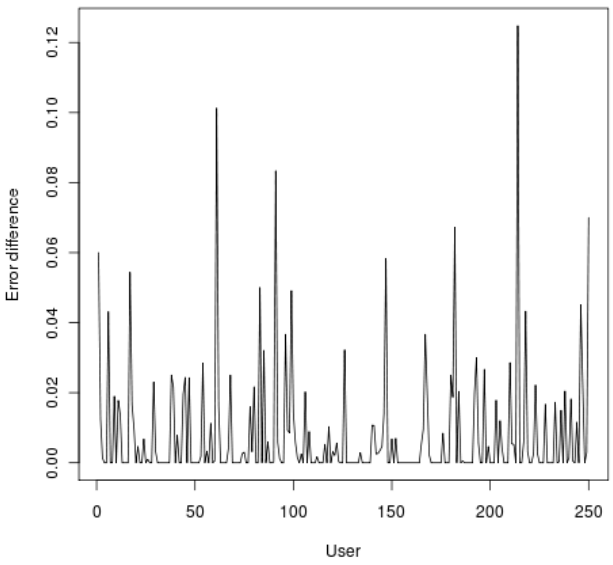


Fig. 6. Magnitud de la mejora con imputación de datos.

Siendo la media del error utilizando el método *ontology filtering* de 0.056, y en el caso de utilizar *ontology filtering* con imputación de valores basados en *knn* el valor es 0.048. En términos relativos ello significa una mejora del 14.1%.

Para determinar si esta diferencia entre los errores medios de ambos métodos es significativa se ha empleado el test de Wilcoxon para muestras emparejadas, ya que no hay normalidad en la distribución de los errores, tal como puede apreciarse en la Fig. 7.

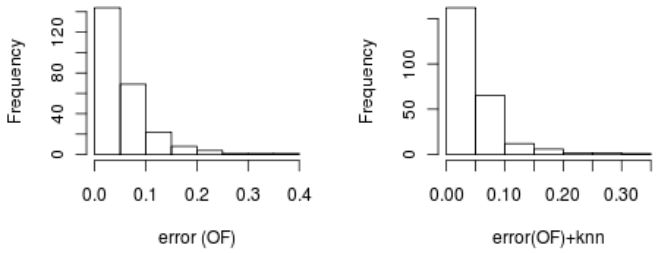


Fig. 7. Test de Wilcoxon.

El *p*-valor del test de Wilcoxon es inferior a 10^{-6} lo que indica que la diferencia entre la magnitud de los errores es significativa y no atribuible al azar.

VI. TRABAJO RELACIONADO

Esta sección la abordamos desde dos puntos de vista, el de recomendación de contenidos audiovisuales y el de la publicidad dirigida (*targeted advertising)*.

A. Sistemas de recomendación de contenidos audiovisuales

En [13] y [14] se presentan sistemas recomendadores de contenidos televisivos. [13] presenta AVATAR, un sistema de recomendación personalizada de contenidos televisivos basados en información semántica. Este trabajo utiliza técnicas bayesianas en combinación con razonamiento semántico, perfiles de usuario y logs de los programas visualizados por el usuario para generar recomendaciones de contenidos televisivos. En [14] se introduce el sistema de recomendación de programas de televisión queveo.tv. Este sistema utiliza un enfoque híbrido que combina las técnicas de filtrado colaborativo con las basadas en contenido. Actualmente no se puede realizar una comparación cualitativa de estos trabajos con el nuestro por dos razones. Por un lado no se dispone de la implementación de AVATAR y queveo.tv, aunque podría resultar bastante interesante realizar experimentos que pudiésemos comparar con nuestro trabajo. Por otro lado, desde el punto de vista de los experimentos, nuestros datos de partida proceden de MovieLens y no disponemos de resultados de AVATAR ni de queveo.tv con respecto a conjuntos de datos públicos que pudieran ser utilizados como referencia para la comparación.

En [15] se presenta un sistema de recomendación de contenidos multimedia que integra técnicas de anotación multimedia con técnicas de minería. Los autores desarrollan diferentes técnicas de anotación que utilizan para conceptualizar vídeos y música, y utilizan la minería para descubrir las relaciones entre los contenidos multimedia conceptualizados y los intereses de los usuarios. En nuestro trabajo las ontologías se generan mediante el filtrado basado en ontologías que no precisa de técnicas de anotación adicionales. En nuestro enfoque la minería interviene en la actualización en tiempo real de estas ontologías.

B. *Publicidad dirigida*

En [16] se presenta un sistema de recomendación de anuncios para televisión. Este sistema genera las recomendaciones en función de diferentes parámetros como el contenido de los programas televisivos/anuncios, intereses de los espectadores, preferencias de los anunciantes, horario de programación, popularidad del programa y slots disponibles para publicidad. Los autores utilizan un enfoque de agrupamiento difuso para agrupar los anuncios que resulten de interés para un conjunto de programas de televisión. En este enfoque tanto los anuncios como los programas de televisión utilizan MPEG-7 como mecanismo de anotación.

En [17] los autores proponen una arquitectura que proporciona anuncios personalizados para iDTV, internet y dispositivos móviles. En este trabajo la publicidad dirigida se consigue combinando técnicas de recomendación basadas en reglas y contenidos, a las que se añade un componente aleatorio con el fin de averiguar nuevas preferencias de los usuarios. Estas técnicas utilizan el perfil del usuario, su comportamiento y los metadatos de los anuncios.

A diferencia de los enfoques de publicidad dirigida presentados, en este trabajo el motor de recomendación utiliza el filtrado basado en ontologías. Este motor se puede ver como un motor de recomendación genérico que puede configurarse para diferentes tipos de contenidos, y uno de ellos es la publicidad.

VII. CONCLUSIONES

En este trabajo se ha presentado el motor de recomendación desarrollado para la implementación del gestor de personalización y de publicidad dentro de la plataforma de distribución de contenidos multimedia Raudos. La principal aportación de nuestro trabajo se encuentra en la arquitectura del motor de recomendación porque permite incorporar fácilmente nuevas técnicas de filtrado y adaptar el motor a diferentes tipos de contenidos. En concreto para los gestores de personalización y publicidad de Raudos se ha implementado la técnica de filtrado basado en ontologías para los siguientes tipos de contenido: contenidos audiovisuales, actividades y elementos publicitarios.

En este trabajo se ha conseguido una mejora en las recomendaciones proporcionadas por el filtrado basado en ontologías mediante una imputación de valores en la matriz de valoraciones realizadas por el usuario.

VIII. LÍNEAS FUTURAS

Uno de los parámetros que se utiliza en las recomendaciones es el perfil del usuario. En este sentido creemos que cuánto más completo sea este perfil, las recomendaciones serán de mejor calidad. El uso extendido de las redes sociales proporciona una medida idónea para completar el perfil del usuario en función de la interacción del usuario dentro de la red social. Asimismo se deberían considerar aspectos como la localización del usuario a la hora de recibir publicidad (en función de la localización del usuario y de sus gustos se le podría mostrar publicidad de restaurantes cercanos).

Aunque la técnica utilizada para generar las recomendaciones proporciona buenos resultados, en nuestra opinión éstos pueden mejorarse aún más. Actualmente nos encontramos trabajando en esta línea.

AGRADECIMIENTOS

Este trabajo ha contado con la financiación del Fondo Europeo de Desarrollo Regional (FEDER) y el Ministerio de Industria, Turismo y Comercio (MITYC) a través del Plan Avanza I+D (TSI-020302-2008-115).

En este trabajo agradecemos la colaboración durante dos años de todos los miembros del consorcio que ha trabajado en el diseño y desarrollo de Raudos: AIDO, Andago Ingeniería, EUVE, iTEAM (Universidad Politécnica de Valencia), La Salle-Universidad Ramón Llull, Solaiemes, Televisión Autonómica Valenciana, Universidad Carlos III de Madrid, Universidad de Vigo y VicomTech.

REFERENCIAS

[1] J. Herlocker, J.A. Konstan, A. Borchers and J. Riedl, *An Algorithmic FrameWork for Performing Collaborative Filtering,* In 22nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, Berkeley, CA, pp. 230-237, Aug. 1999.

[2] B. Sarwar, G. Karypis, J. Konstan, and J. Riedl, *Item-based collaborative filtering recommendation algorithms*, In 10th Conference on World Wide Web, Hong Kong, pp. 285-295, 2001.

[3] E. Vozalis and K.G. Margaritis, *Analysis of Recommender Systems' Algorithms*, In 6th Hellenic European Conference on Computer Mathematics and its Applications (HERCMA), Athens, Greece, Sept. 2003.

[4] M. O´Connor and J. Herlocker, *Clustering Items for Collaborative Filtering*, In Proceedings of the ACM SIGIR Workshop on Recommender Systems: Algorithms and Evaluation, Berkeley, CA, Aug, 1999.

[5] S-T. Park, D. Pennock, O. Madani, N. Good and D. DeCoste, *Naïve Filterbots for Robust Cold-Start Recommendations*, In Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Philadelphia, PA, USA, Aug. 2006.

[6] M.J. Pazzani and D. Billsus, *Content-Based Recommendation Systems*, Lectures Notes in Computer Science, vol. 4321, Springer, pp. 325-341, 2007.

[7] V. Schickel-Zuber, *Ontology Filtering*, Thesis, Lausanne, EPFL, October 18, 2007.

[8] *Raudos*. http://raudos.aido.es/ (visitado 23/03/2010)

[9] V. Schickel and Boi Faltings, *Using Ontological A-priori Score to Infer User's Preferences*, Proceedings of the Workshop on Recommender Systems, pp. 102-106, August 2006.

[10] O. Troyanskaya, M. Cantor, G. Sherlock, P. Brown, T. Hastie, R. Tibshirani, D. Botstein and R.B. Altman, *Missing value estimation methods for DNA microarrays*, Bioinformatics, vol. 17, no. 6, pp. 520-525, 2001.

[11] Dataset Movielens. http://www.cs.umn.edu/Research/GroupLens/data (visitado 23/03/2010)

[12] J.L. Herlocker, J.A. Konstan, L.G. Terveen and J.T. Riedl, *Evaluating Collaborative Filtering Recommender Systems,* In ACM Transactions on Information Systems, vol. 22, no. 1, pp. 5-53, Jan 2004.

[13] Y. Blanco-Fernández, J.J. Pazos-Arias, A. Gil-Solla, M. Ramos-Cabrer, M. López-Nores and B. Barragáns-Martínez, *AVATAR: A Multi-Agent TV Recommender System using MHP Applications*, In Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05), Hong Kong, pp. 660-665, March 2005.

[14] B. Barragáns Martínez, J.J. Pazos Arias, A. Fernández Vilas, J.García Duque and M. López Nores, *What's on TV Tonight? An Efficient and Effective Personalized Recommender System of TV Programs*, IEEE Transactions on Consumer Electronics, vol. 55, no. 1, pp. 286-294, Feb. 2009.

[15] V.S. Tseng, Ja-Hwung, Bo-Wen Wang, Chin-Yuan Hsiao, Jay Huang and Hsin-Ho Yeh, *Intelligent Multimedia Recommender by Integrating Annotation and Association Mining*, In 2008 IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, Taiwan, pp. 492-499, Jun 2008.

[16] S. Velusamy, L. Gopal, S. Bhatnagar and S. Varadarajan, *An efficient ad recommendation system for TV programs"*, Multimedia Systems, vol.14, Springer, pp. 73-87, 2008.

[17] T. Pessemier, T. Deryckere, K. Vanhecke and L. Martens, *Proposed Architecture and Algorithm for Personalized Advertising on iDTV and Mobile Devices*, IEEE Transactions on Consumer Electronics, vol. 54, no. 2, pp. 709-713, May 2008.

Generación de Contexto Colaborativo a partir de herramientas CSCW 2.0

Daniel Gallego Vico, Iván Martínez Toro, Joaquín Salvachúa Rodríguez
Departamento de Ingeniería de Sistemas Telemáticos,
Universidad Politécnica de Madrid
Avda. Complutense 30, Ciudad Universitaria, 28040 Madrid, España.
{dgallego, imartinez, jsalvachua }@dit.upm.es

***Resumen*- Actualmente Internet se ha convertido con toda probabilidad en el medio de colaboración más extendido en el mundo, permitiendo diferentes vías de llevarla a cabo. Este artículo propone un nuevo paradigma de diseño de aplicaciones CSCW orientadas al mundo empresarial siguiendo las nuevas ideas surgidas de la Web Social para, permitir una colaboración completa y además proporcionar un contexto colaborativo detallado a sus usuarios. Una implementación real de estos conceptos se detalla incluyendo descripciones de las herramientas ofrecidas para colaborar en espacios de trabajo, además de una explicación de cómo se realiza la generación de contexto colaborativo a partir de estructuras de datos sociales complejas. Adicionalmente presentamos resultados que validan esta nueva arquitectura para soportar la generación de contexto colaborativo usando datos sociales extraídos tanto de aplicaciones personales, como de aplicaciones empresariales, reforzando por tanto la idea de utilizar como entradas datos sociales alojados en la nube.**

***Palabras Clave*- Contexto colaborativo, Redes sociales, patrones de colaboración, CSCW, Web 2.0**

I. INTRODUCCIÓN

En los últimos años, el nombre "Web 2.0" ha sido el estandarte elegido para describir a todo un movimiento sustentado principalmente por todas las aplicaciones web sociales que han surgido en los últimos años, y que han conseguido revolucionar los cimientos y la forma de entender y usar Internet. Éste área, (con aplicaciones como Blogger, MySpace, Twitter, Facebook, Google Wave o Flickr), se ha convertido en una de las más prolíficas sobre todo porque las nuevas tecnologías son cada vez más importantes en ella, no sólo para ofrecer nuevas funcionalidades, sino para conseguir socializar la Web de una manera difícilmente imaginable hace años.

La idea principal subyacente a este tipo de aplicaciones es ofrecer un interfaz de usuario amigable, intuitivo y altamente usable, acompañado de una capacidad enorme para compartir información fácilmente entre sus usuarios. Dicho de otro modo, los usuarios pueden conectarse con el mundo entero de la manera que ellos prefieran simplemente eligiendo la o las aplicaciones sociales que mejor se adapten a su estilo de vida. Este conocimiento generado por los usuarios se comparte en Internet y es accesible en la mayoría de los casos por cualquier persona localizada en cualquier parte del globo, siendo por tanto una fuente de conocimiento inagotable.

Por otro lado, el mundo empresarial no ha asistido impertérrito a esta evolución, sino todo lo contrario, ya que ha entendido las ventajas de esta nueva forma social de colaboración que produce como hemos visto una cantidad ingente de información de todo tipo de temáticas. Es más, teniendo en cuenta que uno de los problemas principales que suele aparecer en estos entornos es la pérdida de "*know how*" cuando alguno de sus empleados deja la compañía, conocer dónde ha podido permanecer, o mejor dicho, en quién ha podido permanecer ese conocimiento, es un objetivo sumamente importante. Por tanto, sacar a la luz la actividad colectiva y el contexto colaborativo que se crea en una empresa es un tema esencial que se intenta conseguir desde hace años. Es por ello que las herramientas CSCW (*Computer Supported Cooperative Work*) han sido tan importantes para el mundo empresarial desde su aparición en la década de los 80 [1].

Estas herramientas, que solían construirse a partir de estructuras de datos rígidas muy alejadas de las que se manejan actualmente en la Web, han evolucionando de manera paralela para dar lugar a aplicaciones o plataformas de colaboración más potentes como Microsoft Office Communicator 2007 o IBM Lotus Connections, que ya poseen estructuras mucho más dinámicas. Por otro lado, también se han desarrollado trabajos recientes como el presentado en [2] para lograr el reconocimiento de relaciones sociales y lazos colaborativos en grupos de trabajo presentes en herramientas CSCW y CSCL (*Computer Supported Collaborative Learning*).

En este artículo proponemos un nuevo punto de vista de las herramientas CSCW más acorde con las ideas de la Web Social y de estas últimas aplicaciones colaborativas, con el objetivo de ofrecer los aspectos típicos de estas herramientas (colaboración entre usuarios), y en segundo lugar, la posibilidad de generar contexto colaborativo que nos muestre las uniones existentes entre los usuarios del sistema y una información más detallada de su entorno de trabajo desde un punto de vista más social. Este nuevo CSCW 2.0 que hemos desarrollado recibe el nombre de Itecsoft, y actualmente está desplegado en un gran entorno empresarial como es Indra, donde se ha estado usando en los últimos meses.

Por tanto, la estructura del artículo es la que sigue: la siguiente sección establece los requisitos principales que nos marcamos en el diseño del sistema, así como un caso de uso protagonizado por un trabajador imaginario llamado Bruce. La sección posterior describe la arquitectura e implementación del sistema que llamamos Itecsoft. La sección 4 expone las ideas principales detrás de la

generación de contexto colaborativo para, en las siguientes dos secciones, describir la manera en la que generamos contexto colaborativo a partir de las estructuras sociales de Itecsoft, así como los resultados obtenidos mediante la resolución del problema de Bruce gracias a la generación de dicho contexto colaborativo. Finalmente, en la última sección presentamos las conclusiones extraídas tras este desarrollo, así como unas pinceladas de los posibles trabajos futuros que se plantean tras la labor realizada.

II. Requisitos Funcionales y de Usuario

Antes de adentrarnos en la construcción de Itecsoft, decidimos analizar los requisitos de usuario además de revisar las funcionalidades que un sistema CSCW debería incluir. Para ello tuvimos presente en primer lugar la palabras que Reinhard et al [3] utilizaron para describir este tipo de sistemas en 1994, en las que hacían especial hincapié en que un sistema CSCW relaciona requisitos funcionales propios de un sistema colaborativo con aspectos sociales que se derivan del trabajo en grupo. Concretamente, cada una de estas funcionalidades va a tener un impacto directo en el trabajo que lleve a cabo dicho grupo, facilitando o modificando tanto el comportamiento del mismo, como mejorando en muchos aspectos la eficiencia de las tareas que practican. Asimismo, dichas funcionalidades también repercutirán en el comportamiento o la actuación individual de cada uno de los miembros del grupo de manera personalizada, por lo que habrá que cuidar que lo que para un individuo sea un funcionamiento correcto de la aplicación, también lo sea para el grupo al completo, que en muchos casos puede tener un contexto social o cultural distinto cuando se trabaja en equipos multidisciplinares, y por ello es importante conseguir que el sistema CSCW que desarrollemos sea aceptado por todos las personas que vayan a utilizarlo. Por estas razones, en nuestro diseño seguimos las diferentes propiedades que un sistema CSCW debe tener de acuerdo a la taxonomía descrita en [3], intentando conseguir de esta manera que la colaboración entre usuarios esté asegurada y que sea posible salvaguardar el conocimiento de los mismos, a la vez que se consigue un grado de aceptación de la plataforma adecuado entre sus usuarios.

A. *Interacción*

En un entorno CSCW pueden existir dos tipos de colaboración: síncrona (audio conferencia, videoconferencia, mensajería instantánea o compartición de escritorio) y asíncrona (foros o correo electrónico). Como hemos dicho antes, nuestra intención es seguir los movimientos sociales propios de la Web, por lo que ambas interacciones deberían estar disponibles para los usuarios de nuestro sistema.

B. *Coordinación*

Esta propiedad está basada en el tamaño de los grupos de usuarios y en cómo se comunican e interactúan entre ellos. Dependerá esencialmente del contexto en el que se muevan (conferencias, foros de debate, sesiones de *brainstorming*, etc.). Por lo tanto, es necesario establecer diferentes roles de usuario como administrador, revisor o invitado.

C. *Distribución*

Tener la posibilidad de trabajar y colaborar en un entorno distribuido es esencial para poder hacerlo desde cualquier parte del mundo. En consecuencia, hemos elegido la arquitectura Cliente-Servidor para que los usuarios sean capaces de conectarse al sistema desde cualquier terminal con Internet a través de un cliente web.

D. *Adaptable a diferentes tipos de usuarios*

El sistema debe ser consciente en todo momento del tipo de usuario que está conectado. Esto es, debería comportarse de una manera distinta en base al tipo de rol que posee dicho usuario, mostrando un interfaz adaptado a sus permisos.

E. *Visualización*

De acuerdo a la importancia que la experiencia de usuario ha alcanzado en la Web 2.0, nosotros nos propusimos construir un sistema que siguiese las tendencias de las RIAs (*Rich Internet Applications*) [4], donde la experiencia de usuario es muy superior a la de las aplicaciones tradicionales, hasta el punto de compararse con aplicaciones de escritorio por su alto nivel de usabilidad.

F. *Datos públicos y privados*

Todas las aplicaciones sociales (Facebook es un buen ejemplo), separan los datos públicos de los privados. Debido a esto, diseñamos la estructura de colaboración de Itecsoft en torno a espacios de trabajos o grupos de colaboración donde los usuarios con intereses similares pueden acceder y compartir datos propios que sólo serán accesibles para los miembros de ese espacio.

Adicionalmente, y llegados a este punto, nosotros decidimos agregar una nueva propiedad muy importante enfocada a resolver los problemas propuestos en la introducción.

G. *Consciencia social (awareness)*

Tener la posibilidad de generar contexto social a partir de las estructuras sociales y temporales inherentes a la aplicación, podría ayudar a los usuarios a entender las actividades y proyectos en los que colaboran, así como ser conscientes del entorno social que los rodea y de la posición que ocupan en él. Por tanto, para conseguir esto analizaremos los datos sociales que Itecsoft almacenará, generando contexto colaborativo a partir de ellos.

Finalmente, y para entender claramente a qué nos referimos con estas propiedades que acabamos de ver, vamos a proponer un caso de uso en el que comprobaremos cómo nuestra propuesta puede resolver problemas que surgen a menudo en la colaboración diaria:

"*Bruce es un diseñador software que acaba de ser trasladado a un nuevo departamento en su compañía en el que se trabaja en un proyecto relacionado con el área de cloud computing. Bruce no conoce demasiado la materia por lo que necesita hablar con sus nuevos compañeros para ponerse al día. Sin embargo, desconoce quiénes son los expertos en su nuevo grupo ya que está formado por personas de varias sedes repartidas por diferentes países. ¿Qué puede hacer?*".

A lo largo de este artículo podremos ver cómo nuestro sistema resuelve esta clase de problemas muy comunes en las grandes empresas actuales.

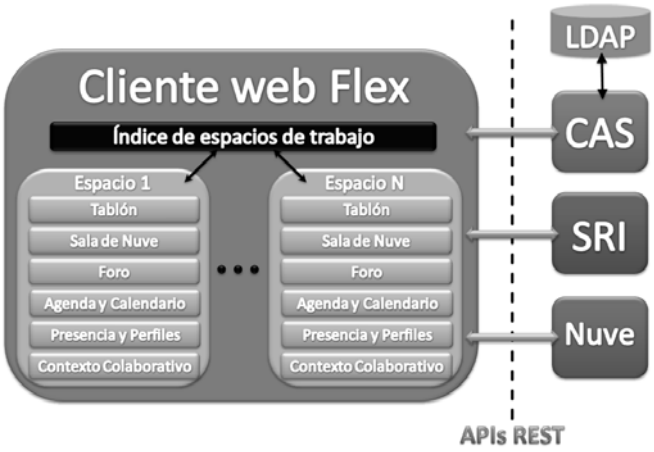


Fig. 1. Arquitectura general de Itecsoft en la que el cliente web se comunica con los módulos del lado servidor mediante APIs REST

III. La Plataforma Colaborativa Itecsoft

En esta sección describimos los detalles generales de la implementación de la plataforma colaborativo Itecsoft, diseñada para cubrir los objetivos y requisitos comentados previamente.

Como ya hemos argumentado en la sección anterior, la arquitectura elegida fue Cliente-Servidor, por lo que describiremos en primer lugar el lado servidor, hablando de manera diferenciada de cada uno de los módulos que lo conforman, para después hacerlo con el cliente explicando cómo realiza el recubrimiento de las estructuras de datos provistas por el servidor.

A. Servidor

1) SRI: Social Resource Infrastructure

Es la infraestructura responsable de proporcionar los datos sociales y las estructuras colaborativas necesarias para construir el sistema, actuando como pasarela entre la base de datos y el cliente web, por lo que es el componente más importante del lado servidor. El SRI es una aplicación web implementada en Ruby On Rails [5] siguiendo el patrón de diseño software Modelo-Vista-Controlador (MVC) [6]. Además, posee un API REST (como se puede ver en la Fig. 1) diseñado siguiendo los conceptos expuestos por Roy Fielding en su tesis [7]. De esta manera ofrecemos comunicación con el cliente web a través de llamadas HTTP con las que poder gestionar los recursos sociales almacenados en la base de datos. Los recursos REST disponibles son los siguientes, que se acompañan de la Tabla 1 que indica los métodos disponibles para todos ellos:

- *Usuarios*: todos los usuarios de la aplicación.
- *Espacios*: los espacios de trabajo que identifican a un proyecto o determinado grupo de usuarios.
- *Eventos*: usados para gestionar los eventos de la agenda y el calendario.
- *Artículos*: los mensajes y comentarios usados en la herramienta de foro.
- *Permisos*: cada usuario tendrá un fichero de permisos que especificará los diferentes roles que pueda tener en los espacios a los que pertenezca, aportando la propiedad de coordinación.

Tabla 1. Métodos disponibles en el API REST Atom del SRI

Petición HTTP	Incluye Atom	URI	Método Rails	Devuelve Atom
GET	No	/recurso.atom	Index	Si
POST	Si	/recurso.atom	Create	No
GET	No	/recurso/id.atom	Show	Si
PUT	Si	/recurso/id.atom	Update	No
DELETE	No	/recurso/id.atom	Destroy	No

Adicionalmente, debemos destacar que el formato elegido para llevar a cabo la comunicación entre el SRI y el cliente web fue Atom. Esta decisión estuvo basada en el uso generalizado que este formato ha adquirido en los últimos años en Internet. Concretamente, el SRI usa *namespaces* Atom estandarizados (algunos de ellos usados por ejemplo por Google en Blogger), lo que permite a Itecsoft conectarse con otras aplicaciones sociales sin coste alguno. Asimismo, es importante poner énfasis en el hecho de que para realizar todas las operaciones CRUD (*Create Read Update Destroy*) en Atom son necesarios dos protocolos definidos en sendas RFCs: *The Atom Syndication Format* [8] para leer los recursos, y *The Atom Publishing Protocol* [9] para crearlos, editarlos y borrarlos.

De esta forma, y teniendo en cuenta el uso que se hace de los protocolos anteriores, y de los métodos de la interfaz Atom ilustrados en la Tabla 1, podemos ver en la Fig. 2 la arquitectura general y los procesos de comunicación que se llevan a cabo internamente cuando se comunica el cliente web con el módulo SRI del lado servidor. Como se desprende de dicha figura, y ya comentamos anteriormente, el SRI actúa como un recubrimiento de la base de datos MySQL donde almacenamos la información sobre los diferentes recursos sociales que ofrecemos mediante el API REST.

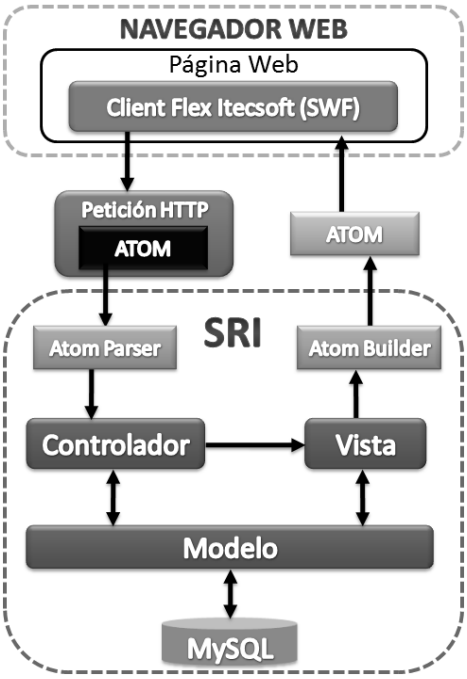


Fig. 2. Arquitectura y comunicación entre el cliente Flex y el módulo servidor SRI mediante el API REST Atom

2) Nuve: Videoconferencia como Servicio

Como podemos ver la Fig. 1, otro de los módulos pertenecientes al lado servidor es Nuve [10], que ofrece salas de videoconferencia como servicio mediante una arquitectura *cloud*. Sin embargo, este servicio no es tan simple como pueda parecer a priori, ya que permite a los usuarios acceder a un entorno colaborativo completo que incluye compartición de audio y vídeo, mensajería instantánea y compartición de escritorio.

Nuve, desarrollado por el grupo de investigación al que pertenecen los autores de este artículo, es la evolución de Marte 3.0 [11], un servicio de videoconferencia Cliente-Servidor. La arquitectura de Nuve extiende la implementación anterior para convertirlo en un servicio escalable mediante técnicas de *cloud computing*, ofreciendo de esta manera salas virtuales a los usuarios de Itecsoft. Para hacer esto, Nuve posee al igual que el SRI un API REST para permitir que el cliente web solicite y gestiones dichas salas. En otras palabras, este interfaz pretende transformar un sistema tradicional de telecomunicaciones, como es la videoconferencia, en un recurso que puede ser usado por aplicaciones de terceros.

Otro detalle a tener en cuenta es la conexión entre el SRI y Nuve, pues cuando creamos un nuevo espacio en Itecsoft, éste lleva asociado una sala de Nuve donde los usuarios del espacio son registrados. En consecuencia, tenemos una relación uno a uno entre espacios del SRI y salas de Nuve.

3) Autenticación Single Sign-On

El último módulo que nos queda por explicar es el encargado de la autenticación en Itecsoft. Dicho módulo está dividido en dos componentes. Por un lado tenemos un servidor de CAS que nos ofrece un servicio de *Single Sign-On* (SSO) válido para autenticar al cliente web en el SRI (y posibles módulos futuros). Así, el cliente se comunica con este componente a través de peticiones HTTP usando para ello el API RESTful [12] que posee esta implementación de CAS. Por otro lado, tenemos una base de datos OpenLDAP [13] que almacena las credenciales de los usuarios y sus permisos. Por lo tanto, el servidor de CAS autenticará contra la base de datos LDAP las credenciales (usuario y contraseña) enviadas desde el cliente web, generando posteriormente los tickets correspondientes para iniciar la sesión SSO de usuario.

B. Cliente

El cliente web de Itecsoft ha sido desarrollado siguiendo la filosofía de las aplicaciones RIA. Para ello se ha usado Adobe Flex como tecnología de implementación, ya que facilita el diseño de este tipo de aplicaciones con interfaces de usuario avanzados y nos permite cumplir las propiedades de adaptación de la aplicación a diferentes tipos de usuarios y visualización. Esto además tiene una ventaja añadida: los usuarios no necesitarán instalar nada en sus ordenadores debido a que la mayor parte de los navegadores tienen actualmente instalado el plug-in de Flash Player. Volviendo a la arquitectura del cliente, hay que mencionar que fue diseñada utilizando el *framework* de código abierto Cairngorm [14], ya que proporciona facilidades para diseñar las aplicaciones Flex siguiendo el patrón de diseño software MVC, lo que facilita la implementación de un cliente adecuado para una arquitectura de tipo Cliente-Servidor.

Por consiguiente, el cliente web se construye como recubrimiento de las estructuras de datos sociales existentes en el SRI y actúa como capa de presentación avanzada para permitir a los usuarios colaborar entre ellos utilizando el conjunto de herramientas que se obtienen de este recubrimiento, y que están disponibles para ellos en los diferentes espacios de trabajo en los que estén registrados (como se ilustra en la Fig. 1). En consecuencia, la unidad organizativa más importante dentro de la aplicación es el "espacio de trabajo". Un espacio de trabajo aglutina todos los contenidos relacionados con un proyecto o grupo de usuarios que colaboran en un trabajo común. Dicho de otro modo, los usuarios no pertenecen a la aplicación en sí misma, sino que pertenecen a uno o varios espacios de trabajo existentes en Itecsoft, cada uno de ellos con un fin distinto.

De esta manera, cada uno de los espacios tendrá los siguientes componentes que poseen integración horizontal entre ellos al ser gestionados de manera única por el cliente que es el encargado de permitir que actúen conjuntamente de manera simultánea y que puedan comunicarse entre ellos:

- *Tablón*: es el sitio central de un espacio en el que se informa cuál es el objetivo del mismo, además de conocer en todo momento cuáles van a ser los próximos eventos o los mensajes con más actividad del foro.
- *Sala de Nuve*: proporciona una sala de videoconferencia con mensajería instantánea y compartición de escritorio.
- *Foro*: recubriendo los "artículos" del SRI, construimos un foro donde los usuarios del espacio pueden abrir hilos de conversación para poder colaborar de manera asíncrona.
- *Agenda y Calendario*: de nuevo, usando la estructura de datos "eventos" del SRI, proporcionamos una herramienta de agenda y calendario donde poder fijar reuniones o eventos propios de la actividad del grupo de trabajo al que representa el espacio.
- *Presencia y Perfiles*: proporciona por un lado los perfiles de usuario públicos de las personas registradas en el espacio, así como un servicio de presencia que nos informa en todo momento de quién está conectado, dando la posibilidad por ejemplo de iniciar sesiones de videoconferencia o mensajería instantánea con aquellos que se encuentren disponibles.
- *Contexto colaborativo*: este componente es el encargado de generar contexto colaborativo a partir de un grupo de usuarios en un espacio, de manera que ellos puedan ser conscientes de las interacciones y lazos sociales que mantienen dentro de la aplicación, así como del conocimiento que se encuentra presente en su grupo de trabajo.

Una vez llegados a este punto, ya podemos entender correctamente la Fig. 1. Además, teniendo en cuenta que el cliente es el encargado de integrar de manera unificada todos los módulos del lado servidor y realizar la gestión conjunta de todos ellos, podemos afirmar que la orquestación entre

todos los servicios existentes se ha conseguido lograr de manera satisfactoria, cumpliendo las propiedades que nos marcamos como requisitos de diseño inicialmente en lo que a un sistema CSCW respecta.

IV. ¿Qué entendemos por Contexto Colaborativo?

Comprendidas las capacidades que ofrece y posee Itecsoft, ahora es el momento de detenernos un instante para definir qué es exactamente el contexto colaborativo del que hemos hablado ya en varias ocasiones.

Se define como la capacidad de percibir o ser consciente de eventos, relaciones o patrones que lleven al entendimiento del contexto en que se desenvuelve un individuo.

Este concepto, entendiendo su interés como la posesión de toda la información relevante acerca de un entorno concreto necesaria para operar y decidir de forma óptima ante cualquier cambio presentado, es utilizado en diferentes ámbitos. Éstos van desde los puestos de control de mecanismos críticos como aeropuertos o centrales nucleares, hasta la optimización de procesos de negocio que necesitan de colaboración entre miembros que pueden o no estar ubicados en el mismo emplazamiento.

El *awareness* soportado por herramientas software surge con el nombre de *context awareness* (término utilizado en la literatura inglesa para referirse al concepto que hemos traducido como contexto colaborativo), y está muy ligado a la ciencia computacional y a la computación ubicua, evolucionando después hacia la teoría de negocio en relación con la gestión de procesos de negocio y la gestión de grupos de trabajo y lazos sociales que existen entre sus miembros. Es en esta última acepción del término en la que nos centramos en este artículo.

De esta forma, vamos a estudiar ahora cuales son los conceptos que nos permiten su generación y que por tanto son las piezas que dan lugar al contexto colaborativo que buscamos generar. En nuestro caso, seguiremos las ideas descritas por Fisher y Dourish en 2004 [15], que desarrollamos a continuación.

A. Redes Sociales

Son probablemente la pieza fundamental de la generación de contexto colaborativo. El análisis de redes sociales ha sido estudiado ampliamente desde hace mucho tiempo especialmente en las áreas de ciencias sociales [16], aunque más recientemente en las redes y movimientos sociales que se han formado en Internet. Describen las relaciones existentes entre conjuntos de personas mediante el análisis de los aspectos sociales que comparten y los lazos personales o colaborativos que los unen. Así, usando el análisis de redes sociales podremos encontrar las estructuras sociales y grupos de trabajo que aparecen cuando existe colaboración entre personas, entendiendo de esta manera los diferentes roles que interpretan cada una según su contexto actual.

B. Estructuras Temporales

Son complementarias a las redes sociales, pues describen cómo éstas evolucionan a lo largo del tiempo. Por tanto, nos muestran los ritmos de colaboración que una persona experimenta en los diferentes grupos o proyectos en los que trabaja o colabora, permitiéndonos comprender en mayor detalle cuál es su relación con el resto de usuarios en cada momento dentro de un grupo.

Luego, como consecuencia de la unión de estos dos conceptos o áreas de estudio y por supuesto, de su análisis, vamos a poder generar el contexto colaborativo que estábamos buscando y que nos mostrará cómo se comporta un grupo de usuarios que colabora y cuáles son sus relaciones durante todo el tiempo que permanecen en contacto.

V. Generando Contexto Colaborativo en Itecsoft

Llegados a este punto, la pregunta es obvia: ¿cómo generamos contexto colaborativo en Itecsoft?

Como ya hemos visto, tenemos un conjunto muy rico en lo que a datos sociales se refiere, ya que hemos inspirado nuestras estructuras en las que se utilizan actualmente en las aplicaciones sociales propias del movimiento de la Web 2.0. Ahora bien, lo interesante es usar estos datos como entrada para nuestro sistema, de manera que podamos en primer lugar generar patrones colaborativos, para después analizarlos y obtener el contexto colaborativo deseado. Por tanto, para generar esta información vamos a plantear las diferentes opciones complementarias que se nos presentan a partir de los recursos disponibles en el SRI: usuarios, espacios, eventos y artículos.

A. Generación basada en espacios y usuarios

Un espacio de trabajo, tal y como lo hemos definido anteriormente, es en sí mismo una estructura colaborativa ya que es un lugar donde personas que trabajan en el mismo proyecto o tarea, están registradas para colaborar unas con otras. Luego, la primera cosa que un usuario descubre al ingresar en un espacio es qué personas le acompañan y por tanto están registradas como él en dicho espacio.

En consecuencia, la generación de patrones colaborativos basados en los recursos del SRI “espacios” y “usuarios” es relativamente trivial en algunos casos, pues hay una relación directa entre ellos, y como veremos en el ejemplo siguiente, más compleja cuando deseamos extraer información que no es explícita.

La Fig. 2 muestra un ejemplo de cómo realizamos dicha generación de patrones, y por tanto, de cómo logramos obtener el contexto colaborativo. Como se puede ver, se muestran cuatro espacios de trabajo que podrían pertenecer a Itecsoft, donde el usuario A pertenece a dos de ellos en los que colabora con diferentes usuarios. De acuerdo al patrón de Red Completa, podemos comprobar rápidamente con quién colabora de manera directa simplemente analizando qué usuarios comparten espacio de trabajo con él, ya que son lazos explícitos entre usuarios.

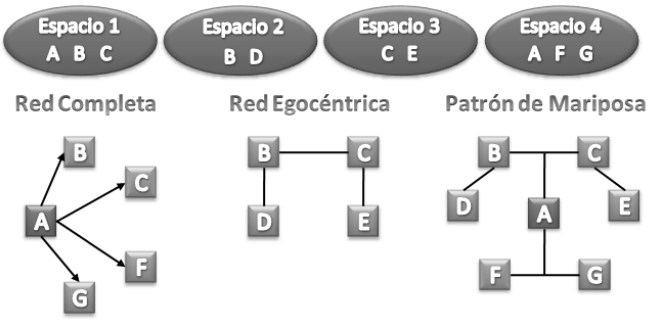


Fig. 3. Generación de patrones colaborativos a partir de espacios y usuarios

Si por el contrario nos fijamos en el patrón de Red Egocéntrica [17], obtenemos información de contexto colaborativo implícita relacionando a los usuarios anteriores entre sí. Esto lo logramos analizando los lazos que unen a aquellos usuarios con A. Así, podemos ver cómo los equipos formados por (B, D) y (C, E) que a priori son disjuntos y con los que no tiene ninguna relación directa A, están de hecho unidos por la colaboración que A mantiene con B y C en el espacio 1. Es decir, gracias a que A tiene relación con B y con C en el primer espacio, A podría relacionarse de manera indirecta con D y E a través de B y C respectivamente, lo que por ejemplo podría permitirle descubrir los campos de conocimiento de estos usuarios si llegado el caso necesitase su ayuda.

Finalmente, el patrón de Mariposa (también conocido como el de Roles Duales), nos informa de que A es el nexo de unión entre dos grupos de trabajo totalmente disjuntos, lo que nos permite identificar con este tipo de patrones los roles de A dentro de la empresa (por ejemplo, un directivo que lidera varios proyectos o que trabaja con consultores externos que podrían ser F y G), consiguiendo situarlo en su contexto colaborativo de una manera mucho más certera.

B. Generación basada en artículos y usuarios

Ahora nos centraremos en el recurso "artículos" del SRI que utilizamos para generar el foro asociado a cada uno de los espacios. Mediante el análisis de estos hilos de conversación que incluirán mensajes iniciales y comentarios realizados como respuesta, podemos extraer información social. Es más, podemos conectar a usuarios entre sí en base a la estructura padre-hijo (mensaje-comentario) que poseerá este tipo de colaboración asíncrona.

Y lo que es más importante si cabe, podemos analizar temporalmente estas estructuras de redes sociales que hemos generado con el estudio anterior utilizando las fechas que van asociadas a la dupla (usuario, mensaje), dándole por tanto un peso a esta información que puede depender del nivel de profundidad temporal que estemos dispuestos a analizar.

En la siguiente sección veremos en mayor detalle un caso de aplicación de este tipo de técnicas, así como los resultados obtenidos de la ejecución de estas herramientas de generación de contexto en Itecsoft.

C. Generación basada en eventos y usuarios

Otra manera de generar patrones de colaboración temporales y por lo tanto, obtener un contexto colaborativo más detallado, consiste en el estudio de los recursos "eventos" y "usuarios" de manera conjunta. Específicamente, si prestamos atención a los eventos que se utilizan en el componente de Agenda y Calendario que relacionan usuarios, tipos de reunión y temáticas dentro de un espacio, la información que nos brindan es tremendamente rica y obtener patrones similares a los de los casos anteriores no sería complicado.

D. Macro patrones

Por último en esta sección dónde analizamos las diferentes vías de generar contexto colaborativo en Itecsoft, podemos dar un paso más allá basándonos en el conjunto de patrones colaborativos que hemos obtenido de los recursos sociales anteriores. Esto es, tenemos la posibilidad de analizar a un nivel superior los datos sociales de los que disponemos realizando análisis conjunto de los resultados previos. Si tenemos en cuenta que normalmente los patrones colaborativos no suelen aparecer de manera aislada, y lo que es todavía más común, que suelen aparecer solapados. Por ello podemos combinarlos para obtener Macro patrones. Este nuevo tipo de patrones nos dará una información mucho más veraz y completa sobre el contexto colaborativo que rodea al grupo de usuarios que estamos analizando, en comparación con los patrones generados tras un primer análisis.

Por ejemplo, el patrón de Mariposa ilustrado por la Fig. 2 tiene implícitamente en su interior el patrón de Red Egocéntrica y el de Red Completa, por lo que se trata de un macro patrón que nos da una información más detallada sobre el usuario A y su entorno. Evidentemente, podemos realizar de manera consciente la unión de patrones para obtener información más detallada de la que cada uno por separado puede ofrecernos.

De esta manera, cuando deseemos generar contexto colaborativo, podemos analizar los datos sociales de los que disponemos a varios niveles de complejidad, dependiendo del nivel de detalle e interrelación entre usuarios que estemos buscando, y del tiempo que dispongamos para realizar dicho análisis.

VI. RESULTADOS

Llegados a este punto, es el momento de mostrar algunos de los resultados que hemos obtenido tras el desarrollo de Itecsoft. Para hacer esto vamos a resolver el problema de contexto que planteamos al comienzo de este artículo con el caso de Bruce.

Lo primero que haremos será suponer que la empresa u organización donde Bruce trabaja ha desplegado Itecsoft hace un tiempo para proporcionar una plataforma de colaboración completa que puedan utilizar todos sus trabajadores, indiferentemente desde dónde lo hagan físicamente. En ese caso, "*Bruce usa el Motor de Búsqueda de Expertos existente en la aplicación para encontrar a expertos en temas de cloud computing en su nuevo grupo de trabajo que posee un espacio llamado DIT en la aplicación*".

La Fig. 3 ilustra un patrón social de Top 5 en el que informa de los expertos en *cloud computing* en dicho espacio durante los últimos cuatro meses. Nuestro módulo de generación de contexto colaborativo internamente ha analizado la evolución temporal de los usuarios que han escrito mensajes en el foro o han organizado eventos sobre este tema. Tras eso, los ha ordenado por su importancia, teniendo en cuenta los diferentes lazos sociales que puedan existir entre ellos.

Como resultado, la herramienta destaca al experto más importante en base a su mayor número de mensajes y eventos (es decir, a su mayor aportación colaborativa al proyecto), además de indicar su evolución durante los meses analizados.

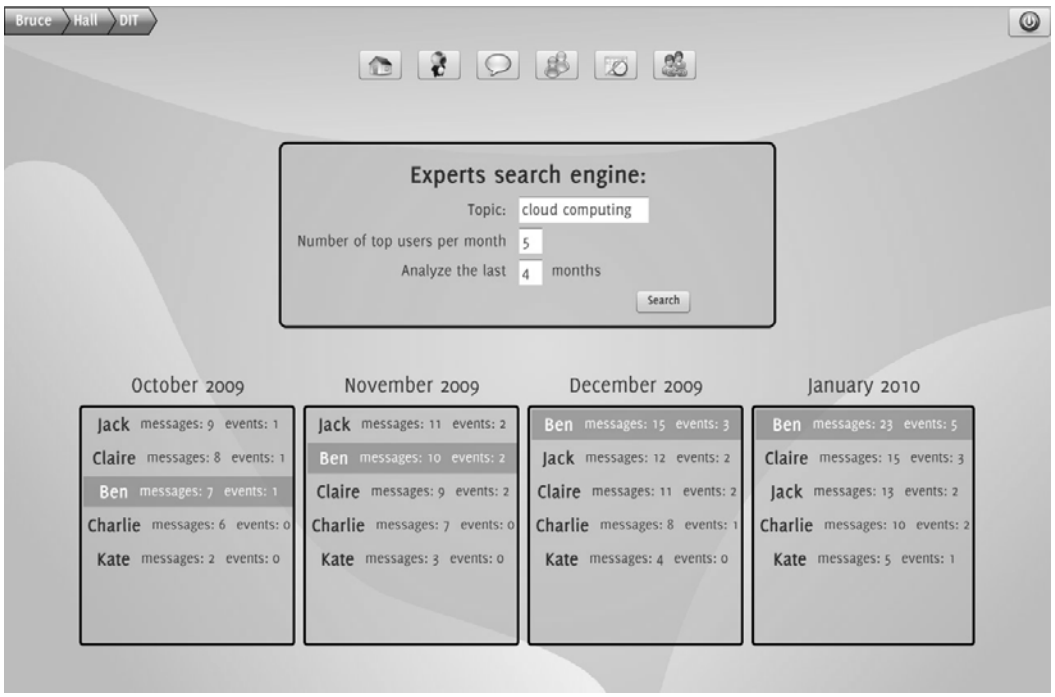


Fig. 4. Resultado de la ejecución de la herramienta de Búsqueda de Expertos de Itecsoft que hace uso del generador de contexto colaborativo

"Ahora Bruce sabe quiénes son los expertos que estaba buscando, y más concretamente, ha descubierto que Ben es el experto más destacado en este campo dentro de su nuevo departamento. Por tanto, una vez este contexto colaborativo ha sido generado para Bruce, podría hablar con Ben en tiempo real (mediante videoconferencia o mensajería instantánea), seguir las conversaciones que ha mantenido en el foro o unirse a los próximos eventos que Ben u otro experto organice en el componente de Agenda y Calendario para tratar temas relacionados con el cloud computing".

VII. Conclusiones y Trabajos Futuros

Comenzamos este artículo con el objetivo principal de generar contexto colaborativo a partir de estructuras de datos ricas en contenidos sociales, similares a las que se han venido utilizando en el mundo de Internet desde la aparición de la Web 2.0, en lugar de basarnos en una única entrada de datos simples como el correo electrónico, tal y como hacía por ejemplo la herramienta Soylent [15].

Por esa razón, decidimos construir una aplicación web completa a la que llamamos Itecsoft. Ésta seguiría las nuevas ideas de las filosofías colaborativas surgidas a partir de la Web Social, de manera que fuésemos capaces de construir un renovado tipo de plataformas colaborativas o CSCW 2.0, capaz de proveer diferentes niveles de colaboración y además, generar contexto colaborativo que permitiese a los usuarios de grandes empresas vivir una experiencia de colaboración lo más completa posible y con una experiencia de usuario renovada que siguiese el nuevo movimiento de las RIAs, donde la usabilidad es una pieza clave.

Por lo tanto, a través del presente artículo, hemos mostrado las principales funcionalidades de la arquitectura Cliente-Servidor construida, así como los módulos y herramientas colaborativas de los que dispone. Asimismo, hemos explicado las diferentes formas que tenemos de generar contexto colaborativo a partir de los datos sociales sobre los que se sustenta nuestro sistema y que son almacenados en el lado servidor.

Adicionalmente, hemos demostrado con los resultados de una ejecución de nuestra aplicación que problemas tan cotidianos como la búsqueda de conocimiento en una empresa están cubiertos por las herramientas de contexto colaborativo que hemos implementado. Además, estas herramientas son capaces de analizar datos sociales tan usuales en la web como usuarios, espacios, eventos o mensajes de foros para crear patrones sociales y temporales de colaboración que, combinados para formar macro patrones, nos pueden proporcionar un contexto colaborativo aún más detallado e interesante.

Luego, aunque Itecsoft ha sido desplegado dentro de un entorno empresarial real como es Indra, y sin duda alguna la realimentación obtenida de sus usuarios siempre será un importante parámetro y fuente de información a tener en cuenta a la hora de seguir evolucionando y probando el sistema en el futuro, no debemos dejar de mirar más allá, pues existen otras líneas de investigación muy prometedoras que hemos podido descubrir durante el transcurso de este desarrollo que son igualmente interesantes.

En primer lugar, el área de la generación de contexto colaborativo y sobre todo, el análisis de estructuras de datos sociales para obtener patrones de colaboración a partir de redes sociales y estructuras temporales son áreas que difícilmente se agotarán en el futuro. Más si cabe si tenemos en cuenta que cada día las relaciones entre usuarios en Internet son cada vez más complejas de acuerdo al alto grado de lazos sociales que se forman en los diferentes contextos en los que una persona puede colaborar socialmente hoy en día. Es por esto que estudiar nuevos métodos y algoritmos que nos permitan analizar más profundamente estos datos será siempre un vía investigadora en la que deberíamos trabajar para incluir los resultados que obtengamos en nuestro sistema, haciéndolo por tanto mucho más potente.

En segundo lugar, y basándonos en las ideas que se están proponiendo actualmente en el *Social Web Incubator Group* del W3C, y sobre todo en el interesante concepto del *Socially Aware Cloud Storage* propuesto por Tim Berners-Lee [18], se abre un campo de investigación sumamente atractivo, ya que intenta promover una reestructuración de las aplicaciones de redes sociales (Facebook, LinkedIn o Twitter) para que los datos de sus usuarios puedan ser usados por aplicaciones de terceros de manera estandarizada. Si pensamos por un momento en el modelo actual de almacenamiento de los datos de estas redes sociales, que en la mayoría de los casos actúan más como silos que como almacenes ordenados, y lo que es peor, que no permiten que dichos datos sean accedidos si no es a través de sus APIs específicas (normalmente completamente diferentes entre sí), podemos comprender rápidamente que es necesaria una forma de conseguir una arquitectura común de compartición de dichos datos, logrando que aplicaciones de terceros pueda hacer uso de ellos con una filosofía *cloud* que haga independiente su gestión mediante un API unificado.

Luego, creemos que alcanzar este tipo de arquitecturas en la Web nos permitiría en un futuro unir los datos sociales que un usuario tuviese en dichas redes sociales con los datos que estuviesen almacenados en Itecsoft, consiguiendo de esta manera una integración muy interesante que nos permitiría generar un contexto colaborativo de ese usuario mucho más complejo y detallado, pudiendo ofrecerle una información sobre su entorno social y colaborativo mucho más útil y eficiente que la que proveemos actualmente.

Finalmente, y para concluir tras la investigación llevada a cabo, podemos afirmar que la integración de los datos sociales, tanto aquellos personales como los relacionados con el entorno de trabajo de una persona, nos proporcionará con toda seguridad en el futuro una poderosa herramienta de generación de contexto colaborativo.

AGRADECIMIENTOS

Este trabajo ha sido soportado por el proyecto ITECBAN, el cual ha sido financiado por el CDTI (Centro para el Desarrollo Tecnológico e Industrial) y el Ministerio de Industria, Turismo y Comercio. Asimismo, los autores agradecen a Juan Carlos Macho, Fernando Alcántara y Gonzalo Pando de INDRA Sistemas, S.A. su valiosa contribución a este trabajo.

REFERENCIAS

[1] J. Grudin, “Computer-supported cooperative work: history and focus”. *Computer*, vol. 27, no. 5, pp. 19-26, 1994.

[2] J. J.P. Tsai, J. Zhang, J. J.S. Huang and S. J.H. Yang, “Supporting CSCW and CSCL with Intelligent Social Grouping Services”. *International Journal of Software Science and Computational Intelligence (IJSSCI)*, vol. 1, no. 1, pp. 51-63, 2009.

[3] W. Reinhard, J. Schweitzer, G. Völksen and M. Weber, 1994. “CSCW tools: concepts and architectures”. *Computer*, vol. 27, no. 5, pp. 28-36, May 1994.

[4] F. Moritz, “Rich Internet Applications (RIA): A Convergence of User Interface Paradigms of Web and Desktop - Exemplified by JavaFX”. Diploma Thesis of University of Applied Science Kaiserslautern. Zweibrücken, Germany, January 2008.

[5] D. Thomas and D. Heinemeier, *Agile Web Development with Rails*, Second Edition, USA : The Pragmatic Bookshelf, 2006.

[6] E. Curry and P. Grace, “Flexible Self-Management Using the Model-View-Controller Pattern”. *IEEE Software*, vol. 25, no. 3, pp. 84-90, May 2008.

[7] R. Fielding, “Architectural Styles and the Design of Network-based Software Architectures”. Doctoral dissertation, University of California, Irvine, USA, 2000.

[8] RFC 4287, “The Atom Syndication Format”, *The Internet Engineering Task Force (IETF)*, 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4287.txt [Accessed: April 16, 2010].

[9] RFC 5023, “The Atom Publishing Protocol”, *The Internet Engineering Task Force (IETF)*, 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5023.txt [Accessed: April 16, 2010].

[10] P. Rodriguez, D. Gallego, J. Cerviño, F. Escribano, J. Quemada and J. Salvachua, “VaaS: Videoconference as a service”, in Proceedings of the 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2009. Washington, DC. November 2009, pp. 1-11.

[11] J. Cerviño, P. Rodríguez, J. Salvachúa, G. Huecas and F. Escribano, “Marte 3.0: una videoconferencia 2.0”, in Proceedings of JITEL 2008, Madrid, Spain, September 2008, pp. 209-216.

[12] Jasig Wiki, “RESTful API CAS User Manual”, 2009. [Online]. Available: http://www.ja-sig.org/wiki/display/CASUM/RESTful+API [Accessed: April 16, 2010].

[13] OpenLDAP, “A open source implementation of the Lightweight Directory Access Protocol”, 2009. [Online]. Available: http://www.openldap.org/ [Accessed: April 16, 2010].

[14] Adobe Open Source, “Cairngorm”, 2007. [Online]. Available: http://opensource.adobe.com/wiki/display/cairngorm/Cairngorm [Accessed: April 16, 2010].

[15] D. Fisher and P. Dourish, “Social and temporal structures in everyday collaboration”, in Proceedings of the Conference on Human Factors in Computing Systems. Vienna, Austria, 2004, pp. 551-558.

[16] S. Wasserman and K. Faust, *Social network analysis: methods and applications*, Cambridge, UK : Cambridge University Press, 1994.

[17] D. Fisher, “Using Egocentric Networks to Understand Communication”, *IEEE Internet Computing*, vol. 9, no. 5, pp. 20-28, September 2005.

[18] T. Berners-Lee, “Socially Aware Cloud Storage. First draft”, 2009. [Online]. Available: http://www.w3.org/DesignIssues/CloudStorage.html [Accessed: April 16, 2010].

Selección Semántica de Servicios de Infraestructura basada en Propiedades No Funcionales

Henar Muñoz Frutos [(1)], Guillermo Vega Gorgojo [(2)], Yannis Dimitriadis [(2)]

[(1)] Capacidades e Infraestructuras Cloud Orientada a Negocio, [(2)] Grupo de Sistemas Inteligentes y Cooperativos

[(1)] Telefónica I+D, [(2)] Universidad de Valladolid

[(1)] Parque Tecnológico de Boecillo 47151 Boecillo (Valladolid), [(2)] Paseo Belén 15, 47011 Valladolid

henar@tid.es, guiveg@tel.uva.es, yannis@tel.uva.es.

***Resumen*- El modelo de *Utility-Computing* permite el suministro de recursos computacionales, como procesamiento y almacenamiento, por Internet encapsulados como servicios de infraestructura. Sin embargo, la selección de los servicios más adecuados basada en propiedades no funcionales se ve seriamente limitada por el uso de terminología propietaria por parte de los proveedores de servicios. Este artículo propone un nuevo proceso de selección de servicios de infraestructura basado en ontologías. Mediante un ejemplo práctico, se ilustra y se analiza el procedimiento propuesto e implementado, que consiste en la conversión de las descripciones de los servicios a un modelo común que es compartido entre todos los participantes, y la aplicación de reglas de conversión de propiedades y algoritmos de evaluación.**

***Palabras Clave*- Servicios de Infraestructura, Selección de servicios, propiedades no-funcionales, Ontologías.**

I. INTRODUCCIÓN

La entrega de computación está evolucionando hacia un modelo de *Utility-Computing* [1], donde recursos computacionales, como procesamiento y almacenamiento, se ofrecen como servicio, de forma similar a las utilidades públicas tradicionales (la electricidad, el teléfono…). En este modelo, los clientes acceden a un conjunto de recursos (aplicaciones, bases de datos, servicios, almacenamiento...) [2], que están encapsulados como servicios, sin necesidad de conocer su localización y el modo de provisionamiento [3]. Estos servicios se conocen como Servicios de Infraestructura (SOI) y proporcionan la utilidad de computación a usuarios finales [3]. Aunque los servicios SOI pueden implementar diversas funcionalidades (computación, almacenamiento, entorno de desarrollo, etc. [4]), su elemento diferenciador son sus propiedades no-funcionales, que caracterizan los recursos que encapsulan [3].

Debido a la aparición de nuevos proveedores de servicios de infraestructura (como *Amazon Elastic Cloud Computing* – EC2 [5], *Joyent Cloud* [6], *Google App Engine* [7]…), el mercado global de servicios SOI está ganando en importancia, en el que proveedores ofrecen recursos y los clientes los consumen pagando por su uso. En este ecosistema, los clientes pueden encontrar dificultades en la selección de los servicios de forma automática, dado que las descripciones están realizadas en texto plano, en terminología propietaria, y el número de servicios en el mercado va aumentando [8][9].

Así pues, el proceso de selección de servicios SOI se convierte en un elemento importante a la hora de decidir el mejor servicio que se ajuste a las restricciones del cliente [3][9][15]. Este proceso de selección incluye tanto la obtención de servicios candidatos que se ajusten a la funcionalidad requerida, así como sus propiedades no funcionales y las características del hardware que encapsulan (RAM, disco, etc.), que son los elementos diferenciadores en la decisión de selección [3]. Esto significa, por ejemplo, elegir el mejor servicio entre *EC2* y *Joyent Cloud*, servicios que ofrecen capacidad de computación, comparando sus propiedades no funcionales.

Sin embargo, la definición de las propiedades no funcionales suele estar especificada por un vocabulario (o terminología) propietario del proveedor del servicio utilizado [9]. Por ejemplo, una instancia de *EC2* describe términos como *Compute unit*, *RAMMemory* y *Storage* en EC2 [5], mientras que *Joyent Cloud* [6] utiliza CPU, *hard disk* y RAM. Además, los proveedores utilizan diferentes unidades de medida y formas de medir: ECU (*EC2 Compute Unit*) en *EC2* vs. 1/32 de un *AMD Opteron* en *Joyent.* La utilización de vocabularios heterogéneos complica en gran medida la selección del servicio más adecuado a las características demandadas por el cliente.

El uso de terminologías propietarias se debe especialmente a que las especificaciones de servicios no cubren la descripción de propiedades no funcionales, además de carecer de expresividad semántica por basarse en XML [11]. Algunas de estas especificaciones son *Web Service Description Language* (WSDL) para la descripción de servicios Web [12], *Web Service Resource Framework* para servicios Grid [13], o *Service Level Agreement* (SLA) [14] para la especificación de plantillas especificando las características no-funcionales que el servicio ofrece [9][15].

Una posible solución a este problema sería la utilización de una terminología para la descripción de servicios (especialmente sus propiedades no funcionales) compartida

por todas las partes y en un lenguaje procesable computacionalmente [11]. Precisamente éstas son las características de una ontología [16] que define la conceptualización de un dominio compartido por una comunidad y que es procesable por máquinas. Así, podría definirse un modelo conceptual compartido entre clientes y proveedores para proporcionar un entendimiento común de los parámetros y su semántica. De esta forma las descripciones de los servicios y las peticiones se pueden relacionar con los elementos de la ontología extendiendo el modelo conceptual.

Así pues, el objetivo de este artículo es proponer un procedimiento para la selección de servicios SOI en el que se aplican tecnologías semánticas para resolver el problema de la heterogeneidad. En el resto del artículo, se motivará el problema mediante un ejemplo en la Sección 2, para pasar a la explicación del procedimiento de selección de servicios basado en ontologías en la Sección 3, mientras que la evaluación de la propuesta mediante un ejemplo real se presenta en la Sección 4. Finalmente, la Sección 5 analizará brevemente otros trabajos relacionados y la 6 comentará las principales conclusiones obtenidas.

II. MOTIVACIÓN

Los servicios de infraestructura permiten ofrecer a los usuarios infraestructura hardware a través de servicio en un modelo de pago por uso. Técnicamente, se implementan mediante la arquitectura *Service Oriented Infrastructure* (SOI) (del inglés Infraestructura basada en Servicios) que proporciona las capacidades de computación o almacenamiento como servicios, vía un conjunto de recursos [2].

Según su funcionalidad los servicios SOI se pueden clasifican en 4 categorías: [4]: Infraestructura como servicio, *Infrastructure as a Service* (IaaS), que proporciona la capacidad de computación, Plataforma como servicio, *Platform as a Service* (PaaS), que ofrece el entorno parcial o total de desarrollo, o servicio, *Data Storage as a Service* (DaaS), donde el disco es provisto y Software como servicio, *Software as a Service* (SaaS). Actualmente existen muchos servicios en el mercado que ofrecen estas funcionalidades: *Amazon Elastic Compute Cloud* (EC2) [5], *Joyent Cloud* [6], *AppNexus* [17], *Windows Azure* [18] son de tipo IaaS, *Amazon Simple Storage Service* (S3) [19] se puede considerar como DaaS y *Google App Engine* [7] es el principal ejemplo de PaaS.

En este mercado, en el que nuevos participantes van surgiendo para proporciona sus infraestructuras o recursos hardware como servicio, un factor diferencial es la mejora de los mecanismos de selección de servicios SOI. Un objetivo a conseguir consiste en la automatización del proceso de selección y la disminución de la intervención humana en el mismo. De forma que se simplifica la tarea de selección para el usuario final, haciéndola más efectiva. Este proceso de selección dependerá mucho de las especificaciones utilizadas en la definición de los servicios, principalmente de sus propiedades no-funcionales, que son las que principalmente los caracterizan [3]. No obstante, como se comentó anteriormente, estas descripciones utilizan terminología propietaria de los proveedores, creando un problema de heterogeneidad en la descripción de los servicios. El siguiente ejemplo trata de ilustrar el problema.

A. Escenario Propuesto

El escenario elegido para analizar el problema de heterogeneidad en la definición de las descripciones SOI se ha tomado del escenario de ingeniería del proyecto BREIN [20]. En él, una empresa de ingeniería intenta externalizar la infraestructura de computación de las simulaciones de software para reducir costes. La Figura 1 muestra los parámetros y métricas que el cliente puede pedir (CPU, espacio en disco, memoria RAM…) y los diferentes proveedores de infraestructura (*Amazon*, *Joyent* y *Microsoft)* puede proporcionar en sus diferentes servicios *EC2*, *Joyent accelerator* y *Azure* respectivamente).

Se puede ver que los parámetros entre el cliente y los diferentes proveedores están relacionados pero no están expresados de la misma manera, lo que da lugar a un problema de heterogeneidad en forma de:

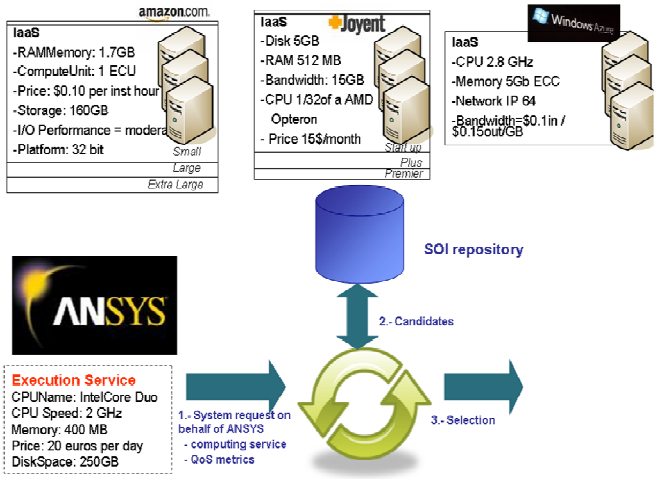


Fig. 1. Escenario de ejemplo

- *Diferentes terminologías*: la forma en que las métricas y los parámetros están expresados (DiskSpace vs. Storage vs. Disk o RAM Memory vs. Memory vs. RAM). Además se puede añadir el problema de diferentes lenguajes no considerados en el ejemplo.
- *Diferentes unidades de medidas:* dólares vs. euros, precio por día vs. precio por hora.
- *Diferentes formas de expresar el valor de las métricas*: GHz vs. ECU (*Elastic Computing Unit*) vs. 1/32 of a AMD Opteron. Una unidad EC2 Computing Unit (ECU) proporciona la equivalencia de capacidad CPU de 1.0 a 1.2 GHz 2007 Opteron o el procesador Xeon 2007 [5].

Además, cada proveedor puede ofrecer diferentes instancias, es decir, diferentes valores para las propiedades del mismo servicio. Por ejemplo, *Amazon* proporciona diferentes las instancias *Small*, *Large* o *Extra Large*, como muestra la Figura 1, para el servicio *EC2* [5], especificando propiedades como *RAMMemory*, *ComputeUnit*, *Storage*, *Platform*, *Price*… Estas instancias comparten la terminología pero no los valores de las propiedades. Por su parte, *Joyent* ofrece las instancias *Startup*, *Plus* y *Premier* [6], con la terminología *Disk*, *RAM*, *Bandwidth*, *CPU*, *Price*. En este

sentido, considerado las diferentes instancias del mismo proveedor y la existencia de múltiples proveedores y clientes, que pertenecen a diferentes empresas usando diferentes terminologías y vocabularios, el problema de heterogeneidad puede dificultar el proceso de selección.

III. PROCEDIMIENTO DE SELECCIÓN DE SERVICIOS

En esta sección se describe el procedimiento propuesto para la selección de servicios SOI basado en el uso de ontologías, mientras que la siguiente sección proporciona un ejemplo real de validación de la propuesta.

A. *Utilización de ontologías para la selección*

La mayor parte de especificaciones en la descripción de servicios, tales como WSDL o WSRF o de descripciones de propiedades no-funcionales como se puede considerar a las plantillas de SLA [9][15], están basados en XML. Este lenguaje carece de la expresividad semántica suficiente en la definición [11], dado que sólo es un formato y no proporciona una definición de la información involucrada. El uso de estos lenguajes limita la habilidad de selección de descripciones de servicios a partir de peticiones a un emparejamiento sintáctico. El carácter sintáctico de este emparejamiento implica que los términos utilizados deben ser exactamente los mismos y que no se tengan en cuenta sinónimos o conceptos relacionados. No obstante, según se comentó en la Figura 1, cada proveedor está utilizando terminologías propietarias y diferentes, dentro de especificaciones basadas en XML, lo que a priori no es una solución factible para el proceso de selección y requiere de alguna solución complementaria.

Las ontologías pueden resolver la heterogeneidad dado que permiten que el significado de los datos sea expresado en un lenguaje entendible por las maquinas [16]. De esta forma, se pueden extender las descripciones XML usando ontologías y formalizándoles en un lenguaje más expresivo como *Web Ontology Language* (OWL) [21] o *Web Service Modelling Language* (WSML) [22]. En realidad, el uso de este tipo de lenguajes permite la existencia de un modelo conceptual conteniendo información de los servicios, tanto propiedades funcionales como no funcionales, que es compartido por clientes y proveedores, formalizado en una ontología para proporcionar un modelo común de los parámetros y su semántica. De esta forma existe un acuerdo previo mutuo de las propiedades para desarrollar el método para el emparejamiento semántico, y así mejorar la interoperabilidad en la definición de las propiedades.

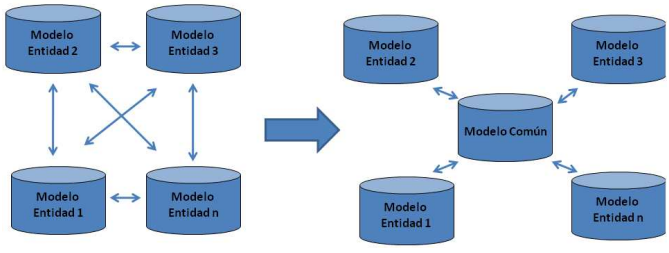


Fig. 2. Reduciendo el número de mapeos con un modelo común compartido.

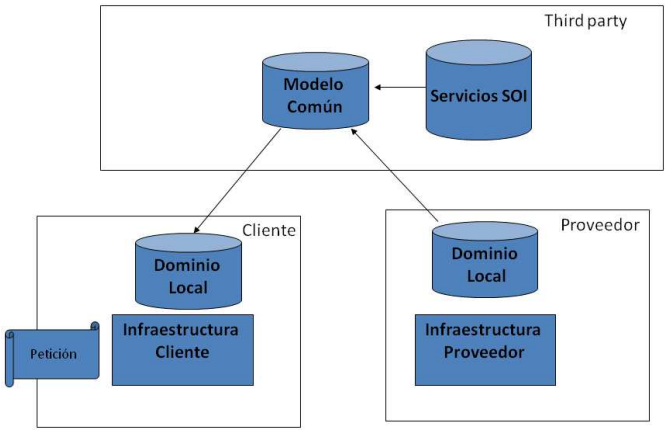


Fig. 3. Propuesta de uso de una ontología como medio de compartición de un modelo conceptual común

En el ejemplo que estamos considerando, para simplificar los mecanismos de traducción entre los proveedores y clientes, se puede plantear el uso de una ontología común centralizada que cada entidad involucrada extenderá con sus requisitos concretos. De esta forma estamos hablando de una propuesta que necesita $n+m$ mapeos donde n es el número de clientes y m de proveedores, ya que el participante mapea su terminología a una común. Así pues con el modelo común se evita la necesidad de $n*m$ mapeos, si se necesitara enlazar todas las terminologías de todos los participantes. Esta situación se muestra en la Figura 2. Así, cada vez que surja una nueva entidad en el mercado, ésta no tiene más que mapear su terminología al dominio común. De la misma forma, cualquier cambio en el dominio local puede requerir algún cambio en el mapeo con el dominio común.

Todas las entidades comparten un modelo conceptual común formalizado por la ontología como muestra la Figura 3. Cada una de las entidades puede extender la ontología común para incorporar requisitos locales en el repositorio local. Proveedores publican todas las descripciones de los servicios en un repositorio común, que son convertidos a parte del modelo conceptual. Además se proporcionan los mapeos entre cada modelo y el modelo conceptual, de forma que todas las descripciones de los servicios son volcados en la ontología. Finalmente el cliente, el cual también tiene sus mapeos y sus reglas de conversión en el modelo local, se descarga el modelo común y compartido junto al conjunto de reglas de otros proveedores o entidades involucradas. La infraestructura del propio cliente será el lugar encargado de ejecutar el procedimiento de selección de servicios SOI basado en ontologías que se comenta a continuación.

B. *Proceso de Selección de Servicios SOI*

El procedimiento de selección de servicios SOI implica una serie de etapas que se ilustran en la Figura 4. Conlleva desde la conversión de las descripciones de los servicios y de las peticiones de los clientes, a la obtención de una valoración del servicio según los requisitos del cliente. Para que se pueda llevar a cabo, requiere que todos los proveedores y clientes especifiquen sus mapeos, es decir, la relación de su terminología con la del modelo común, formalizado a través de reglas que se aplican al mismo modelo.

Así pues, el proceso de selección de servicios SOI consiste en:

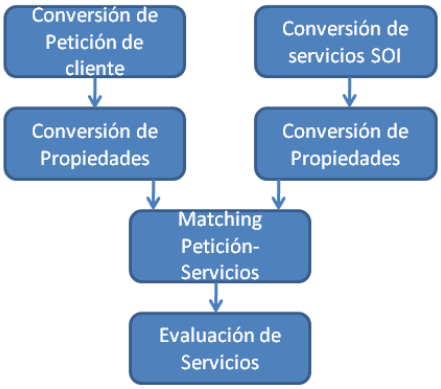


Fig. 4. Procedimiento de Selección de Servicios SOI

- **Convertir las peticiones de los clientes al modelo conceptual.** Cuando se recibe la petición del cliente, ésta petición debe ser convertida al modelo conceptual. Así pues, la petición se transforma a instancias OWL del modelo conceptual, es decir de la ontología común en el repositorio local de conocimiento.
  Como el cliente, a priori, ya ha especificado sus mapeos con el modelo común formalizado como un conjunto de reglas, la petición del cliente finalmente se almacena en el modelo local en la terminología común.
- **Convertir las descripciones de los servicios SOI al modelo conceptual**: Las diferentes descripciones de los servicios candidatos (por ejemplo, las diversas instancias de *Amazon*, o de *Joyent*…) son convertidas a instancias OWL del modelo conceptual y almacenadas en el modelo común. Dado que anteriormente, los proveedores han especificado sus mapeos con el modelo común como una serie de reglas, los servicios SOI son almacenados en el modelo común en la terminología común.
- **Conversión de propiedades**: Las propiedades no funcionales, unidades de media y los valores se traducen al modelo común conceptual aplicando las reglas establecidas en los mapeos de las entidades al modelo común. Estas reglas se almacenan en el repositorio local. Un ejemplo dado es la conversión son las reglas para pasar de ECU (*Amazon CPU unit*) [4] a GHz. Esto implica el cambio de unidades y modificación de su valor. De esta forma, gracias al modelo conceptual común y las reglas aplicadas, todos los términos de cliente y proveedores se expresan de la misma forma, así pues es posible hacer búsquedas, *rankings* y selección de las ofertas de los proveedores con respecto a las peticiones del cliente.
- **Emparejamiento de petición-servicios**: Todos los servicios disponibles necesitan estar relacionados a la petición en este paso. Así a partir de la petición del cliente, una búsqueda SPARQL [23] se crea para obtener los servicios que satisfacen las descripciones.
- **Evaluación de Servicios**: La evaluación se usa para asignar un valor número a cada servicio, normalizado, que representa la satisfacción a los requisitos del cliente. Así pues los servicios son asociados a un valor, que permite su ordenación, creación de *rankings* para su posterior selección. Para la evaluación del servicio, nos hemos basado en el algoritmo de selección de Wang et al [24]. En este algoritmo, el valor de la métrica *j* del servicio *i* se calcula teniendo en cuenta los valores máximos y mínimos de los servicios candidatos para la métrica *j*, y teniendo cuenta lo requerido por el cliente. En este caso se distingue una función cuando la condición a conseguir sea maximizar el valor pedido (1) y otra para minimizarlo (2).

$$q'_{ij} = 1 - \frac{q_{\max} - q_{ij}}{q_{\max} - q_{\min}} \quad (1)$$

$$q'_{ij} = \frac{q_{ij} - q_{\min}}{q_{\max} - q_{\min}} \quad (2)$$

El valor final del servicio se calcula como una suma ponderada considerando todas las métricas involucradas.

IV. CASO PRÁCTICO

El escenario elegido para demonstrar la aplicabilidad del proceso de selección, es el ejemplo mostrado en la Figura 1. En el que hay tres proveedores (*Amazon*, *Joyent* y *Windows*) que está ofreciendo servicios IaaS con diferentes instancias utilizando recursos diferentes. Además, *Amazon* y *Joyent* tienen diferentes instancias (conjunto de propiedades de servicios) que pueden ser ofrecidos. Por ejemplos para el caso de *Amazon* se ofrece *Small*, *Large* y *Extra Large*.

Así pues el cliente es ayudado por el proceso de selección para que se le proporcione el proveedor que mejor servicio le puede dar según sus requisitos. La situación actual involucra que el cliente tuviera que mirar en las diferentes páginas web de los proveedores, hiciera las traducciones de unidades y medidas a mano y evaluara los diferentes ofertas para encontrar las mejores.

A. *Artefactos necesarios*

La Figura 3 mostraba la arquitectura a alto nivel para aplicar este procedimiento así como los artefactos necesarios para su uso. Existe una ontología común que se encuentra en una entidad externa, extensiones de este modelo conceptual en cada entidad involucrada (cliente o proveedor).

La ***ontología común*** formaliza el modelo conceptual común compartido entre cliente y proveedores, la cual es extendida según los requisitos de las entidades involucradas. Como ontología común se utiliza la ontología de QoS y de negocio para la descripción de los servicios de BREIN, que cubre las propiedades no funcionalidades con un foco especial al dominio SOI. Parte del extracto de la ontología que se muestra a continuación, utilizando la nomenclatura N3, contiene conceptos como *RAMMemory*, *CPUSpeed*, *euro*, *EC2ComputeUnit*, conceptos que extienden el modelo común para añadir los requisitos de *Amazon EC2*.

```
qos:RAMMemory a owl:Class; rdfs:subClassOf
qos:InfraestructureQoS.
qos:euro a owl:Class; rdfs:subClassOf
qos:MonetaryUnit.
qos:StorageUnits a owl:Class; rdfs:subClassOf
qos:MeassurementUnits.
qos:CPUSpeed a owl:Class; rdfs:subClassOf
qos:InfraestructureQoS.
qos:EC2 ComputeUnit a owl:Class ; rdfs:subClassOf
qos:FrequenceUnit.
```

Por otro lado, para la ***especificación*** de las propiedades no funcionales de los servicios SOI, en este ejemplo, utilizamos las plantillas SLA como se muestra en el trabajo

[15]. Un ejemplo de un extracto de esta plantilla para el servicio EC2, se muestra a continuación.

```
<wsla:SLAParameter name=CPUSpeed type=double
unit=ECU>
  <wsla:Metric>defaultECU</wsla:Metric>
    </wsla:SLAParameter>
  <wsla:Metric name=ComputeUnit type=double
unit=ECU>
    <MeasurementDirective xsi:type=ECU
resultType=double>
  </wsla:Metric>
<wsla:Predicate xsi:type=wsla:Equal>
<wsla:SLAParameter>ComputeUnit</wsla:SLAParameter>
<wsla:Value>1</wsla:Value>
</wsla:Predicate>
```

Finalmente, el repositorio local refina localmente el modelo conceptual común, que es compartido por clientes y proveedores, para especificar los requisitos de empresas. Para formalizar el modelo local, el proveedor crea una serie de reglas, utilizando conceptos de la ontología común que mapean diferentes términos, unidades de medida y valores. Por ejemplo, para *Amazon EC2* se necesita proveer reglas para convertir las métricas y unidades (*Compute Unit*, *ECU*, *dollars*, etc.) en el vocabulario común. Las líneas siguientes muestran la conversión de euros a dólares en los parámetros de QoS utilizados.

```
qos:QoSParameter(?p) ? qos:hasMeasuredUnit(?p,
dollars) ?
qos:parameterValue(?p, ?v1) ? swrlb:divide(?v2,
?v1, 1.39) ?
hasLocalMUnit(?p, euros) ? hasLocalValue(?p, ?v2)
and next ones the translation from ECU unit to GHz
qos:CPUSpeed(?param) ? qos:hasMeasuredUnit(?param,
ECU) ?
qos:parameterValue(?param, ?v1) ?
swrlb:divide(?v2,?v1,0.83) ?
hasLocalMUnit(?param, GHz) ? hasLocalValue(?param,
?v2)
```

Para el proceso de conversión, cada parámetro y métrica se define por propiedades relacionadas al proveedor y el modelo local. Así pues, propiedades como *hasMeasuredUnit* y *parameterValue* se usan para especificar las unidades originales (dólares en el ejemplo) y *hasLocalMUnit* y *hasLocalValue* para los valores y unidades traducidos (por ejemplo euros).

B. *Convertir servicios en instancias*

Los servicios SOI candidatos deben convertirse a instancias OWL y almacenarse en el repositorio local. Así pues las descripciones de servicio son interpretadas y convertidas a instancias en representación OWL. La Figura 5 muestra este proceso, donde los elementos de la descripción del servicio de la instancia *Small EC2* son extraídos por el parseador, como el nombre del parámetro (*ComputeUnit*), unidad (EC2) y valor y enlazados al modelo conceptual.

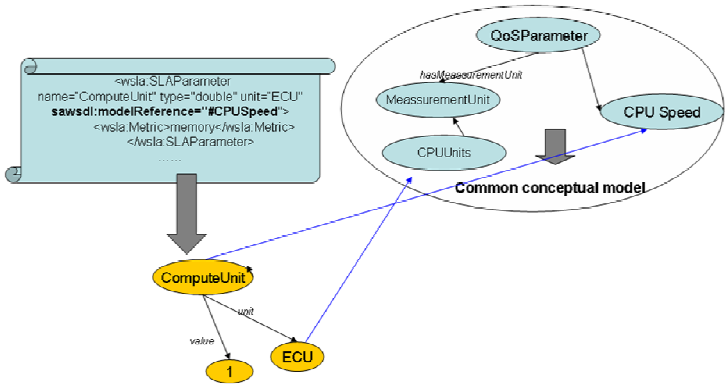


Fig. 5. Conversión de descripción de servicio a instancia.

El resultado del servicio convertido puede verse en las siguientes líneas:

```
local:SmallInstanceAmazonService a
qos:QualityModel;
qos:hasQualityFactor local:RAMMemory,
local:ComputeUnit, local:Storage,
local:Price; qos:namemodel
SmallInstanceAmazonService.
local:ComputeUnit a qos:CPUSpeed; qos:hasOperation
qos:equal;
qos:hasMeasuredUnit local:ECU; qos:parameterName
ComputeUnit;
qos:parameterValue 1.0 .

local:ECU a qos:CPUUnit
local:Price a qos:Cost ; qos:hasMeasuredUnit
local:dollars;
qos:hasMetric local:localpricemodel;
qos:hasOperation qos:greaterequal;
qos:parameterName Price ; qos:parameterValue 2.4 .
```

C. *Conversión de propiedades*

Las propiedades del servicio se traducen en el dominio común mediante la aplicación de reglas. Así pues unidades, y valores son traducidos, como se ve en la Figura 6, utilizando las reglas de conversión que se mostraban anteriormente.

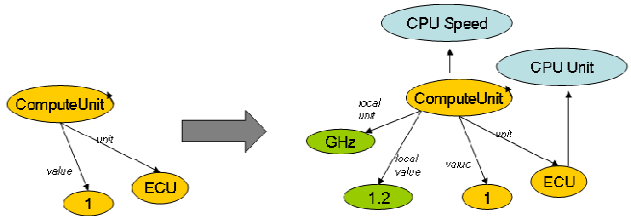


Fig. 6. Conversión de Propiedades

ECU y el valor en la instancia original se traducen en GHz y su valor correspondiente, utilizando la misma terminología. Como se observa, cada parámetro y métrica se define por propiedades relacionadas al proveedor y el modelo local. Así pues, propiedades como *hasMeasuredUnit* y *parameterValue* se usan para especificar las unidades y valores originales (ECU y 1 en el ejemplo) y *hasLocalMUnit* y *hasLocalValue* para los valores y unidades traducidos (GHz y 1,2 respectivamente).

```
local:ComputeUnit a qos:CPUSpeed ;
qos:hasMeasuredUnit local:ECU; qos:hasOperation
qos:greaterequal;
qos:parameterName ComputeUnit ; qos:parameterValue
1.0 .
```

```
local:hasLocalValue 1.2048193 ; local:hasLocalMUnit
local:GHz .

local:Price a qos:Cost ; qos:hasMeasuredUnit
local:dollars;

qos:hasMetric local:localpricemodel ;

qos:hasOperation qos:greaterequal ;

qos:parameterName Price ; qos:parameterValue 2.4 .

local:hasLocalValue 1.7266188 ; local:hasLocalMUnit
local:euros.
```

D. Emparejamiento de petición-servicio

Los servicios disponibles necesitan estar relacionados a la petición en este paso. Para ello, a partir de la petición de cliente, se crear una *query* SPARQL para obtener los servicios que satisfacen la descripción. De la petición del cliente, se crea una búsqueda para acceder al domino local, con la instancias correspondientes a los servicio incorporando los parámetros de la petición. Un ejemplo de SPARQL para el ejemplo se muestra en:

```
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-
schema#>

PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-
syntax-ns#>

PREFIX qos:
<http://brein.dsd.sztaki.hu/onto/core/business/qos.
owl#>

PREFIX local:
<http://brein.dsd.sztaki.hu/onto/core/business/loca
l.owl#>

SELECT ?soiservices

WHERE { ?soiservices qos:hasQualityFactor ?param.

?param rdf:type qos:CPUSpeed.

?param rdf:type qos:RAMMemory.

?param rdf:type qos:StorageCapacity.

?param rdf:type qos:Cost;}
```

Como resultado de la *query*, se obtienen todas las instancias de los servicios de *Amazon y Joyent*, mientras que el servicio *Windows Azure* no es considerado dado que no tiene en cuenta todos los parámetros especificados en la petición del cliente.

E. Evaluación de Servicios

La evaluación se usa para asignar un valor numérico y normalizado a cada servicio, que representa la satisfacción a los requisitos del cliente. De esta forma, los servicios tienen asociados un valor que permite su ordenación posterior y selección. Como algoritmo de evaluación, se ha escogido el algoritmo propuesto por Wang et al [24] donde se normaliza la matriz constituida por las métricas QoS para mapear todas las variables a un rango común [0, 1] escalando los rangos de los valores entre los máximo y mínimos de los valores de cada métrica. Finalmente, se obtiene el valor del servicio, sumando los valores de cada métrica y dividiendo por el número de métricas. Así de esta forma, el algoritmo proporciona una valoración del servicio entre 0 y 1, donde 1 satisface perfectamente los requisitos de los clientes y 0 es el menor valor.

Una vez que las instancias de los servicios SOI son obtenidas del dominio local, se consiguen los valores locales (almacenados con la propiedad *hasLocalValue)* para aplicar el algoritmo de selección. La Tabla 1 presenta la valoración final de cada uno de los servicios SOI involucrados en el escenario propuesto. Esta valoración consistirá en un número normalizado entre 0 y 1 y que corresponde al algoritmo propuesto en [24].

EC2 Small	**EC2 Large**	**EC2 Extra Large**	**Windows Azure**
0.38	0.98	0.75	0
Joyent Startup	**Joyent Plus**	**Joyent Premier**	
0.5	0.75	0.5	

Tabla 1. Valoración de los servicios SOI del ejemplo según los requisitos del cliente según el algoritmo de [24]

Como resultado, el mejor servicio de infraestructura según los requisitos del cliente es la instancia de *Amazon EC2 Large*, que satisface tres de las 4 restricciones de las métricas (*CPU speed*, *memory and storage capacity*) y está cerca de la condición de precio: 27 euros/día vs. 28.8 euros/día (0.4 dólares/hora e instancia). De esta forma será el servicio que será devuelto al usuario para realizar su invocación.

V. TRABAJOS RELACIONADOS

Uno de los principales problemas de los Servicios Web se refiere a la heterogeneidad de datos para garantizar interoperabilidad entre servicios [26], como ya analizamos en la Sección II. Los Servicios Web Semánticos (SWS) tratan de resolver este problema con la descripción del servicio mediante ontologías. Utilizando anotaciones semánticas en las funcionalidades e interfaces de los Servicios Web, se pueden automatizar tareas de descubrimiento, composición, ejecución etc. [11].

Así pues, algunos trabajos que introducen tecnologías semánticas en la descripción del servicio son:

- *Web Service Execution Environment* (**WSMX**) proporciona un entorno para descubrir e invocar Servicios Web según las peticiones del cliente. Presenta un entorno conceptual y un lenguaje formal para la representación de los servicios y sus características, mediante la ontología *Web Services Modeling Ontology* (WSMO) [27]. Incorpora un proceso para seleccionar al mejor candidato según una serie de preferencias definidas por parte del usuario.
- **IRS-III** (*Internet Reasoning Service*) [28], es un marco para crear y ejecutar Servicios Web Semánticos, que incorpora la ontología WSMO y la creación de conocimiento estructurado según UPML *(Unified Problem-solving Method Development Language*). Tanto WSMX como IRS-III presentan modelos conceptuales formalizados como ontologías para extender las descripciones de los servicios. Sin embargo, esta solución incrementa la complejidad para el usuario en la anotación de los servicios y el marco que implementa la solución.
- Por otro lado, el trabajo **WSMO-Lite** [30] proporciona una solución ligera para la anotación de los servicios introduciendo anotaciones semánticas dentro de la propia

descripción del servicios mediante *Semantic Annotations for WSDL and XML Schema* (SAWSDL) [29]. SAWSDL, que es una recomendación de W3C, define una extensión a WSDL y el XML *Schema* de forma que se puede enlazar elementos del documento con conceptos de la ontología. WSMO-Lite evita la complejidad de la definición de la ontología, mediante la anotación directa de los elementos necesarios. No obstante, este trabajo está limitado ya que se basa en las propiedades funcionales y no considera las propiedades no funcionales, principal objetivo de nuestro trabajo.

VI. CONCLUSIONES

Los servicios de infraestructura están principalmente caracterizados por sus propiedades no funcionales, que típicamente se especifican por cada proveedor en terminología propietaria. En un mercado donde va aumentando el número de entidades involucradas, el problema de heterogeneidad puede ser importante en la selección de servicios. Dado que las ontologías permiten mejorar la interoperabilidad entre proveedores y clientes, y la existencia de un modelo conceptual común reduce el número de mapeos existente, se propone una selección de servicios basados en ontologías. De hecho tanto el modelo conceptual como los mapeos se codifican con lenguajes formales. Además se propone un procedimiento de selección de servicios constituido por conversión a instancia, conversión de propiedades, emparejamiento de servicios y evaluación de servicios. Con este procedimiento, somos capaces de obtener aquellos servicios que se ajusten a las peticiones del cliente y obtener un valor que indica la cercanía a la petición.

Todo el proceso ha sido mostrado y evaluado a través de un ejemplo ilustrativo basado en ejemplos reales de servicios SOI existente en el mercado. A través de ese ejemplo práctico, se ha comprobado que especificaciones existentes de servicios o descripciones no funcionales de servicios webs, pueden ser convertidos a instancias de la ontología del modelo conceptual. Además, gracias a los mappings creados por los proveedores anteriormente al proceso de selección, todas las propiedades, unidades y valores son convertidos a los términos del modelo conceptual eliminando el problema de heterogeneidad. Además, el uso de *queries* permite la obtención de servicios candidatos del modelo conceptual y el algoritmo de evaluación una valoración objetivo de los diferentes servicios a partir de los requisitos del cliente.

Un aspecto importante a analizar y definir a partir de este trabajo, es la identificación de la especificación más adecuada a los servicios SOI teniendo en cuenta que un aspecto importante son las propiedades no funcionales. Además, es necesario desarrollar los mecanismos necesarios para la conversión de esta especificación a instancias de la ontología. La propia ontología, desarrollada en el marco del proyecto BREIN, deberá ser analizada y validada de forma extensa para los servicios SOI a través de ejemplos. Además, más experimentación será requerida para evaluar el algoritmo de selección o extenderlo en caso de ser requerido.

AGRADECIMIENTOS

Este trabajo ha sido realizado parcialmente en el proyecto BREIN (http://www.gridsforbusiness.eu) bajo el 6º Programa Marco. Los autores quieres agradecer a los integrantes del consorcio de BREIN y NUBA por las ideas aportadas, a Luis Miguel Vaquero de Telefónica I+D y a los miembros del grupo GSIC/EMIC de la Universidad de Valladolid por sus valiosas aportaciones y discusiones en el tema.

REFERENCIAS

[1] J.P. Degabriele, and D. Pym 2007. Economic aspects of a utility computing service. In Proceedings of the First international Conference on Networks for Grid Applications, pp. 1-7, Lyon, France, 2007.

[2] E. Castro-Leon, M. Chang, J. Hahn-Steichen, J. H. Heobbs, G. Yohanan, Service orchestration of intel-based platforms under a service-oriented infrastructure, 2006. http://www.intel.com/technology/itj/2006/v10i4/2- service/1-abstract.htm.

[3] R. Buyya, C. Shin Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6):599–616, 2009.

[4] C. Howe. Considering cloud computing for the anywhere enterprise, Yankee Group, July 2008.

[5] Amazon Web Services. Amazon elastic compute cloud (amazon ec2), 2009. http://aws.amazon.com/ec2/.

[6] Joyent. Joyent: Web hosting: Product overview, 2009. http://www.joyent.com/connector/web-hosting/

[7] Google. Google Apps, 2009. http://www.google.com/a/help/intl/es/index.html

[8] D Hamilton. Cloud computing' seen as next wave for technology investors. Financial Post, 4, 2008.

[9] H. Muñoz Frutos, A Proposal of a SOI Broker based on Semantic SLA descriptions, Trabajo de Investigación Tutelado, Universidad de Valladolid, 2009

[10] L. Youseff, M. Butrico and Da Silva, D. Toward a Unified Ontology of Cloud Computing. In Proceedings of the Grid Computing Environments Workshop (GCE '08), pp. 1-10, Austin, Texas, USA, 2008.

[11] D. Fensel, H. Lausen, A. Polleres, J. de Bruijn, M. Stollberg, D. Roman, and J. Domingue. Enabling Semantic Web Services: The Web Service Modeling Ontology. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[12] M. P. Papazoglou, P. Traverso, Schahram Dustdar, and Frank Leymann. Service-oriented computing: State of the art and research challenges. Computer, 40(11):38–45, 2007.

[13] S. Tuecke, K. Czajkowski, I. Foster, J. Frey, and S. Graham. Open grid services infrastructure (OGSI), 2003, http://www.globus.org/toolkit/draft-ggf-ogsi-gridservice-33_2003-06-27.pdf

[14] Grid Resource Allocation Agreement Protocol WG (GRAAP-WG). Web Services Agreement Specification (WS-Agreement), Proposed Recommendation, 2007. http://www.ogf.org/documents/GFD.107.pdf.

[15] H. Muñoz Frutos, I. Kotsiopoulos, L.M. Vaquero González, and L. Rodero Merino. Enhancing Service Selection by Semantic QoS. In Proceedings of the 6th European Semantic Web Conference on the Semantic Web: Research and Applications, Heraklion, Crete, Greece, 2009.

[16] T. R. Gruber. Toward principles for the design of ontologies used for knowledge sharing. International Journal of Human-Computer Studies, 43(5-6):907–928,1993.

[17] Appnexus. The AppNexus Cloud, 2009. http://www.appnexus.com/products/overview.php.

[18] Microsoft. Windows Azure Platform, 2009. http://www.microsoft.com/azure/default.mspx.

[19] Amazon Web Services. Amazon simple storage service (amazon s3), 2009. https://s3.amazonaws.com/.

[20] The BREIN Consortium. The BREIN Project, 2008. http://www.eubrein.com/.

[21] OWL Working Group. Web ontology language (OWL), 2004. http://www.w3.org/2004/OWL

[22] J. de Bruijn, H. Lausen, R. Krummenacher, A. Polleres, L. Predoiu, M. Kifer, and D. Fensel. D16.1v0.2. The Web Service Modeling Language WSML. WSML Final Draft March, 20, 2005.

[23] E. Franconi, and S. Tessaris. 2006. The logic of RDF and SPARQL: a tutorial. In Proceedings of the Twenty-Fifth ACM SIGMOD-SIGACT-

SIGART Symposium on Principles of Database Systems, p. 355, Chicago, IL, USA, 2006.

[24] X. Wang, T. Vitvar, M. Kerrigan, and I. Toma. A QoS-aware selection model for semantic web services. In Proceedings of the Service-Oriented Computing – ICSOC 2006, pp. 390–401, Chicago, IL, USA,. 2006.

[25] L. Aroyo, P. Traverso, F. Ciravegna, P. Cimiano, T. Heath, E. Hyvönen, R. Mizoguchi, E. Oren, M. Sabou, and E. Simperl, Eds. Lecture Notes In Computer Science, vol. 5554. Springer-Verlag, Berlin, Heidelberg,

[26] M. Nagarajan, K. Verma, A.P. Sheth, J. Miller, and J. Lathem. Semantic interoperability of web services - challenges and experiences. In Proceedings of the IEEE International Conference on Web Services, pp. 373–382, Washington, DC, USA, 2006

[27] H.Lausen, A.Polleres, and D. Roman. Web Service Modeling Ontology (WSMO). W3C Member Submission, 3, 2005.

[28] J. Domingue, L. Cabral, S. Galizia, V. Tanasescu, A. Gugliotta, B. Norton, and C. Pedrinaci. IRS-III: A broker-based approach to semantic web services. Web Semantics: Science, Services and Agents on the World Wide Web, 6(2):109–132, 2008.

[29] J. Kopeck´y, T. Vitvar, C. Bournez, and J. Farrell. Sawsdl: Semantic annotations for WSDL and XML schema. IEEE Internet Computing, 11(6):60–67, 2007.

[30] J. Kopeck´y and T. Vitvar. Wsmo-lite: Lowering the semantic web services barrier with modular and light-weight annotations. In Proceedings of the 2008 IEEE International Conference on Semantic Computing, pp. 238–244, Washington, DC, USA, 2008.

Diseño y Análisis Experimental de una Plataforma de Gestión para Redes Personales

José A. Irastorza, Ramón Agüero, Luis Muñoz.
Departamento Ingeniería de Comunicaciones
Universidad de Cantabria
Avd. Los Castros, S/N, 39005 Santander.
e-mail: {angel, ramon, luis}@tlmat.unican.es

***Resumen*- Es ampliamente conocido que las tareas de gestión son fundamentales a la hora de poner en operación cualquier tipo de infraestructura de comunicaciones. Las arquitecturas usadas en entornos de gestión tradicionales estaban basadas habitualmente en modelos centralizados, los cuales no son aptos ni para las características particulares de las redes personales ni para las topologías multi-salto que las soportan. En este trabajo se propone un modelo jerárquico y distribuido e implementa dicho marco sobre una plataforma de simulación para validarlo, iniciando una serie de medidas sobre la interacción del modelo de gestión y las redes personales.**

***Palabras Clave*- Redes personales, Modelo de organización de gestión, Modelos distribuidos y jerárquicos, Simulación SNMP sobre redes personales.**

I. INTRODUCCIÓN

La evolución de los dispositivos y periféricos inalámbricos junto con el desarrollo de las tecnologías de red que los interconecta han sido cruciales para dar el despegue definitivo a redes centradas en los entornos personales. Las comunicaciones inalámbricas aportan a estas redes características tales como: movilidad de los nodos, heterogeneidad en los dispositivos y en las tecnologías de la comunicación, pero también restricciones de la conectividad dependiendo del canal y de la variabilidad de los entornos físicos o topológicos, así como del ancho de banda disponible y, por tanto, del rendimiento de dichas redes. Un escenario típico podría incluir varios tipos de dispositivos, desde modernos ordenadores portátiles hasta sensores o actuadores de bajo coste y capacidad, interconectados a través de una red inalámbrica multisalto ("Personal Network"), la cual puede desplegarse de forma autónoma sobre un área limitada geográficamente. Los desarrollos de estas redes están fundamentados en una conectividad subyacente formada por topologías de redes malladas o multi-salto.

Las topologías multi-salto o malladas son una forma relativamente nueva de desplegar redes de comunicaciones, donde los nodos son dispositivos inalámbricos que, actuando juntos de forma coordinada, crean de forma instantánea y arbitraria una estructura de comunicaciones para compartir e intercambiar información. Una de las características intrínsecas a este tipo de redes proviene del hecho que los nodos se mueven de forma libre y, como consecuencia, las conexiones entre ellos se mantienen mediante el uso de unos protocolos de enrutamiento específicos que son capaces de reconfigurar de forma dinámica la topología de la red. Estas redes han suscitado el interés de la comunidad científica, que ha puesto especial atención en las llamadas redes ad hoc, en las que cabe resaltar el papel de liderazgo investigador que ha tomado el grupo IETF MANET. Sin embargo, estos escenarios, que han servido para potenciar el auge de estas redes, caracterizados por un número relativamente grande de nodos que establecen dinámicamente una red de comunicaciones, normalmente sin una infraestructura previa subyacente que la soporte, no coinciden con los característicos de una red personal inalámbrica. En este sentido se puede indicar que las redes ad hoc multi-salto se caracterizan por fundamentarse principalmente sobre las siguientes propiedades: movilidad, cobertura variable, topología cambiante, necesidad de rutas alternativas, nodos con autonomía energética limitada, necesidad de equilibrar el tráfico entre los nodos de la red (posibilidad de desactivar el reenvío con nodos bajos de batería) e influencia del tráfico de gestión en la red en relación al tráfico de datos. Por su parte las redes personales se pueden entender como una particularización de las redes ad hoc multisalto, fundamentalmente centradas en el entorno de la persona y por lo que se matizan algunas características de las redes ad hoc, de manera que se particularicen algunas de las características anteriormente citadas, como por ejemplo: número de nodos, modelos de movilidad asociados a la persona, nodos que viajan con la persona y fijos, nodos heterogéneos (batería y prestaciones), modelos de seguridad controlados por una única entidad, necesidades de interconexión con otras redes personales o públicas, entidades de gestión administradas en el entorno de la persona.

La gestión es aspecto crucial para cualquier tipo de red y en especial para las redes personales. Por lo tanto, las tareas de gestión asociadas a las redes personales son consideradas como primordiales a la hora de garantizar su funcionamiento. A pesar de que se han estudiado ampliamente diferentes arquitecturas y modelos de gestión sobre infraestructuras de redes fijas, no ha sucedido lo mismo con las redes personales, las cuales añaden nuevas dificultades a la tarea de gestión dadas sus específicas características. En primer lugar, los enlaces de comunicaciones son intrínsecamente, poco fiables, dinámicos (debido al movimiento de los nodos) y muestran capacidades variables. Además, los nodos presentan una serie de restricciones, tales como limitaciones en las baterías y sus capacidades de procesamiento. La principal consecuencia es que la topología resultante no es predecible y, por tanto necesita de procedimientos automáticos de reconfiguración bajo demanda. Todos estos hechos imponen una serie de requerimientos a la tarea de

gestión y, en general, a cualquier servicio que vaya a implementarse sobre estas redes. Cuestiones como procedimientos/protocolos de descubrimiento, reconfiguración de los nodos y la topología, seguridad y sobrecarga de la señalización, por nombrar los más relevantes, deben ser resueltos con el objetivo de gestionar de forma eficiente una red personal.

El diseño de un marco de gestión para este tipo de redes tendrá que tener en consideración las particularidades anteriormente expuestas. En particular, el diseño del marco de gestión deberá tener especial consideración en la definición de un modelo de organización apropiado, esto es, una adecuada definición de los papeles de gestor-agente y su correcta disposición y selección entre los nodos de la red de forma que la carga de gestión afecte lo menos posible al tráfico de datos de la red, sin que la tarea de gestión y tanto la disponibilidad y calidad del servicio requerida por los usuarios de la red, se vea penalizada.

El trabajo presentado en este artículo introduce un modelo de organización que se adapta a las características de las redes personales, de forma que minimiza su impacto sobre el modelo de gestión, así como de las tecnologías inalámbricas en entornos multi-salto sobre las tareas de gestión de dichas redes. Inicialmente en el artículo se muestra una primera validación basada en un prototipo. A partir de éste, el artículo propone una mejora del modelo de organización, derivando la solución de partida hacia la definición de un modelo distribuido y jerárquico, que permite repartir de forma inteligente los papeles de agente y gestor entre los distintos nodos de la red. La necesidad de extender el análisis a entornos de red con un número elevado de nodos, justifica la utilización de herramientas de simulación que permitan validar el modelo propuesto.

Hay algunos trabajos que han analizado las implicaciones de las topologías multi-salto sobre la red de gestión, dos de los más ampliamente referenciados son el marco GUERRILLA [1] y "Ad Hoc Network Management Protocol" [2], planteando ambos una propuesta jerárquica. El primero emplea una división de los nodos en clusters, mientras el segundo utiliza unas sondas activas introduciendo cierto grado de inteligencia en el modelo. El trabajo presentado en [3] es relevante desde el punto de vista que introduce un completo modelo de información e implementa un prototipo de arquitectura de gestión basada en sondas. Un denominador común a los tres trabajos anteriores es que analizan tanto el modelo de organización como el de información. Otros trabajos centran su contribución en el modelo de organización, poniendo especial énfasis en arquitecturas de gestión basadas en una combinación de modelos distribuidos y jerárquicos. De entre ellos son destacables [4], [5] y [6], principalmente basados en técnicas específicas de clustering, o [7], que analiza como distribuir las operaciones de gestión de forma óptima en la red.

Algunos de estos trabajos usan la simulación para validar los modelos propuestos, evaluando principalmente algoritmos de clustering [2], [6]. En este trabajo se plantea la simulación como una herramienta que permite analizar tanto el modelo de organización, como la interacción de una aplicación de gestión (implementada bajo el protocolo SNMP) sobre el modelo de red personal. En la misma línea que la presentada, [8] evalúa el impacto del trafico de gestión sobre un entorno de redes de sensores, aunque utiliza un modelo no estandarizado para el protocolo de gestión.

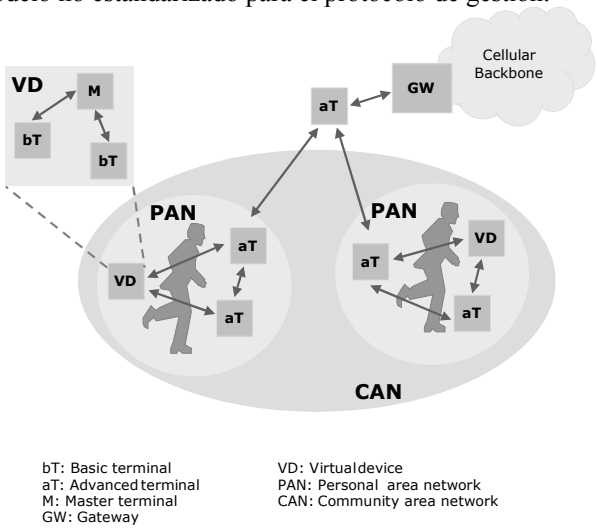


Fig. 1. Arquitectura de Red Personal.

El artículo se organiza según la siguiente estructura: La sección II presenta un primer modelo de gestión que se implementa sobre un prototipo de red personal y deriva, como propuesta de mejora, un segundo modelo, mas adecuado a las redes personales, fundamentado en paradigmas jerárquicos/distribuidos. La sección III describe la implementación del modelo mejorado de gestión sobre un entorno de simulación basado en el simulador ns y detalla los nuevos módulos que han sido necesarios implementar. La sección IV verifica la validez del modelo de gestión y presenta algunos resultados interesantes sobre el comportamiento de SNMP sobre las redes personales. Finalmente la sección V concluye el artículo, anticipando futuras líneas de trabajo que aporten mejoras al trabajo ya realizado.

II. Hacia la Gestión Distribuida de Redes Personales

En esta sección se muestra, en primer lugar, una aproximación a una arquitectura de red personal para seguidamente presentar un modelo de gestión basado en un modelo de organización jerárquico, donde la tarea de gestión sigue un patrón centralizado. A continuación dicho modelo se implementa sobre un prototipo real, validando su funcionamiento. Finalmente se presenta un modelo mejorado de organización, en el que los roles de gestión son distribuidos, permitiendo adaptarse mejor a las características de las redes personales.

La Fig. 1 muestra una arquitectura de comunicaciones que representa un escenario real en un entorno de redes personales, recogiendo características tales como la heterogeneidad, escalabilidad y movilidad, sobre una organización de tres niveles:

- Una pequeña red formada por dispositivos de baja capacidad (LDR, low data rate,) o terminales básicos (basic Terminals, bTs), con topología en estrella, donde un dispositivo Maestro (Master, M), con dos interfaces inalámbricos, coordina la comunicación, actuando como punto de control central. Al conjunto de bTs y su Maestro se le llama dispositivo virtual (virtual device, VD).

- Otra red que engloba un dispositivo virtual y uno o más dispositivos de media/alta capacidad (Medium/High Data Rate, M/HDR), también llamados terminales avanzados (avanced Terminals, aTs), formando todo el conjunto una red de área personal (Personal Area Network, PAN). Esta PAN estará estrechamente asociada a una persona.
- Una red más extensa, que comprende una asociación de PANs comunicándose entre ellas en un momento dado, a través de una topología mallada, con la posibilidad de conectarse a través de otras redes intermedias por medio de un gateway (GW), este concepto se denomina red de área comunitaria (CAN, Community Area Network).

La arquitectura mostrada se refleja en una red inalámbrica formada por una serie de dispositivos aTs ó M/HDR, y otra, constituida por terminales LDR, los cuales teóricamente no necesitan tener capacidades IP y que son controlados por el dispositivo Maestro. La conectividad los dispositivos aTs se consigue gracias al uso de un modelo multi-salto entre los distintos nodos.

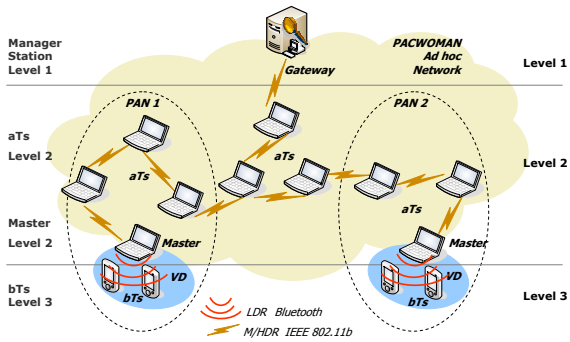


Fig. 2. Demostrador para el marco de gestión sobre redes personales.

A. Modelo de Gestión Jerárquico

El modelo de gestión jerárquico diseñado, ver Fig. 2, está compuesto por tres niveles: la llamada estación gestora se sitúa en el primer nivel, siendo la responsable de recoger (tanto directa como indirectamente) toda la información de gestión procedente de los dispositivos que están bajo su control (niveles 2 y 3). El segundo nivel comprende todos los aTs, tanto si trabajan como Maestro como si no. Los niveles 1 y 2 se comunican usando el protocolo de gestión SNMP [9]. Dentro de este nivel todos los dispositivos necesitan por tanto implementar un agente de nivel 2; adicionalmente el Maestro requiere un agente proxy que le permitirá gestionar los bTs que pertenecen a su VD y que están bajo su control. Finalmente, el tercer nivel se refiere a los bTs (fundamentalmente sensores o actuadores), que incorporan un agente de nivel 3 para intercambiar información de gestión con el gestor de nivel 2, incluido en el la implementación del dispositivo Maestro, usando un protocolo de gestión propietario.

B. Marco de red del Prototipo

El modelo de gestión descrito en el apartado anterior se implementa bajo un demostrador que básicamente está compuesto por terminales portátiles y dispositivos tipo PDA. Los terminales portátiles van a desempeñar el papel de dispositivos aTs (sean Maestros o no) y las PDAs representarán a los dispositivos bTs (emulando sensores o actuadores). El demostrador está centrado en el nivel CAN, que comprende una red ad hoc basada en la tecnología 802.11b, que interconecta dispositivos aTs y permite la comunicación entre PANs. El concepto de Dispositivo Virtual se implementa mediante la tecnología Bluetooth, que interconectará el Maestro con sus correspondientes dispositivos LDR, situados en la misma PAN, ver Fig.2.

Para completar el prototipo de gestión se han implementado dos Bases de Información de Gestión (Management Information Bases, MIBs): La MIB asociada a los dispositivos LDR define variables tales como el valor medido por el sensor, el porcentaje de batería restante, y el nombre identificativo de el sensor; por su parte, la MIB de los dispositivos M/HDR, asociada a los dispositivos aTs, recoge la siguiente información de gestión: información de identificación , tabla de enrutamiento (lo suficiente genérica para adaptarse a distintos protocolos), estado de las baterías, parámetros específicos de operación asociados a la tecnología del interfaz inalámbrico (802.11.a/b/g), como la potencia de transmisión. Para una descripción mas detallada del demostrador, el lector puede consultar [10].

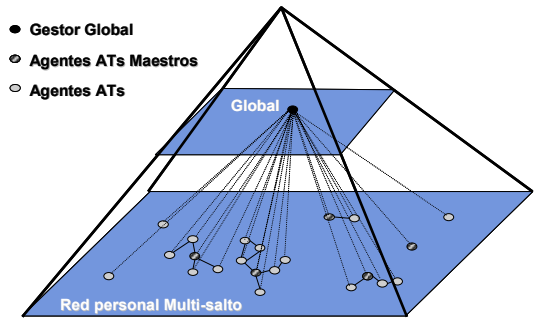


Fig. 3. Modelo centralizado/jerárquico del demostrador.

C. Modelo de Gestión Distribuido

El modelo de gestión implementado sobre el demostrador es un modelo jerárquico, pero la gestión de la red de nivel 2 formada por los aTs depende totalmente de la conectividad con el nodo gestor de nivel 1, por lo que carece de la escalabilidad y caracterizado por un modelo de organización centralizado, Fig. 3. En este sentido, asumir una única estación gestora podría provocar el intercambio de un gran tráfico de gestión entre ésta y los agentes correspondientes, así como una alta carga de procesado en dicho nodo gestor, lo que podría derivar en un unos altos tiempos de ejecución para las operaciones de gestión. Este hecho que se acrecienta sobre las redes personales, donde la importancia de las operaciones de gestión (contabilidad, configuración, etc.) es mayor y por lo tanto la sobrecarga resultante puede alcanzar valores muy altos, con el consiguiente empeoramiento del rendimiento de la red. En resumen, se puede decir que algunas características intrínsecas de las redes personales y las topologías multi-salto/malladas, como la temporalidad de los enlaces, los recursos limitados y el escaso ancho de banda, imponen una metodología para el marco de gestión diferente de la tradicional centralizada.

Con el propósito de superar estos inconvenientes, algunos trabajos han propuesto soluciones que refinan el esquema básico centralizado. Una de las más relevantes es la propuesta llamada Management by Delegation [11], que fomenta la delegación de ciertas tareas asignadas al gestor hacia los correspondientes agentes haciendo uso de scripts descargables de forma dinámica. Otras extensiones de este esquema centralizado están basadas en el establecimiento de

cierta jerarquía de agentes, permitiendo una interacción directa entre ellos. Sin embargo, estas mejoras (todavía basadas en un modelo centralizado), no solventan eficazmente todos los inconvenientes enumerados con anterioridad y, por el contrario, refuerzan la idea de usar arquitecturas de gestión basadas en modelos descentralizados con mecanismos de gestión autónoma. Siguiendo esta idea, se presenta un modelo de organización con una estructura distribuida y jerárquica.

El marco de gestión que se propone está lógicamente estructurado siguiendo una jerarquía de tres niveles, compuesta por un gestor de nivel superior, el cual puede ser seleccionado de entre un número de gestores de segundo nivel. Estos toman un rol de gestor local, controlando un conjunto de nodos, los cuales pueden entenderse como un cluster (caracterizado por algún tipo de conectividad entre sus componentes). Así, los agentes se localizan en el tercer nivel de la jerarquía. Aunque se definen tres niveles, solo existen dos planos de comunicación de gestión: uno conformado por los agentes y su correspondiente gestor (segundo nivel), y otro que interconecta todos los gestores de segundo nivel entre ellos y el gestor global (nivel 1). Como puede verse en la Fig. 4, este plano gestor crea una red superpuesta "overlay" por encima de la red personal que interconecta los gestores de segundo nivel por medio de enlaces lógicos o virtuales, cada uno de los cuales puede corresponder a una ruta particular, correspondiéndose con varios enlaces físicos, bien sobre la red subyacente, bien usando otro servicio de comunicación paralelo.

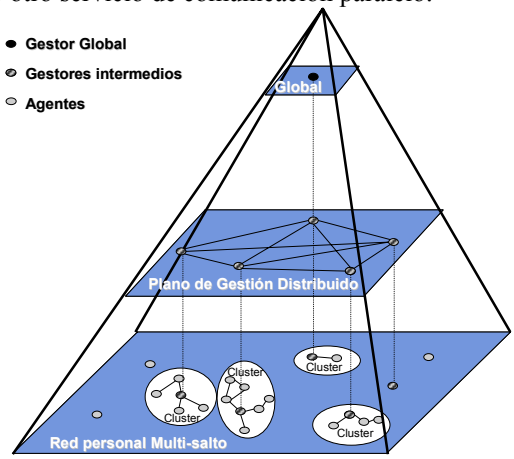


Fig. 4. Modelo de organización distribuido/jerárquico para redes personales

La arquitectura propuesta supone un plano de gestión distribuido (red superpuesta) con un número de nodos que toman el papel de gestor, cada un de ellos controlando una subred (o porción de red) y comunicándose con el resto de los gestores bajo una modalidad colaborativa y entre iguales. Esta propuesta distribuida permite que el subsistema de gestión adquiera una mayor fiabilidad y eficiencia, así como una menor sobrecarga, tanto en las comunicaciones como en los recursos de sistema.

Adicionalmente a este plano distribuido, la arquitectura de gestión también presenta una propuesta jerárquica, ya que el papel de gestor está distribuido entre dos niveles diferentes: el superior representa al gestor global, mientras que los gestores de segundo nivel pueden entenderse como gestores intermedios. Cada uno de ellos controla su propio dominio (porción de la red o cluster), recogiendo y procesando información proveniente de sus respectivos agentes y reenviando, en caso de que fuese necesario, estos datos al gestor global. También entrega información de gestión desde el gestor global hacia sus propios nodos del dominio.

III. Plataforma de Simulación: Diseño e Implementación

Network Simulator (ns) [12] es una plataforma de simulación ampliamente utilizada en numerosos trabajos procedentes de la comunidad científica, especialmente para estudios de viabilidad y escalabilidad de diferentes protocolos usados sobre redes inalámbricas. Este simulador incorpora un gran número de estrategias de enrutamiento para topologías de red ad hoc, como las utilizadas en este trabajo, así como modelos de la tecnología IEEE 802.11 muy fieles a los estándares y bien probados. Pese a ciertos defectos que afectan principalmente al modelado de los canales inalámbricos, se puede concluir que es una herramienta razonablemente fiable para llevar a cabo las evaluaciones que se proponen en este trabajo.

El entorno *ns* usa dos lenguajes de programación que se complementan: *C++* se usa para realizar un modelado detallado de los distintos protocolos, algoritmos, y entidades, mientras *tcl* (lenguaje script) es más utilizado para actuar como interfaz con el usuario, que lo utiliza para definir los escenarios a simular. En este sentido, se combinan las facilidades del primero para modelar con precisión distintas entidades, con la flexibilidad y velocidad del último, que evita la necesidad de recompilar cada vez que el escenario varía. Esta herramienta es una plataforma de simulación basada en eventos lanzados desde un programador de eventos interno que actúa como entidad fundamental.

A pesar de su gran potencial y uso generalizado, no hemos localizado otros trabajos que hayan empleado ns para evaluar la viabilidad de una arquitectura de gestión basada en el protocolo de gestión SNMP. A continuación se describen los módulos que se han implementado para posibilitar la evaluación del modelo de gestión propuesto sobre ns.

Básicamente se han implementado tres módulos: el módulo de Gestión SNMP, el módulo de adaptación rtProxy y el módulo de descubrimiento de las entidades Agente/Gestor desplegadas en la red. Existe un cuarto módulo que se encarga de seleccionar que nodos van a realizar el papel de gestores y cuáles van a ser únicamente agentes. En una secuencia temporal esté módulo será el que primero actúe sobre el nodo, pues deberá decidir que papel, Agente o Gestor, va a realizar en el modelo de gestión. Este módulo no está todavía implementado sobre ns pero sí se ha realizado un estudio fundamental con la implementación de distintos algoritmos que deciden cuál es la mejor ubicación de los gestores, optimizando una serie de métricas definidas a tal efecto. Una descripción detallada de los algoritmos y las métricas usadas puede consultarse en [13]. Para la simulación ns se parte de una asignación previa de los nodos que van a realizar el papel de gestores en la red. El módulo de descubrimiento será el encargado de lanzar los protocolos de descubrimiento para que los nodos agentes determinen el nodo que será su gestor. A partir de ese momento el módulo de gestión SNMP empezará a actuar, enviando los mensajes SNMP que permitirán obtener la información de gestión o

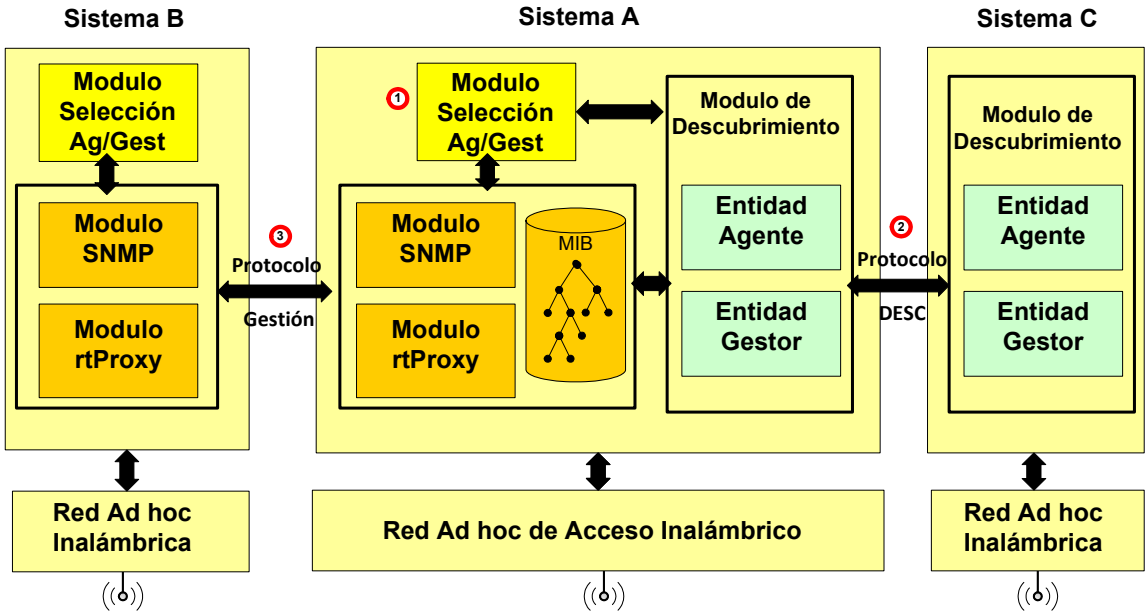


Fig. 5. Arquitectura de comunicación entre nodos: Protocolos de Gestión y Descubrimiento

actuar sobre los elementos en caso de notificaciones por parte de los agentes, ver Fig. 5

A. Módulo de Gestión SNMP sobre ns

La implementación de las entidades SNMP (agente y gestor) está basada en la clase definida sobre ns llamada *ns-agent* (se añade el prefijo *ns-* para diferenciarla de rol agente en el modelo SNMP). La correspondiente clase (*snmp*) es capaz de actuar tanto de agente como de gestor, dependiendo del rol adoptado por cada nodo de la red. Adicionalmente se crea otra clase para manejar y conformar apropiadamente los mensajes SNMP tanto de entrada como de salida a los nodos (se usa un formato de paquete basado en SNMPv2 UDP, aunque no sería complicado ampliar hacia otras versiones de SNMP).

En la Fig. 6 se describe la arquitectura de un nodo (agente/gestor) donde se resaltan los principales componentes implementados sobre ns. Los componentes GenMensSnmp y RecMenSnmp se ocuparán de crear los distintos tipos de mensajes SNMP así como de recibir y procesar los mensajes entrantes, interactuando con los componentes AgentProc y GesProc según si el nodo actúa como agente o como gestor. En el caso de un nodo realizando el papel de agente SNMP, este se encargará de recoger la información a su cargo, por medio del procedimiento Chec&Control MIB, por ejemplo información topológica obtenida de los protocolos de enrutamiento que el nodo utiliza, estado del nodo (batería), información de los sensores asociados en caso de ser un dispositivo aT Maestro, etc. En el caso de ser un nodo gestor, ejecutará el procedimiento Muestreo & Control que supone realizar un muestreo de todos sus agentes asociados y actuar sobre el enrutamiento de aquellos nodos que le notifiquen que sus baterías se encuentran por debajo de un umbral previamente fijado.

Una de las cuestiones fundamentales en una arquitectura de gestión recae sobre la información que maneja la Base de Información de Gestión o MIB. Las particularidades de una implementación basada en la simulación son sensiblemente distintas a su evaluación sobre un sistema real. En el caso de la MIB, se cuenta con una abstracción de toda la información de gestión de los nodos y de los tamaños de los propios identificadores de las variables presentes en la MIB y que se incluirán en el envío de los mensajes SNMP. En este sentido se necesita abstraer también la propia implementación del mensaje SNMP para su uso sobre la plataforma de simulación. De este modo la codificación tipo-longitud-valor de los mensajes SNMP basada en la notación ASN.1 complica notablemente (así como innecesariamente) su implementación sobre el simulador, considerando la forma en la que ns genera los paquetes. De este modo se hace uso de una lista de los posibles mensajes SNMP, asociados a su tamaño correcto en bytes, lo cual es suficiente para realizar el análisis.

B. Módulo rtProxy: Gestión Enrutamiento e Interacción con otras entidades

Tal y como se ha mencionado anteriormente, además de las entidades exclusivas de gestión, se han incluido algunos

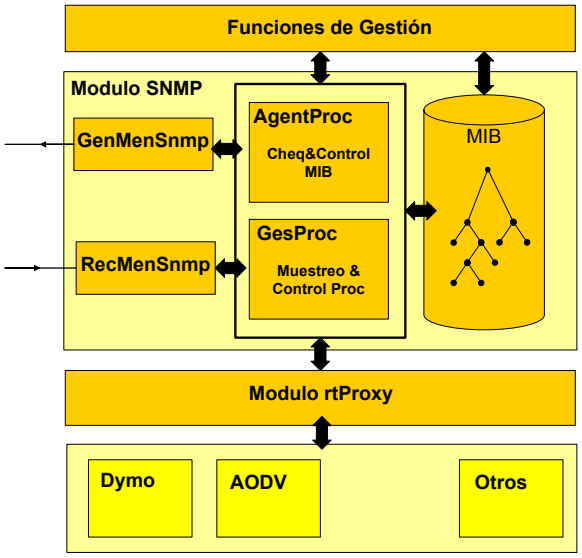


Fig. 6. Arquitectura de un nodo (agente/gestor): Módulos *ns* implementados

mecanismos para poder interactuar con otras entidades de los nodos, de forma que se pueda recoger y, eventualmente actuar, sobre información susceptible de ser gestionada. En este sentido se ha dotado a la implementación de dos distintas capacidades: (1) obtener la información del nivel de energía remanente de un nodo, por lo que se hace uso de un modelo de consumo de energía, ya que este parámetro es clave para las comunicaciones inalámbricas; (2) recoger información procedente de los protocolos de enrutamiento que el nodo está utilizando y, adicionalmente, influir sobre el modo que el nodo está trabajando referente a los procedimientos de enrutamiento, ya que puede establecer nuevas rutas, desactivar la funcionalidad de reenvío, etc.

Para facilitar la integración del módulo SNMP (ns) con el resto de la plataforma, especialmente con las entidades de enrutamiento, e independizar la implementación del módulo SNMP, se ha diseñado un Proxy (Módulo rtProxy) que actúa como un API, de manera que se puede utilizar cualquier protocolo de enrutamiento (ej. AODV, DYMO) sin tener que modificar el módulo SNMP.

C. *Módulo de Descubrimiento*

El módulo de descubrimiento implementa el protocolo que, una vez seleccionados los nodos que van a tomar el papel de gestor, permitirá que cada agente descubra qué nodo de la red va a ser su gestor, esto es, dicho protocolo permitirá hacer patente a cada nodo la pertenencia a un determinado cluster y, por lo tanto, cada gestor también conocerá qué agentes son los que controla (hacia los que debe enviar las peticiones de gestión). Igualmente los agentes conocerán sobre que nodo gestor deben enviar las notificaciones cuando se sobrepasen ciertos umbrales en variables concretas de su MIB.

Se han diseñado e implementado dos protocolos diferentes: uno proactivo y otro de tipo reactivo. El primero de ellos funciona de manera que los gestores se anuncian y son los agentes los que deciden, en caso de recibir anuncios de más de un gestor, a cual de ellos se une para formar el cluster de gestión. En el protocolo reactivo, serán los agentes los que realicen una petición en forma broadcast, solicitando unirse a un gestor. Por otro lado, son los propios agentes los que tienen la responsabilidad última acerca del gestor al cual se van asociar.

Cada uno de estos protocolos presenta una serie de ventajas e inconvenientes frente al otro; en principio, el modo proactivo puede que requiera de un consumo energético mayor, ya que los agentes deberán participar en el proceso de reenvío de los anuncios transmitidos por los gestores. Sin embargo, se garantiza en todo momento, disponer de un conocimiento más preciso acerca de la topología de la red (y la situación de los gestores) por lo que pueda que incurra en un retraso menor a la hora de establecer la asociación con el gestor correspondiente.

IV. VIABILIDAD Y MEDIDAS PRELIMINARES

Una vez que la implementación de todos los módulos que forman parte del sistema de gestión en ns-2, se plantean una serie de medidas que permitan, por una parte, analizar con mayor nivel de detalle, los resultados obtenidos sobre la plataforma real (utilizando un mayor número de nodos, incorporando movilidad, etc) y, además, corroborar el estudio llevado a cabo desde un punto de vista analítico [13], en términos de qué estrategia es mejor desde la perspectiva del despliegue de los gestores.

Se plantean una serie de medidas, para estudiar diferentes aspectos del protocolo, desde la sobrecarga de los procedimientos de descubrimiento, el tiempo necesario para asociarse a un gestor, hasta el análisis desde la perspectiva del tráfico de gestión: mensajes SNMP, influencia sobre el resto de tráfico de la red, etc.

Las características de la simulación permiten acometer esta serie de análisis, ya que se pueden llevar a cabo las medidas correspondientes de manera metódica y repetitiva. En este primer trabajo se presentarán una serie de casos de uso que ponen de manifiesto el correcto funcionamiento de los diferentes componentes implementados.

El primer escenario consiste en cuatro nodos que forman una topología en rombo, de manera que los dos extremos no son capaces de comunicarse directamente (están fuera de su rango de cobertura) [14]. Al comienzo de la simulación, el protocolo de encaminamiento usado determina emplear uno de los nodos intermedios para encaminar el tráfico entre la fuente y el destino; este proceso de reenvío supone un gasto energético adicional, por lo que el agente SNMP de dicho nodo se encarga de monitorizar el nivel de batería restante. Tras un tiempo reenviando información, el nivel de energía disponible cruza el umbral definido por la arquitectura de gestión, por lo que se genera una *Trap* que es recibida por el gestor de la red, que determina que dicho nodo debe desactivar su función de reenvío, en aras a extender su vida útil. El gestor SNMP envía una trama a dicho nodo, que desactiva su función de reenvío. A partir de ese momento es el propio agente de encaminamiento quien se percata del cambio que se ha producido en la red y busca establecer una ruta alternativa a trasvés del otro nodo intermedio que existía en el escenario. Como se puede ver en la Fig. 7, la comunicación se reinicia tras un periodo no muy relevante de tiempo, con lo que se garantiza la calidad del servicio percibida por el usuario final no sufre una degradación relevante.

Una vez que se comprueba el correcto funcionamiento del agente/gestor SNMP se trata de analizar la influencia del tráfico SNMP sobre la red, para lo que se dispone una topología relativamente sencilla, compuesta por tres nodos diferentes, que conforman una ruta de dos saltos sobre la que se envía una cierta carga de tráfico en un único sentido. El

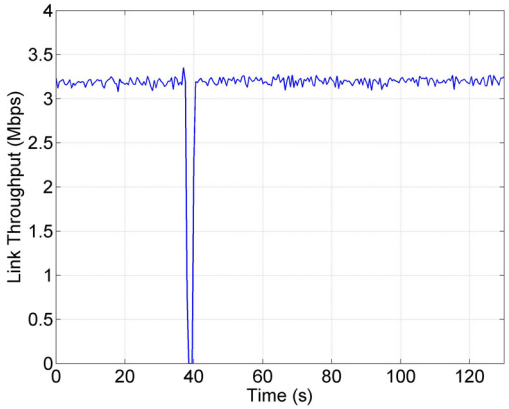


Fig. 7. Evolución temporal del throughput tras deshabilitar la función de reenvío en un nodo intermedio a través del sistema de gestión

nodo intermedio, además, actúa como gestor, que periódicamente interroga a los otros dos nodos para conocer su MIB. Como se puede ver en la Fig. 8, el efecto del tráfico de gestión es prácticamente despreciable, ya que no se percibe ningún tipo de degradación en el rendimiento del sistema, independientemente de la carga de tráfico que se esté transmitiendo (obteniendo el rendimiento teórico máximo sobre una ruta de dos saltos IEEE 802.11b). Se puede concluir, por tanto, que, a pesar de la complejidad de los procedimientos y protocolos involucrados en el sistema de gestión, el tráfico SNMP no causa una sobrecarga relevante en la red, independientemente de la frecuencia de interrogación, ya que en cualquier caso se llega al límite máximo teórico (alrededor de 3.2 Mbps sobre una ruta de 2 saltos). Se puede destacar que en cada interrogación se consulta la MIB completa, lo que podría mejorarse, preguntando por un subconjunto de la misma cada vez, garantizando una sobrecarga menor.

V. Conclusiones

Es evidente que en el entorno de redes personales, caracterizadas por la presencia de un número elevado de nodos, la necesidad de arquitecturas de gestión apropiadas es cada vez más acuciante. En esta línea de trabajo se han presentado diferentes propuestas de arquitecturas de gestión jerárquicas, que han sido analizadas desde diferentes perspectivas.

Dichos estudios pertenecen, principalmente, a dos grandes grupos: analíticos, mediante modelos matemáticos más o menos precisos, o empleando prototipos reales. Ambas estrategias presentan limitaciones, pues la primera de ellas no puede recoger una serie de detalles relevantes que sería interesante considerar, mientras que con una plataforma real se vuelve complicado desplegar el número necesario de nodos para disponer de unos resultados contrastados. Es por ello que en este trabajo se acomete el diseño, implementación y validación de la implementación de una arquitectura de gestión jerárquica/distribuida, basada en el protocolo SNMP, para ser empleada sobre redes personales, en el marco del simulador ns-2. A pesar de la innegable relevancia de esta herramienta, no existen demasiados trabajos que haya propuesto su uso para acometer el análisis de protocolos de gestión SNMP.

El diseño se ha llevado a cabo de manera modular, constando de una entidad de gestión principal, a la que se une un componente para poder llevar a cabo el descubrimiento de los nodos que toman el papel de gestor, así como un elemento necesario para poder interactuar, de manera rápida y sencilla, con el protocolo de encaminamiento (sea cual sea), lo que es fundamental en el ámbito de la gestión de redes personales.

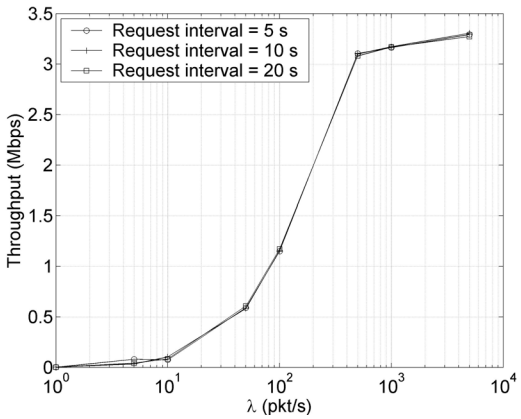


Fig. 8. Sobrecarga causada por el tráfico SNMP

Se ha comprobado el correcto funcionamiento de la implementación, a partir de casos de uso sencillos. En la actualidad, se está comenzando a analizar, de manera exhaustiva, las prestaciones de la arquitectura de gestión implementada, incorporando topologías de red más complejas, modelos de movilidad en los nodos, etc.

Agradecimientos

Los autores querrían expresar su agradecimiento al Gobierno de España por su financiación en los siguientes proyectos: Mobilia - Programa CELTIC (Avanza I+D TSI-020400-2008-82) y "Comunicaciones Cognitivas y Cooperativas sobre Entornos Heterogéneos", C3SEM (TEC2009-14598-C02-01)

Referencias

[1] C-C. Shen, C. Srisathapornphat, and C. Jaikaeo, “An Adaptive Management Architecture for Ad Hoc Networks”, IEEE Communications Magazine, vol. 41, no. 2, February 2003, pp. 108-115

[2] W. Chen, N. Jain, and S. Singh, “ANMP: Ad Hoc Network Management Protocol” IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, August 1999, pp. 1506-1531

[3] R. Badonnel., R. State, and O. Festor, “Management of Mobile Ad Hoc Networks: information model and probe-based architecture”, International Journal of Network Management, vol. 15, Issue 5, September 2005, pp. 335-347.

[4] S. Sivavakeesar, G. Pavlou, and A. Liotta, "Stable Clustering Through Mobility Prediction for Large-Scale Multihop Intelligent Ad Hoc Networks", Proc. of WCNC 2004, Atlanta, USA, March 2004.

[5] L. Fallon, D. Parker, M. Zach, M. Leitner, and S. Collins: “Self-forming Network Management Topologies in the Madeira Management System”, Proc. of AIMS 2007, Oslo, Norway, June 2007, pp. 61-72.

[6] R. Badonnel, R. State, and O. Festor, “A Probabilistic Approach for Managing Mobile Ad Hoc Networks”, Transactions on Network and Service Management, vol. 4, no. 1, June 2007, pp. 39-50.

[7] K-S. Lim, C. Adam, and R. Stadler, “Decentralizing Network Management”, KTH Technical Report, December 2005.

[8] L.B. Ruiz, F.A. Silva, T.R.M. Braga, J.M.S. Nogueira and A.A.F. Loureiro, "On impact of management in wireless sensors networks," *Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP* , vol.1, no., pp.657-670 Vol.1, 23-23, April 2004.

[9] SNMPv3, Official Internet Protocol Standard (STD 62); RFCs (3411 to 3418), http://www.rfc-editor.org/rfcxx00.html, December 2002

[10] J.A. Irastorza, R. Agüero, V. Gutierrez, and L. Muñoz, “ Beyond Management in Ad Hoc, Heterogeneous WPAN Environments: an Experimental Approach” IEEE/IFIP Network Operation and Management Symposium (NOMS), April 3-7 2006, Vancouver, Canada

[11] Y. Yemini, G. Goldszmidt, and S. Yemini, “Network Management by Delegation”, Second International Symposium on Integrated Network Management IM’91, Washington, D.C., April 1991, pp. 95-107.

[12] “Ns-2 network simulator”, http://www.isi.edu/nsnam/ns/.

[13] J.A. Irastorza, R. Agüero, L. Muñoz, “ Selección de gestores sobre una arquitectura de gestión jerárquica y distribuida para redes personales, Jornadas de Ingeniería Telemática, JITEL 2009, Cartagena, Murcia, Septiembre 2009.

[14] J.A. Irastorza, R. Agüero, and L. Muñoz, “Fostering the simulation-based evaluation of management architectures over multi-hop topologies“ IEEE/IFIP Network Operation and Management Symposium (NOMS’08), Salvador do Bahia, Brazil, April 2008.

AVISS: Aplicación Adaptativa de *Streaming* de Vídeo

Guillermo Díaz-Delgado[a, b], Cristina Muñoz Jaime[a], Carolina Tripp Barba[a], Mónica Aguilar Igartua[a]

[a] Departament d'Enginyeria Telemàtica
Universitat Politècnica de Catalunya (UPC)
C/ Jordi Girona 1-3, Mòd. C3, Campus Nord, 08034 Barcelona

[b] Facultad de Informática
Universidad Autónoma de Querétaro (UAQ)
Av. de las Ciencias s/n, Juriquilla, Querétaro, C. P. 76230, México

{gdiaz, ctripp, monica.aguilar}@entel.upc.edu, crismj84@gmail.com

***Resumen*- En este trabajo presentamos AVISS (*Adaptive VIdeo-Streaming Application*), una aplicación para la transmisión adaptativa de *streaming* de vídeo en redes móviles ad-hoc (MANET, *Mobile Ad-hoc Networks*). AVISS pretende ofrecer una mejor Calidad de Experiencia (QoE, *Quality of Experience*) al usuario final mediante la auto-adaptación a las condiciones cambiantes de operación de la red. Para medir la calidad del vídeo recibido, también se ha definido una nueva métrica llamada Calidad del GoP (QoG, *Quality of GoP*). Esta métrica se calcula en el destino final en tiempo real y depende de la cantidad y tipo de cuadros de vídeo recibidos por cada GoP (*Group of Pictures*) transmitido, por lo que está relacionada con la QoE que el usuario final podría percibir. AVISS ha sido implementado utilizando la versión de RTP/RTCP del simulador de redes NCTUns, y sus prestaciones se han evaluado bajo diferentes condiciones de operación en redes MANET, reconocidas por ser altamente dinámicas.**

***Palabras Clave*- Aplicación adaptativa, Calidad de Experiencia, Calidad del GoP, MANET, *Streaming* de Vídeo.**

***Abstract*- In this paper we present AVISS (Adaptive VIdeo-Streaming Application), an adaptive Client-Server application for video-streaming over Mobile Ad-hoc NETworks (MANETs). AVISS pretends to offer a better Quality of Experience (QoE) to the end user of the video-streaming system by adapting itself to time-varying operating conditions of the network. In order to measure the quality of the received video, we also define a new metric called Quality of GoP (QoG), which is easy to measure at the destination node, it does not require the original transmitted video as reference and it is related to the QoE end-user could perceive. As a proof of concept, AVISS has been implemented over a modified version of the RTP/RTCP implementation included with the NCTU network simulator (NCTUns) and we have evaluated its performance on simulated MANETs under several different operating conditions.**

***Keywords*- Adaptive Application, MANET, Quality of Experience, Quality of GoP, Video-streaming.**

I. INTRODUCCIÓN

Durante varias décadas, los servicios de vídeo se han utilizado con diversos fines, tales como educativos, divulgativos, de entretenimiento y para la seguridad en lugares públicos y privados. Inicialmente, el vídeo era capturado, registrado, transmitido y reproducido de forma completamente analógica. Pero la llegada de los circuitos digitales integrados y de los ordenadores condujo a la digitalización del vídeo, trayendo consigo el desarrollo de técnicas de compresión para su almacenamiento y transmisión de forma más eficiente [1].

Por otro lado, el actual ritmo de vida de las personas impone la necesidad de trabajar y comunicarse sin depender de las ataduras impuestas por una infraestructura fija de comunicaciones de una determinada tecnología. Hoy día todo individuo quiere estar informado y comunicado, independientemente del momento y de su ubicación, lo que implica que los dispositivos terminales deben ser polivalentes y multifuncionales. El constante incremento del número de terminales inalámbricos y ordenadores portátiles con múltiples interfaces a diferentes tecnologías de comunicación, es sólo una muestra del creciente interés por los sistemas ubicuos y descentralizados [2]. Por ello, en los últimos años se han dedicado gran cantidad de recursos al estudio y desarrollo de las redes inalámbricas en general, y particularmente a las redes ad-hoc y a su versión móvil, las MANET (*Mobile Ad Hoc Networks*) [3], que aún se hallan en proceso de desarrollo e investigación.

Paralelamente, la mejora constante de las prestaciones de los dispositivos empleados ha permitido el desarrollo de nuevos servicios que demandan un mayor nivel de Calidad de Servicio (QoS, *Quality of Service*) a la red de transmisión de datos, tales como la videoconferencia y el *streaming* de vídeo (*video-streaming*). Entendemos por *video-streaming* el servicio que proporciona la transmisión continua de flujos de vídeo para su reproducción o "consumo" en tiempo real (p. ej. YouTube). Esta demanda de QoS se traduce en un requerimiento de ancho de banda dedicado exclusivamente a la aplicación, así como en la imposición de restricciones respecto a la tasa de pérdidas y al retardo máximo tolerados durante la transmisión de los paquetes de datos entre emisor y receptor. Sin embargo, las redes utilizadas para la provisión de estos servicios (p. ej. Internet o las redes ad-hoc) no ofrecen actualmente ningún tipo de QoS, aunque en los últimos años se han propuesto numerosos mecanismos, protocolos y plataformas que ofrecen cierto nivel de QoS a los servicios multimedia [4-7]. Además, es importante considerar que la provisión de QoS en redes altamente dinámicas requiere de un enfoque holístico, basado en una arquitectura de comunicación entre capas (*cross-layer*), que

incluya la adaptabilidad de la propia capa de aplicación a las posibilidades cambiantes de la red [8]. Esto último es especialmente apropiado para redes inalámbricas que deben brindar soporte a la movilidad de los usuarios [9].

El primer objetivo de este artículo es presentar AVISS (*Adaptive VIdeo-Streaming Application*), una aplicación adaptativa para *streaming* de vídeo diseñada para mejorar la Calidad de Experiencia (QoE, *Quality of Experience*) del usuario. El algoritmo de adaptación de AVISS tiene en cuenta las condiciones dinámicas de operación de las redes de datos IP en general, es decir, la posibilidad de la variación del ancho de banda disponible y el cambio de topología (esto último debido a la congestión en alguna parte de la red o a la caída de los enlaces entre los nodos). Una solución similar ha sido propuesta en [11] para redes IP con infraestructura cableada (p. ej. Internet y ATM), en las que la tasa de error de bit (BER, *Bit Error Rate*) es baja y la mayoría de las pérdidas de paquetes de datos pueden atribuirse a la congestión en la red. AVISS, por su parte, ha sido diseñada pensando sobre todo en la transmisión de *streaming* de vídeo en escenarios muy hostiles como los presentados por las MANETs, las cuales son altamente dinámicas debido a la movilidad de los nodos que las conforman y a que no depende de una infraestructura fija. Gracias a que la transmisión de vídeo en tiempo real es relativamente tolerante a la pérdida de datos, pero poco tolerante respecto al retardo de los mismos [11], AVISS ha sido desarrollada en torno a los protocolos RTP/RTCP (*Real Time Protocol/Real Time Control Protocol*) [12] sobre UDP (*User Datagram Protocol*) [13] como protocolos de transporte.

El segundo objetivo de este trabajo consiste en presentar un análisis de prestaciones que ayude a determinar si la utilización de una aplicación adaptativa de *streaming* de vídeo como AVISS es capaz de proporcionar una mejor QoE.

El resto de este documento está dividido como sigue. En la Sección II se describen las características del servicio de *streaming* de vídeo que ofrece AVISS y los mecanismos de adaptación implementados. Las características específicas de la secuencia de vídeo original y el proceso de codificación utilizado para generar los ficheros de vídeo que requiere la aplicación se presentan en la Sección III. Luego, en la Sección IV se describen los experimentos realizados mediante simulación y las métricas analizadas, mientras que en las Secciones V y VI se presentan y discuten los resultados obtenidos al utilizar AVISS en redes ad hoc estáticas (Sección V) y con nodos móviles (Sección VI), los cuales se contrastan contra los resultados obtenidos con una aplicación de *video-streaming* no adaptativa. En la Sección VII se hace una discusión general de los resultados obtenidos en todos los experimentos realizados. Finalmente, en la Sección VIII se presentan algunas conclusiones y se describe el trabajo futuro.

II. CARACTERÍSTICAS DEL SERVICIO

La aplicación diseñada, AVISS, consta de dos partes diferenciadas en función del tipo de elemento que la ejecute; es decir, dependiendo de si el nodo actúa como emisor o receptor las funciones a realizar serán diferentes (servidor o cliente del flujo de vídeo, respectivamente).

En la Fig. 1 se muestra cómo el servidor almacena dos flujos de un mismo vídeo codificados con diferentes pasos de cuantificación, y por tanto diferentes calidades de vídeo: alta calidad (HQ, *High Quality*) y baja calidad (LQ, *Low Quality*). El nodo fuente emite el flujo de vídeo de una u otra calidad en función del estado de la red. La información para evaluar el estado de la red la genera el receptor en función de las pérdidas detectadas y la transmite a la fuente mediante paquetes de señalización RTCP.

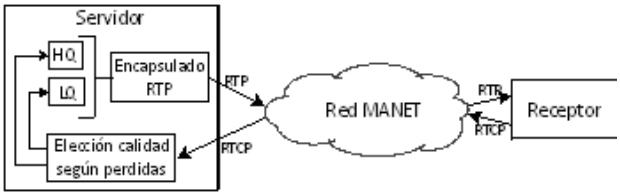


Fig. 1. Esquema general de AVISS.

A. Control adaptativo del flujo de vídeo

La red se monitoriza de forma continuada desde el emisor, mediante la información contenida en los paquetes RTCP generados por el nodo destino, los cuales contienen información (retardo, pérdidas) relativo al flujo de vídeo encapsulado en los paquetes RTP transmitidos por el servidor. Al recibir la información de control, el emisor actualiza una variable que monitoriza las pérdidas del canal. Para realizar este cálculo se ha aplicado un filtro EWMA (*Exponential Weighted Moving Average*) como el definido en la ecuación (1), de forma que se pondera la medida instantánea (*current_losses*) por un factor (α) y el valor acumulado, procedente del histórico (*losses*[*i*-1]), por un factor (1-α). Cuando las pérdidas están por debajo de un determinado umbral se transmite el flujo de alta calidad (HQ), mientras que si están por encima del umbral se transmite el flujo de baja calidad (LQ).

$$losses[i] = (1-\alpha) * losses[i-1] + \alpha * current\_losses \quad (1)$$

Este mecanismo de adaptación presenta, sin embargo, un inconveniente importante en el caso de que las pérdidas de la transmisión se hallen alrededor del único umbral definido, pues la calidad del vídeo transmitido cambiaría constantemente y en consecuencia se tendría un sistema "nervioso". Una pequeña variación del porcentaje de paquetes perdidos podría hacer que cambiara el estado percibido de la comunicación, cuando en realidad la desviación es mínima.

Con el objetivo de reducir los cambios innecesarios de calidad del vídeo transmitido, se ha implementado en AVISS, como en [10], un ciclo de histéresis (Fig. 2). Así, cuando el valor de las pérdidas es cercano a alguno de los umbrales y si éstos se traspasan, es necesario un incremento o decremento considerable para volver al estado anterior.

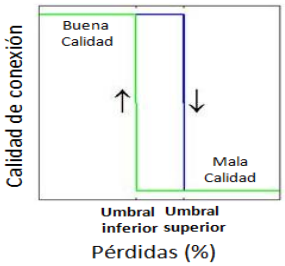


Fig. 2. Ciclo de histéresis.

Por otro lado, en caso de considerarse necesario un cambio en la codificación de los cuadros de vídeo emitidos, el servidor deberá esperar al inicio del siguiente GoP (*Group of Pictures*), pues todos los cuadros de vídeo de un GoP están codificados con la misma calidad y su interdependencia (Fig. 3) obliga esta medida. Para ello, en el encapsulado del primer paquete RTP de todos los cuadros I se ha incluido un campo que indica la codificación utilizada en cada GoP (HQ o LQ).

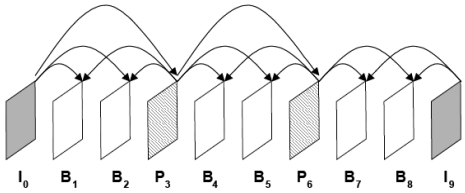


Fig. 3. Dependencias entre cuadros de un GoP.

B. Emisión adaptativa de paquetes RTCP

El intervalo mínimo entre paquetes de señalización RTCP definido en el RFC1889 [12] es de 5 seg., para evitar ráfagas de paquetes de este tipo que limiten excesivamente el ancho de banda disponible. En nuesro caso, esta restricción puede provocar que la información de control quede obsoleta y que la aplicación no responda adecuadamente a los cambios en la red. Para llegar a un compromiso entre el ancho de banda consumido y la precisión de las medidas, se ha optado por controlar de forma dinámica la frecuencia de envío de paquetes RTCP desde el nodo receptor según sea la calidad de la comunicación de extremo a extremo.

El algoritmo diseñado reduce el período entre emisiones de paquetes de señalización RTCP consecutivos cuando el porcentaje de paquetes perdidos es elevado. Así se consigue tener mayor resolución en las estadísticas. Dicho período se incrementa a medida que la calidad de la comunicación mejora, puesto que no es necesario tal nivel de detalle. Ambas variaciones se realizan de forma gradual, para reducir el impacto de incrementos bruscos en las pérdidas y la consecuente degradación de la calidad experimentada por el usuario. La implementación de este planteamiento se ha realizado mediante la modificación de la fracción del ancho de banda dedicado a la emisión de paquetes RTCP. Tomando en consideración estos dos aspectos, como cota inferior del ancho de banda de señalización (cuando hay buena comunicación) se ha definido el 0.5% del ancho de banda requerido para el envío de datos de vídeo HQ, y como cota superior el 1% (cuando hay muchas pérdidas). El incremento en el número de paquetes de señalización es el costo a pagar por la adaptación dinámica. Cuando la pérdida de paquetes de vídeo es mayor, el número de paquetes RTCP emitidos se incrementa para que la aplicación pueda adaptarse rápidamente a las condiciones de transmisión.

De acuerdo con la especificación de RTP/RTCP [12], el intervalo de emisión entre paquetes RTCP consecutivos debe variar de forma aleatoria en un rango entre 0.5 y 1.5 veces su valor nominal calculado hasta el momento. Esto se hace con el objetivo de disminuir la probabilidad de que se produzca una sincronización indeseada entre paquetes de múltiples participantes de una sesión. Según los valores anteriores, para el caso de una fracción del RTCP del 1%, con un período nominal de 250 ms, el valor resultante se obtendría entre 125 y 375 ms, mientras que para una fracción del RTCP del 0.5% (período nominal de 500 ms), este rango se situaría entre 250 y 750 ms. De esta manera el servidor podría llegar a recibir hasta 4 paquetes de señalización en el intervalo de un GoP. No obstante, para evitar la emisión de paquetes innecesarios se ha decidido disminuir el rango de aleatoriedad a un valor entre 0.8 y 1.2 veces el valor nominal. Bajo estas circunstancias, en caso de tener una comunicación con un bajo porcentaje de pérdidas, el tiempo entre paquetes variaría entre 400 y 600 ms, mientras que para una comunicación de mala calidad este tiempo se reduciría hasta un valor en el intervalo de 200-300 ms. Aunque a primera vista no resulta evidente la transmisión de un mayor porcentaje de paquetes de control cuando el sistema presenta mayor tasa de pérdidas, el tráfico de control es menor que la cota máxima del 5% del ancho de banda utilizado para la transmisión de datos ([12]).

C. Otras funciones implementadas

El principal objeto de esta aplicación es transmitir GoPs de diferentes calidades a lo largo de la sesión RTP, para adaptarse a las circunstancias del sistema. Esto implica que el receptor debe ser capaz de reconocer la codificación que se ha utilizado, para poder decodificar cada cuadro correctamente. La detección de la codificación empleada en un GoP se puede realizar gracias a que se ha introducido un nuevo campo, tras la cabecera RTP del primer paquete de los cuadros de vídeo tipo I, en el que se indica la calidad con que se ha codificado el GoP que inicia (HQ o LQ).

Para facilitar el trabajo del decodificador también se ha optado por marcar el último paquete de cada cuadro de vídeo, mediante el campo *marker* de la cabecera RTP. Así, el receptor podrá detectar el inicio y el fin de cada cuadro de vídeo dentro del flujo de paquetes RTP que envía el emisor.

III. Descripción del vídeo

El vídeo original consiste en una secuencia YUV (luminancia y crominancia) 4:2:0 progresiva con resolución CIF (*Common Intermediate Format*) de 352x288 píxeles con una duración de 300 segundos. La secuencia ha sido codificada en formato MPEG-4 ASP@L3 [14] a 30 cuadros por segundo, y con GoPs cerrados formados por 16 cuadros, según la secuencia: IBBPBBPBBPBBPBBP, con una matriz de cuantificación tipo H.263 [15] sin detección de cambios de escena. Con estas características, se han creado dos ficheros de vídeo comprimido MPEG-4 con calidades diferentes. Para el vídeo de alta calidad (HQ) se utilizó una codificación a tasa constante (CBR, *Constant Bit Rate*) de 384kbps, y para el vídeo de baja calidad (LQ) se utilizó una tasa de 192kbps. A partir de los ficheros de vídeo MPEG-4 se han generado los ficheros de trazas de vídeo con la aplicación MPEG4 [16], los cuales se utilizan como pauta para enviar los datos de los ficheros de vídeo. Gracias a la compresión MPEG-4, el vídeo es adecuado para transmitirse en redes con ancho de banda limitado como las MANETs.

IV. Características de las simulaciones

En esta sección se describen los experimentos realizados con el simulador NCTUns [17] y las métricas analizadas.

A. Características de las redes

Las redes simuladas son redes inalámbricas multisalto formadas por nodos con interfaces IEEE 802.11b trabajando

en modo ad-hoc [18]. Se ha establecido un rango de transmisión de los nodos de 125 m y un radio de interferencia de 200 m, así como una tasa de transmisión nominal de 11 Mbps. El protocolo de encaminamiento utilizado en las simulaciones generadas es AODV (*Ad-hoc On Demand Distance Vector*) [19]. Para el caso de las redes con nodos móviles, las trayectorias de movimiento de los nodos se han generado con la herramienta Bonnmotion [20], utilizando el modelo de movilidad *RandomWaypoint*.

Durante los experimentos, las diferentes sesiones de comunicación simuladas se han incorporado con un desfase de 10 segundos respecto al inicio de la sesión anterior, tal como se puede observar en la Fig. 4. Por lo tanto, la máxima duración de una simulación es de 390 seg (cuando se tienen hasta 10 sesiones de comunicación de forma simultánea).

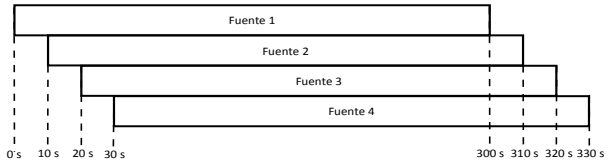


Fig. 4. Inicio desfasado de las comunicaciones.

El ciclo de histéresis programado en la aplicación tiene un umbral inferior igual al 5% de pérdidas de los paquetes RTP, mientras que el umbral superior es del 10%.

B. Diseño de experimentos

Las simulaciones se realizaron siguiendo un Diseño de Experimentos (DOE, *Design of Experiments*) de tipo factorial [21], con el fin de determinar el efecto de diferentes factores en el comportamiento y rendimiento de las redes y de la aplicación desarrollada. Los factores considerados en estas simulaciones han sido los siguientes:

- Tamaño de la superficie de la red
- Número de nodos en la red
- Máximo número de transmisiones simultáneas
- Máxima velocidad de movimiento de los nodos

Así, se definieron los siguientes 3 escenarios de red, en los cuales se ha hecho variar el número de transmisiones simultáneas y la velocidad de los nodos:

- Escenario mediano: Red mediana (20 nodos) y superficie mediana (500m x 500m).
- Escenario grande: Red grande (50 nodos) y superficie grande (1250m x 500m).
- Escenario denso: Red grande (50 nodos) y superficie mediana (500m x 500m).

Asimismo, se definieron tres etapas de experimentación. Las dos primeras fases se realizaron utilizando la aplicación adaptativa, mientras que en la tercera etapa se utilizó una aplicación convencional no adaptativa. Cabe destacar que se realizaron cinco repeticiones de cada una de las simulaciones, a fin de obtener estimaciones más fiables, y los resultados mostrados son el promedio de los valores obtenidos en cada repetición.

En la Fig. 5 se ha representado el conjunto de simulaciones realizadas para cada escenario de red.

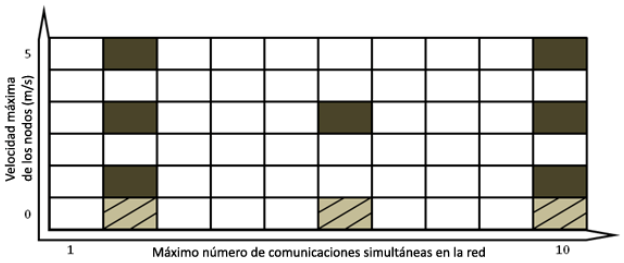


Fig. 5. Simulaciones realizadas para cada escenario de red.

C. Métricas analizadas

Para este estudio se han buscado métricas objetivas y cuantificables, que representen el comportamiento de la aplicación en los escenarios simulados. Con este objetivo se han analizados las siguientes métricas:

- *Retardo extremo a extremo*: Contempla el retardo únicamente de los cuadros de vídeo que el receptor recibe correctamente, y dentro de la ventana temporal establecida.
- *Pérdidas de los paquetes*: Básicamente se analizan las pérdidas de los paquetes RTP, promediando las diferentes fuentes y realizaciones de una misma simulación.
- *Pérdidas de cuadros de vídeo*: Se estudian las pérdidas, considerando como tal los cuadros de vídeo incompletos, pero también aquellos que han llegado en un tiempo superior a 2 segundos al instante en que se requerían.
- *Calidad de GoP* (QoG*, Quality of GoP*): Esta métrica pretende medir, basada en datos estadísticos, la calidad de percepción del vídeo que tendrá el usuario final. Para ello se ha calculado un porcentaje de calidad según la cantidad y tipo de cuadros de vídeo de un mismo GoP recibidos correctamente (a tiempo y decodificables) en el receptor. La QoG se calcula en el destino final en tiempo real, no requiere como referencia el vídeo originalmente transmitido y está relacionada con la Tasa de Vídeo Decodificado y Reproducible (DFR*, Decodable Frame Rate* [22, 23]), por lo que es un estimador de la QoE percibida por el usuario final.

Según la dependencia jerárquica entre los cuadros de un GoP, con respecto al proceso de decodificación del vídeo (ver Fig. 3), se ha asignado un peso específico a cada cuadro. Así pues, se ha considerado como más valioso el cuadro de tipo I, seguido de los cuadros de tipo P, cuya importancia decrece a medida que aumenta su posición dentro del GoP, y finalmente los cuadros de tipo B, manteniendo todos ellos el mismo valor. En la Tabla 1 se presenta la contribución de los diferentes cuadros de vídeo a la QoG.

Tabla 1. Contribución de los cuadros de vídeo a la QoG.

Tipo de cuadro	Contribución
Cuadro I	0.30
1er cuadro P	0.22
2o cuadro P	0.16
3er cuadro P	0.11
4o cuadro P	0.07
5o cuadro P	0.04
1 Cuadro B (x10)	0.01

V. SIMULACIONES EN REDES ESTÁTICAS

En esta sección se presentan los datos globales obtenidos de la evaluación de prestaciones de AVISS en redes ad-hoc estáticas, es decir, en las que los nodos permanecen fijos.

A. *Retardo extremo a extremo*

La evolución temporal del retardo medio extremo a extremo consta de tres fases diferenciadas, como se muestra en la Fig. 6. En primer lugar, se puede apreciar que, cada vez que se establece una nueva transmisión de vídeo desde un nodo fuente (instantes 0, 10, 20 y 30 segundos de la Fig. 4), se incrementa considerablemente del retardo medio para todas las fuentes simultáneas. Luego, cuando se llega al máximo número de fuentes simultáneas, el retardo permanece casi constante (caso de 2 fuentes simultáneas) e incluso decrece ligeramente (casos de 6 y 10 fuentes simultáneas). Por último, en la etapa de finalización de las transmisiones (instantes 300, 310, 320 y 330 segundos de la Fig. 4), el retardo medio decrece rápidamente.

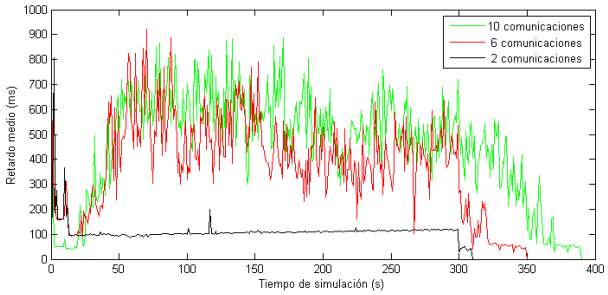


Fig. 6. Evolución del retardo en red densa con aplicación adaptativa.

En la Fig. 6 también se puede observar cómo se produce un incremento puntual en el retardo cada vez que se incorpora una nueva fuente al sistema. Al introducirse un nuevo flujo, el protocolo de enrutamiento necesita un cierto tiempo para hallar un camino entre el origen y el destino, así como para actualizar las tablas de encaminamiento de los nodos intermedios, por lo que el retardo extremo a extremo es ligeramente superior al inicio de cada nueva comunicación.

Cabe destacar que el comportamiento en el eje temporal es similar en ambos tipos de aplicaciones (convencional y adaptativa), si bien se ha comprobado que el retardo medio es mayor cuando se emplea la aplicación adaptativa. Este fenómeno se muestra en la Fig. 7 (columna de la izquierda de cada grupo), junto con los resultados obtenidos con la aplicación estándar al transmitir el vídeo HQ (columna central) y el vídeo LQ (columna de la derecha).

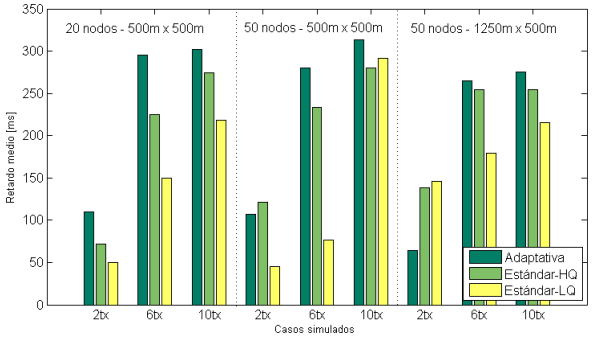


Fig. 7. Retardo medio según el tipo de aplicación empleada.

La razón principal del empeoramiento del retardo, se debe a las nuevas funcionalidades que incorpora la aplicación adaptativa (potencial cambio del flujo a emitir a lo largo del tiempo). De esta manera, al añadir nuevas tareas en los nodos de origen y destino, el retardo se ve afectado.

En la aplicación convencional se ha detectado, además, un comportamiento diferenciado del retardo al aplicar distintas tasas de codificación del vídeo. En la Fig. 8 se observa cómo en una red con tráfico moderado (6 transmisiones simultáneas) se producen retardos mucho mayores cuando se transmite el vídeo con mayor calidad, mientras que para una red con mayor tráfico (10 transmisiones simultáneas) se obtienen unos valores muy similares para ambas calidades del vídeo, debido a la saturación del sistema. Sin embargo, se ha de especificar que el comportamiento mostrado se refiere al retardo de los cuadros de vídeo considerados como válidos. Esto significa que en estos datos sólo se han computado los cuadros de vídeo completos recibidos dentro de la ventana temporal de recepción para su decodificación.

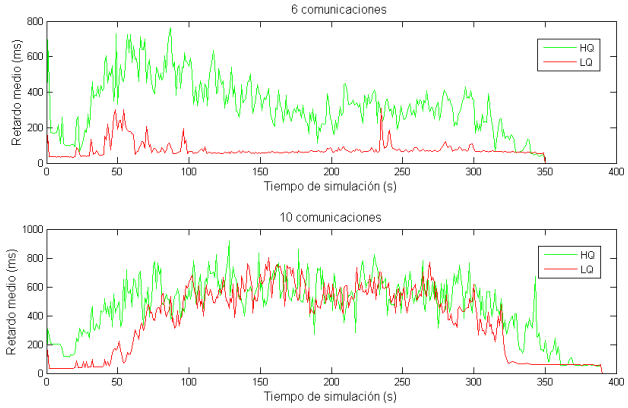


Fig. 8. Evolución del retardo (aplicación convencional).

B. *Comportamiento de los paquetes*

La evolución general de los paquetes se basa en un incremento de las pérdidas a medida que aumenta el número máximo de comunicaciones en la simulación. Cuantas más fuentes se hallen operativas simultáneamente, mayor será el tráfico que circula por la red, y por tanto hay una probabilidad mayor de pérdidas, causadas principalmente por colisiones y saturación en los nodos.

En la Fig. 9 se puede observar cómo, con la aplicación adaptativa, se reduce el porcentaje de pérdida de paquetes en aproximadamente un 5% respecto a la emisión de vídeo de alta calidad.

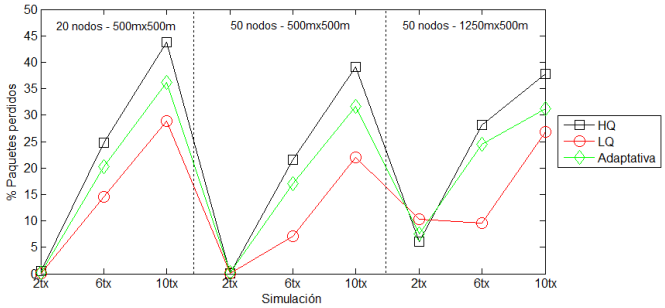


Fig. 9. Paquetes perdidos según aplicación.

Este comportamiento se debe a que, con la aplicación adaptativa, el número medio de paquetes necesario para transmitir un cuadro de vídeo completo es menor que para el vídeo de alta calidad, por lo que hay menos paquetes circulando en la red, y por tanto las pérdidas se reducen. En

el caso específico de 2 fuentes simultáneas en una red de 50 nodos en una superficie de 1250mx500m, se puede observar que se presentan más pérdidas que en los otros escenarios. Esto se debe principalmente a que las rutas entre las fuentes y los destinos móviles se pierden con mayor frecuencia debido a que las distancias entre ellos son mayores.

C. *Comportamiento de los cuadros*

Un cuadro de vídeo se transporta en uno o varios paquetes, de manera que el análisis referente a los cuadros tendrá rasgos similares al comportamiento observado en los paquetes. Así, al transmitir el vídeo con la aplicación adaptativa se obtienen pérdidas menores que al transmitir únicamente el flujo de vídeo de alta calidad, pero mayores que con la secuencia de vídeo de baja calidad. En la Fig. 10 se han representado las pérdidas de los cuadros para un escenario denso, desglosadas en función de la calidad de los cuadros de vídeo emitidos. Según el algoritmo de adaptación de la aplicación diseñada, cuando el canal tenga muchas pérdidas sólo se emitirá los cuadros de baja calidad; por lo mismo se pierde un número mayor de cuadros de vídeo cuando están codificados con una tasa menor.

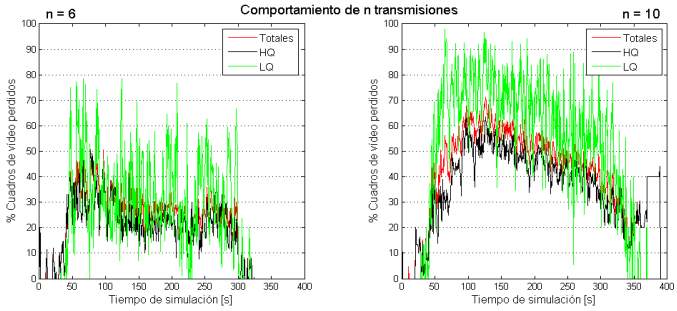


Fig. 10.Cuadros perdidos con aplicación adaptativa.

En estas situaciones se puede apreciar como los elevados valores obtenidos en los cuadros de tasa de codificación menor tiene escasa influencia en el cómputo de las pérdidas. Esto se debe a que los parámetros escogidos provocan que alrededor del 90% se emitan paquetes de alta calidad, por lo que el peso de este tipo de paquetes es mucho mayor.

D. *Calidad subjetiva de vídeo*

La distribución de las pérdidas puede ser un factor más importante para el usuario final que el número de paquetes y cuadros perdidos. Por esta razón, es de gran importancia la calidad global percibida por el receptor. Según se puede observar en la Fig. 11 esta calidad depende en gran medida de la cantidad de tráfico inyectado en el sistema. Así pues, con una cantidad de tráfico reducido la propuesta adaptativa ofrece un mejor comportamiento que con la aplicación estándar y vídeo de alta calidad (HQ), mientras que en intervalos con múltiples comunicaciones activas se observa una notable degradación en la calidad subjetiva respecto de la aplicación estándar y vídeo de baja calidad (LQ), aunque es ligeramente superior a la obtenida con la aplicación estándar y vídeo de alta calidad (HQ). Con la aplicación adaptativa el número de cuadros de vídeo que alcanzan el destino, por cada GoP transmitido, es mayor que con la aplicación estándar transmitiendo vídeo HQ, pero menor que cuando sólo se transmite vídeo LQ. Sin embargo, la calidad promedio de los cuadros de vídeo de la aplicación adaptativa es mayor que cuando sólo se transmite vídeo LQ.

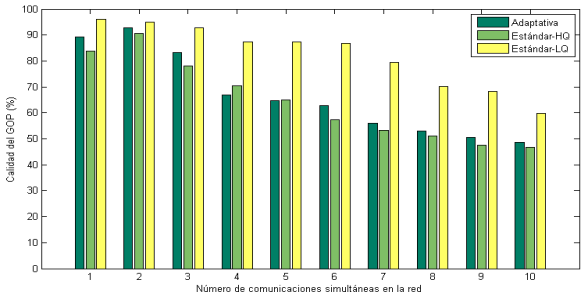


Fig. 11.Calidad del GoP en red grande.

VI. SIMULACIONES EN REDES MÓVILES

En esta sección se presentan los resultados de la evaluación de prestaciones de la aplicación adaptativa de *video-streaming* en redes MANET, esto es, redes ad-hoc con nodos en movimiento.

A. *Retardo extremo a extremo*

Tras evaluar el retardo medio en los tres escenarios bajo diferentes velocidades con la aplicación diseñada, se obtuvieron los resultados que se muestran en la Fig. 12.

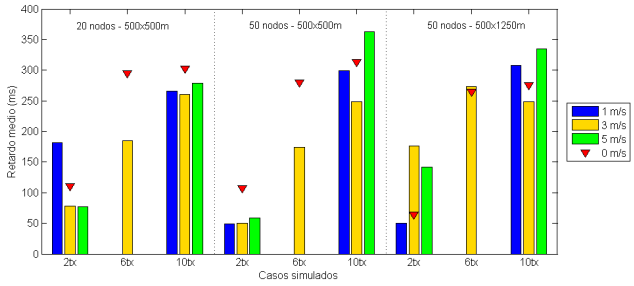


Fig. 12.Retardo en función de la velocidad de los nodos.

Como se puede apreciar, el retardo extremo a extremo de los cuadros tiende a ser mayor en la red estática (triángulos en Fig. 12). Esto se debe a que en una red con cierta movilidad de los nodos, las rutas varían constantemente, lo que favorece la conectividad entre el nodo origen y el destino al menos durante algún período, además de que se disminuye la probabilidad de que un nodo converjan varias rutas, lo que produciría que las colas de esos nodos se llenaran, provocando un mayor retardo debido a un congestionamiento. En resumen, en redes con un cierto grado de movilidad el tráfico parece que se balancea.

B. *Comportamiento de los paquetes y de los cuadros*

La movilidad en los nodos implica casi siempre una pérdida de ruta entre fuente y destino, por lo que es habitual que se produzca un incremento sustancial de los paquetes que se pierden. En casos extremos se pueden ocasionar desconexiones, si la duración de este intervalo con pérdida de información es suficientemente elevada (del orden de decenas de segundos). De manera general, el porcentaje de paquetes y cuadros perdidos aumenta conforme aumenta la velocidad de los nodos y la carga en la red.

Los valores medios obtenidos varían en función del escenario y la velocidad simulados (Fig. 13). En el escenario de mayores dimensiones, las distancias que debe recorrer el flujo hasta llegar al destino son mayores, y por tanto la probabilidad de pérdida del cuadro es mayor, ya que hay más paquetes que llegan tarde y se dan por perdidos.

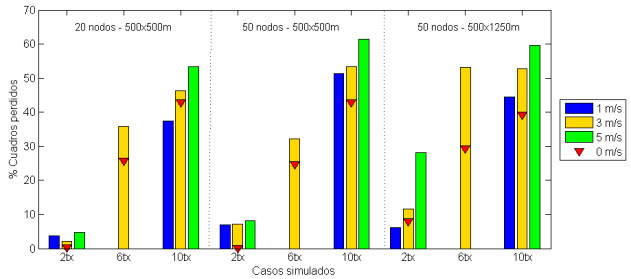


Fig. 13. Pérdidas de cuadros en función de la velocidad de los nodos.

Cabe destacar el elevado porcentaje de cuadros perdidos con la aplicación adaptativa al moverse los nodos. Si bien pareciera que existe una mayor conectividad, es decir mayor número de rutas entre origen y destino que reducirían estas pérdidas, este efecto es compensado por una densidad mayor, lo que provoca un mayor número de colisiones al tratar de acceder al medio compartido.

C. *Calidad subjetiva de vídeo*

El movimiento de los nodos implica un aumento de las pérdidas, por lo que la calidad global percibida se degrada a medida que aumenta la velocidad de los nodos (Fig. 14). Esto se produce principalmente debido a las desconexiones de las sesiones RTP, provocadas por la falta de conectividad entre emisor y receptor, así como por el consiguiente aumento de las pérdidas.

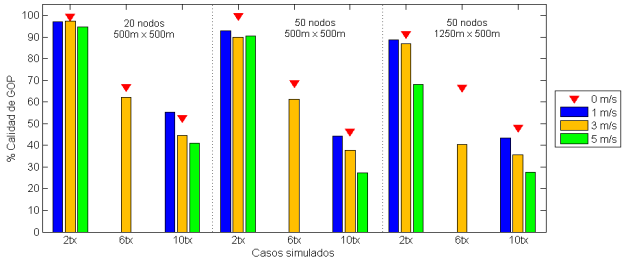


Fig. 14. Calidad del GoP en función de la velocidad de los nodos.

También cabe recordar que a medida que se incrementa la velocidad aumenta la señalización existente en el sistema. Por un lado, la adaptación del intervalo entre paquetes RTCP añade más tráfico al sistema; por otro lado, la movilidad implica tener que buscar más a menudo nuevas rutas alternativas entre emisor y receptor, lo que produce un incremento de la señalización del protocolo de encaminamiento.

VII. Discusión general

En primer lugar, cabe destacar que comparando la aplicación AVISS con la aplicación estándar que transmite sólo cuadros de vídeo de alta calidad, con AVISS se obtiene una mejora de la calidad global del vídeo reproducido en el receptor. Ello se debe a la capacidad de adaptación de la fuente de vídeo diseñada, que envía cuadros de vídeo de dos calidades diferentes (tasas de trasmisión diferentes) según sea el estado de la red a lo largo del tiempo, medido en términos del porcentaje de pérdida de paquetes en la red. Esto puede apreciarse claramente en la Fig. 9, en que se observan mayores pérdidas de paquetes con la aplicación adaptativa que con la aplicación convencional y flujo de baja calidad (LQ), pero menores pérdidas de paquetes que con la aplicación convencional y flujo de alta calidad (HQ). Equivalentemente, la calidad subjetiva percibida por el usuario con la aplicación adaptativa se halla entre las percibidas con la aplicación convencional y un solo tipo de flujo, como muestra la Fig. 11, siendo ligeramente superior a ambos casos para un número alto de comunicaciones simultáneas. Este ligero incremento de la calidad de GoP está asociado a una disminución de los paquetes y de los cuadros perdidos, por lo que estas dos métricas también mejorarán respecto a la emisión en alta calidad. No así el retardo extremo a extremo de los cuadros, representado en la Fig. 7, que por el contrario experimenta un ligero incremento respecto a las dos implementaciones de la aplicación estándar. Esto es debido al tiempo necesario para conmutar entre los flujos de alta y baja calidad. Como ya se ha comentado, este incremento en el retardo se produce por el consumo de recursos del origen y el destino, al incrementarse las tareas que deben realizar estos nodos, específicamente en la gestión de los dos flujos de distintas calidades para ir enviando GoPs de una u otra calidad, así como el hecho de que el control dinámico del flujo RTCP diseñado, introduce un mayor número de paquetes en el sistema. El segundo aspecto a destacar es la disparidad de resultados entre los diferentes escenarios simulados. La bondad de la métrica estudiada en cada caso también depende del resto de variables, es decir, de la velocidad de los nodos, del número de transmisiones y de la aplicación utilizada. Por estas razones no se puede afirmar que exista una red óptima respecto de la evaluación de una métrica o para una velocidad específica de movimiento de los nodos, sino que en función de diversas características pueden esperarse mejores o peores resultados.

Otra característica de gran importancia es el empeoramiento de las medidas cuando se aplica un sustancial grado de movilidad en los nodos que constituyen la red. En estas situaciones la calidad global se degrada, pues aumenta la pérdida de paquetes y, por lo tanto, de cuadros de vídeo, debido a que la movilidad en los nodos produce cambios en la topología de red y enlaces que se rompen. En este estudio se ha comprobado que el comportamiento temporal de las pérdidas, tanto para una carga de tráfico moderada como elevada, es relativamente independiente de otros factores como son la velocidad de los nodos o el número de transmisiones activas. Esta misma tendencia se observa en el retardo extremo a extremo. Ambas métricas tienen una evolución en la que pueden distinguirse tres fases en el escenario analizado en la Fig. 6: incorporación secuencial de nuevas fuentes, mantenimiento del máximo número de fuentes y desconexión progresiva de las comunicaciones. La primera etapa se caracteriza por un fuerte incremento de las pérdidas por cada nueva incorporación al sistema; durante la segunda fase las pérdidas se estabilizan, llegando incluso a decaer ligeramente a partir de un cierto instante que depende de las condiciones del escenario; finalmente, en el intervalo de desconexiones existe también un descenso, sólo que en este caso el decaimiento depende de si en la fase anterior se había producido o no un decremento de las pérdidas. En lo que a pérdidas se refiere, en todos los casos puede distinguirse un fuerte incremento inicial conforme se incorporan nuevas fuentes.

VIII. Conclusiones y Trabajos Futuros

En este trabajo hemos presentado el diseño e implementación de AVISS, una aplicación para la transmisión adaptativa de *streaming* de vídeo en redes MANET que ofrece una mejor Calidad de Experiencia (QoE) al usuario final. La capacidad de adaptación de AVISS está basada en la transmisión de vídeo codificado con diferentes calidades (*multirate*), con lo cual se puede ajustar la tasa de transmisión a las condiciones de operación de la red. A partir de los resultados presentados, los cuales fueron obtenidos mediante la simulación de diversos escenarios de redes móviles ad hoc, podemos concluir que esta implementación de AVISS presenta algunas mejoras respecto de un servicio de *streaming* de vídeo no adaptativo, y supone una mejora en la percepción del vídeo por parte del usuario. No obstante, esto viene asociado a un incremento del retardo extremo a extremo de los cuadros de vídeo.

Para medir la calidad del vídeo se ha definido una métrica llamada Calidad del GoP (QoG) cuyo valor depende de la cantidad y el tipo de los cuadros pertenecientes a un mismo GoP que son recibidos y decodificados en el receptor. Esta métrica es fácil de medir en el destino, no requiere como referencia el vídeo transmitido y está relacionada con la Tasa de Vídeo Decodificado y Reproducible, por lo que es un estimador de la QoE percibida por el usuario.

A lo largo de esta investigación han surgido algunas ideas que podrían ayudar a mejorar los resultados obtenidos. Una primer estudio consistiría en analizar las prestaciones de AVISS en escenarios más densos, en los que se asegure que en todo momento exista conectividad entre el origen y el destino de una comunicación. Igualmente, nos proponemos hacer un análisis de las prestaciones de AVISS utilizando otros protocolos de encaminamiento como DSR [24], así como con otros modelos de movilidad, como el modelo Manhattan o el de Movilidad Grupal hacia Puntos de Referencia (*RPGM, Reference Point Group Mobility*).

Un aspecto que se podría implementar para reducir la pérdida de calidad de los GoPs consiste en proteger los paquetes que transportan datos de los cuadros de vídeo tipo I e incluso P, ya sea mediante un mecanismo de FEC (*Forward Error Correction*) o dándoles un trato diferenciado prioritario en las colas de espera de los nodos. Esto se lograría incluyendo técnicas de gestión de la QoS (*Quality of Service*). Asimismo, podría estudiarse el comportamiento del sistema utilizando el mecanismo RTS/CTS (*Request To Send/Clear To Send*) para reservar el canal de radio al transmitir tramas de datos entre dos nodos.para disminuir el número de colisiones en presencia de nodos concentradores de flujos debido a la topología de la red.

Otro aspecto de estudio es la elección de los umbrales para el cambio del vídeo de una calidad a otra, ya que los umbrales podrían ajustarse de forma dinámica en función del estado de la red. Por último, podría estudiarse la evolución de las diferentes métricas con vídeo codificado a más de dos calidades distintas.

Agradecimientos

Esta investigación ha sido financiada por los proyectos ITACA (TSI2007-65393-C02-02) y CONSEQUENCE (TEC2010-20572-C02-02). Asimismo, G. Díaz-Delgado ha contado con el apoyo de becas de CONACYT, PROMEP-UAQ, México y Fundación Carolina, España. Igualmente, C. Tripp Barba ha contado con la beca FI-Agaur y el programa Doctores Jóvenes en Áreas Estratégicas de la UAS, México. Finalmente, los autores desean agradecer los comentarios de los revisores.

Referencias

[1] J. G. Apostolopoulos, W.-T. Tan, and S. J. Wee, "Video Streaming: Concepts, Algorithms and Systems," Hewlett-Packard Laboratories, September, 2002.

[2] G. Mapp, D. Cottingham, F. Shaikh, P. Vidales, L. Patanapongpibul, J. Balioisian, and J. Crowcroft, "An Architectural Framework for Heterogeneous Networking," WINSYS, August 2006.

[3] S. Corson, and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC2501, January 1999.

[4] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," RFC: 1633, June 1994.

[5] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, December 1998.

[6] S.-B. Lee, G.-S. Ahn, X. Zhang, and A. T. Campbell, "INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks". *Journal of Parallel and Distributed Computing*, Academic Press, Special issue on Wireless and Mobile Computing and Communications, vol. 60, no. 4, pp. 374-406, April 2000.

[7] H. Xiao, W. K. G. Seah, A. Lo, and K. C. Chua, "A Flexible Quality of Service Model for Mobile Ad Hoc Networks," IEEE VTC, May 2000.

[8] G. Díaz Delgado, V. Carrascal Frías, and M. Aguilar Igartua, "Cross-Layer Optimization for Video-streaming Transmission with QoS over Ad hoc Networks: A Holistic Approach," *Journal of Communications Software and Systems*, Special issue on Cross-Layer Design for QoS Support in Wireless and Hybrid Networks, Croatian Communication and Information Society, ISSN 1845-6421, vol. 3, no. 3, September 2007.

[9] Q. Zhang, and Y.-Q. Zhang, "Cross-Layer Design for QoS Support in Multihop Wireless Networks," *Proceedings of the IEEE*, vol. 96, no. 1, pp. 64-76, January 2008.

[10] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS Control of Multimedia Applications based on RTP," *Computer Communicationse*, vol. 19, no. 1, pp. 49-58, January 1996.

[11] M. Postigo-Boix, J. Garcia-Haro, and M. Aguilar-Igartua, "Cost minimization study of semi-elastic flows using Internet," ICC, April-May, 2002.

[12] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," RFC 1889, January 1996.

[13] J. Postel, "User Datagram Protocol, " RFC 768, January 1980.

[14] Moving Picture Experts Group (MPEG), MPEG home page, 2009, [Online]. http://www.chiariglione.org/mpeg/

[15] International Telecommunication Union, "Video Coding for Low Bitrate Communication," ITU-T Recommendation H.263, 1996

[16] Arizona State University, Trace Website, Tools for Research, 2009, [Online]. http://trace.eas.asu.edu/

[17] NCTUns 6.0 Network Simulator and Emulator, 2009, [Online]. http://nsl.csie.nctu.edu.tw/nctuns.html

[18] IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," The Institute of Electrical and Electronics Engineers, Inc. (IEEE), New York, USA, June, 2007.

[19] C. Perkins, E. Belding-Royer, and E. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC3561, July 2003.

[20] University of Bonn, Bonnmotion, 2009, [Online]. http://iv.cs.uni-bonn.de/wg/cs/applications/bonnmotion/

[21] D. C. Montgomery, *Design and Analysis of Experiments*, 6th ed., New York, John Wiley, 2005.

[22] A. Ziviani, B. E. Wolfinger, J. F. Rezende, O. C. M. B. Duarte, and S. Fdida, "Joint Adoption of QoS Schemes for MPEG Streams," *Multimedia Tools and Applications Journal*, Kluwer Academic Publishers, ISSN:1380-7501, vol. 26, no. 1, pp. 59-80, May 2005.

[23] H. Koumaras, A. Kourtis, C.-H. Lin, and C.-K. Shieh, "End-to-End Prediction Model of Video Quality and Decodable Frame Rate for MPEG Broadcasting Services," *International Journal On Advances in Networks and Services*, ISSN:1942-2644, vol. 1 no. 1, pp. 19-29, 2008, [Online]. http://www.iariajournals.org/networks_and_services/

[24] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC4728, February 2007.

Modelado de errores a ráfagas en canales WLAN interiores mediante cadenas de *Markov* ocultas

Juan Ramón Santana, Ramón Agüero, Marta García, Luis Muñoz
Departamento de Ingeniería de Comunicaciones
Universidad de Cantabria
Plaza de la Ciencia s/n, 39005 Santander
{ramon, marta, luis}@tlmat.unican.es

***Resumen*—En este trabajo se analiza el comportamiento de diferentes modelos de canal para reflejar la presencia de ráfagas de errores en entornos de propagación IEEE 802.11 interiores. En particular se centra en las prestaciones que las alternativas basadas en modelos de Markov ocultos pueden aportar, comparándolos con el tradicional Gilber-Elliot y con una propuesta alternativa, que utiliza un filtro AR para establecer cierta memoria en su comportamiento.**

I. Introducción y objetivos

Muchos son los artículos que se encuentran en la literatura que ponen de manifiesto el comportamiento a ráfagas de los canales inalámbricos de interiores en las redes IEEE 802.11, en los que los errores no ocurren de forma independiente, sino que tienden a producirse con una cierta correlación [1], [2], [3], [4], [5], [6]. Por otra parte, se ha observado asimismo que dicho comportamiento depende de la calidad del enlace percibida [7]. Es por ello que se considera necesario desarrollar modelos de canal que reflejen de manera fidedigna el comportamiento de los entornos inalámbricos reales, con un nivel de complejidad que permita integrarlos sin demasiadas dificultades en las arquitecturas de los simuladores más importantes.

Por todo lo anterior, y en base a un conjunto de medidas reales obtenidas sobre un canal IEEE 802.11b en un entorno de oficina, en [8], [9], [10] se propuso el modelo *BEAR* (*Bursty Error Model based on an Auto-Regressive Filter*) que fue integrado en el simulador ns-2 (*Network Simulator*), comparando sus prestaciones con los resultados que se obtienen aplicando otros modelos más tradicionales que el simulador incorpora. Así, el propósito de este trabajo es el de extender dicha comparación a alternativas más complejas como son los modelos ocultos de Markov (*Hidden Markov Models* o *HMM*), basados en cadenas con más de dos estados.

El artículo se ha estructurado como sigue: en la Sección II se revisan brevemente aquellas investigaciones más cercanas a la que se presenta en este artículo; la Sección III introduce las cadenas de Markov ocultas y describe los detalles de la implementación llevada a cabo. Posteriormente, en la Sección IV, se presentan los resultados de aplicar los modelos HMM, comparándolos con los que se obtienen con otros modelos, tales como *Gilbert-Elliot (GE)* o *BEAR*, para finalmente, en la Sección V resumir las aportaciones principales de este trabajo y plantear una serie de futuras líneas.

II. Trabajo relacionado

Los primeros trabajos publicados en esta línea se basan en caracterizaciones realizadas mediante la interfaz inalámbrica WaveLAN de AT&T, anterior a la especificación del estándar IEEE 802.11 en 1997. En este grupo se encuentra la investigación realizada por Eckhardt y Steenkiste [2]. A partir de un conjunto de trazas de paquetes en recepción (incluyendo información acerca del nivel de señal y de ruido y presencia de errores, proporcionada por el controlador inalámbrico), evalúan la influencia de diferentes fuentes de interferencia y atenuación sobre las tasas de pérdida de paquetes y de error de bit observadas en un entorno de propagación en interiores. En particular, se investigan los efectos de la distancia, la presencia de obstáculos y personas en el canal así como las interferencias de banda estrecha en torno a los 900 MHz, generadas por distintas tecnologías de telefonía inalámbrica que operan en dicha frecuencia. En paralelo, Nguyen et al [3], siguiendo una metodología similar a la del trabajo anterior, profundizan en el análisis de las trazas recogidas en una plataforma de medida que emplea también interfaces WaveLAN. Su objetivo era encontrar un modelo realista para emular el comportamiento del canal inalámbrico. A partir de la tasa de error y de las longitudes de las ráfagas, tanto de los paquetes perdidos como de los que se reciben correctamente, proponen un modelo de Markov de dos estados mejorado, en el que sustituyen las distribuciones geométricas para las longitudes de dichas ráfagas por otras que se adaptan con mayor precisión a las observadas experimentalmente. Para validar la propuesta incorporan el modelo en el simulador ns-2 y cuantifican el impacto de los errores sobre el rendimiento del protocolo TCP. Concluyen que la mejora introducida permite que la diferencia entre el throughput simulado y el medido sea inferior a la que se obtiene en el caso de aplicar el modelo de Markov de dos estados tradicional. Sin embargo, los autores no hacen ninguna referencia a la calidad del canal en términos de la SNR recibida y, por tanto, el modelo no incorpora dependencia alguna con la distancia.

Por lo que se refiere a trabajos posteriores que hacen uso de la especificación 802.11b a 11 Mbps, destaca la investigación de Ikkurthy y Labrador [4], en la que analizan el efecto de las perturbaciones que introduce el canal sobre la calidad de una señal de vídeo codificada en MPEG-4. Realizan experimentos con diferentes tamaños de paquete y analizan las ráfagas, en número de paquetes, con o sin error y sus distribuciones de probabilidad correspondientes, para una separación entre los dos dispositivos inalámbricos cercana a 22 m. Comparando dichas distribuciones con las observadas por Nguyen et al a 2 Mbps, llegan a la misma conclusión que éstos en cuanto a que un modelo geométrico simple no refleja, de manera precisa, el comportamiento real observado. También concluyen que,

para paquetes de 1500 bytes, el 90% de las ráfagas de error son iguales o inferiores a cuatro paquetes. Sin embargo, los autores no mencionan el número máximo de retransmisiones MAC que realizan las interfaces 802.11b de la plataforma de medida, de las que tampoco aportan información alguna. De hecho, los autores se refieren a ráfagas de errores cuando, de manera rigurosa, sería más correcto hablar de paquetes perdidos.

Por otra parte, son varios los autores que ponen de manifiesto que modelos tradicionales como el modelo de Gilbert-Elliot no reflejan fielmente el comportamiento de los canales de interiores 802.11 reales. En [5] se demuestra que este modelo no es capaz de capturar periodos de alta tasa de pérdida de paquetes, de vital importancia en la transmisión de vídeo, tanto en lo que se refiere a la calidad percibida por el usuario como al diseño de métodos de control de errores. En [6] utilizan el GE para encontrar los parámetros de calidad percibida en la transmisión de voz que tratan de mejorar a través de un esquema FEC adaptativo, planteando la necesidad de extender sus investigaciones a modelos de canal más realistas.

Recientemente, los autores de [11] se apoyan en los resultados obtenidos en una campaña experimental llevada a cabo en un escenario rural de exteriores para derivar un modelo que refleje la tasa de error de trama observada y manifiestan la necesidad de llevar a cabo estudios similares en entornos de interiores. Finalmente, Cardoso y Ferreira [12] cuestionan de nuevo la exactitud del modelo de Markov de dos estados a la hora de mimetizar las pérdidas de paquetes que se observa en un canal 802.11 de interiores real. Por este motivo proponen y evalúan un nuevo modelo basado también en cadenas HMM. Los resultados que obtienen son comparados con un conjunto de trazas recogidas en una serie de experimentos realizados a una velocidad fija de 11 Mbps, sin realizar retransmisiones MAC al utilizar direccionamiento multicast. Sin embargo, en la generación del tráfico introducen un tiempo entre paquetes de 10 ms, demasiado elevado respecto del tiempo de transmisión de las tramas. Por otra parte, aunque no aportan información relativa a la distancia entre los dispositivos que conforman el testbed o la SNR recibida, los valores de FER y longitudes de las ráfagas que obtienen son sensiblemente inferiores a los que se tratan de modelar en este artículo. A pesar de ello, encuentran que un modelo HMM de 11 estados con una estructura de nacimiento y muerte describe con bastante fidelidad las estadísticas de primer y segundo orden del proceso de pérdida de paquetes.

III. Modelo de canal basado en HMM

Las cadenas de *Markov* ocultas son un modelo matemático no determinista, cuyas variables de caracterización, ya sea las referentes a la transición entre estados o decisión, responden a un proceso estocástico.

Para describir el modelo se debe considerar un sistema de N estados independientes, representados de ahora en adelante por S_i, donde i es el índice del estado referenciado. La transición entre los diferentes estados (que están relacionados entre sí) se lleva a cabo mediante un conjunto de probabilidades estocásticas. Esta probabilidades, llamadas de transición, son representadas por $a_{i,j}$, donde i, j se corresponden, respectivamente, con los estados origen y destino, y representan la probabilidad de cambio entre el estado actual y el siguiente estado (es también posible considerar el suceso de permanencia en un mismo estado). El otro conjunto de probabilidades que se necesitan para definir una cadena de *Markov* son las llamadas de decisión. Están asociadas a cada estado y representan la probabilidad de decisión de cada valor salida del sistema; cada uno de estos valores está definido por $b_i(k)$, donde i es el estado al que está asociada la probabilidad y k el símbolo correspondiente. Destacar que, a diferencia de las cadenas de *Markov*, los valores se encuentran *'ocultos'*, ya que cada estado no se corresponde unívocamente con un valor concreto, sino que existen varias posibilidades. Finalmente, para determinar completamente el sistema es necesario definir también los valores de la distribución inicial de probabilidades de estar en cada estado, π_i, donde i corresponde al índice de cada uno de los estados de la cadena.

Teniendo en cuenta todos los elementos anteriores, se puede definir una cadena de *Markov* oculta mediante los siguientes elementos:

- El número de estados en el modelo, N.
- El número de símbolos observables, M.
- La matriz $\mathbf{A}$ de transición, de dimensión $N \times N$, con todas las probabilidades posibles $a_{i,j}$.
- La matriz $\mathbf{B}$ de decisión (dimensión $N \times M$, con todas las combinaciones posibles $b_i(k)$.
- La distribución inicial de probabilidades de estar en cada estado $\Pi = \{\pi_i\}$.

En [13] se describen tres problemas clásicos que afectan a las *HMM*, a saber: (1) determinar la probabilidad de obtención de una secuencia de observables dados, a partir de un modelo también conocido; (2) establecer la secuencia de estados más probable en función de una secuencia de resultados y el modelo; (3) a partir de una secuencia de resultados, determinar los parámetros del modelo.

De los tres problemas anteriores el que mayor dificultad conlleva es, sin ninguna duda, el tercero. Sin embargo, para acometer el diseño del modelo de canal, en este trabajo se parte de un conjunto de trazas reales (secuencia de resultados observables del sistema), en las que cada elemento binario se corresponde con la recepción de una trama correcta o incorrecta. A partir de dichas trazas se deberá encontrar los parámetros del modelo más probable. Para su resolución se emplea el algoritmo iterativo de *Baum-Welch*, que ofrece una eficiencia razonable. Más concretamente, se ha empleado la implementación que ofrece *Matlab*, a través de la función `hmmtrain`, limitando el número de iteraciones a 1000.

Una de las características que, en mayor medida, presenta el canal real que se trata de *emular* a partir del *HMM* es su gran variabilidad, fruto de la cual se produce un amplio rango de comportamientos, desde situaciones en las que las prestaciones son muy negativas hasta otras en las que se acercan a las que se producirían en un canal libre de errores [8], [9]. Evidentemente los parámetros del modelo *HMM* correspondiente dependen fuertemente de las trazas reales utilizadas para su *'entrenamiento'*, por lo que habrá que seleccionar un conjunto de medidas. En particular se han seleccionado 4 medidas concretas, como ejemplos canónicos de un comportamiento malo (*Bad*), bueno (*Good*) y medio (*Avg-1* y *Avg-2*).

Por otro lado, es necesario establecer una serie de características en lo que concierne al modelo *HMM* antes de determinar sus parámetros, principalmente en lo que se refiere al número de estados. También es necesario determinar alguna restricción más, como limitar las transiciones entre estados adyacentes, o establecer que el resultado de algún estado en concreto siempre sea el mismo. Con el objetivo de cubrir convenientemente varias posibilidades se hicieron pruebas con un conjunto relativamente extenso de posibles configuraciones, tal y como se menciona a continuación. En todos los casos se asume que el estado 0 se corresponde con el peor y el $N-1$ (siendo N el número total de estados) con el que refleja una situación menos hostil del canal. Además se supone que un 1 a la salida del modelo implica una trama correcta, mientras que el 0 se corresponde con una situación de error.

- Modelo de 3 estados
  1) Libertad total.
  2) Modelo de nacimiento y muerte, con $a_{i,j} = a_{j,i} = 0$ para $(i,j) = (0,2)$.
  3) Limitación de la decisión siendo $b_0(1) = b_2(0) = 0$.
  4) Combinación de las dos restricciones anteriores.
- Modelo de 4 estados
  1) Libertad total.
  2) Restringiendo las probabilidades de transición entre los estados 0 y 3, $a(0,3) = a(3,0) = 0$.
  3) Modelo de nacimiento y muerte.
  4) Limitación de la decisión, siendo $b_0(1) = b_3(0) = 0$.
  5) Combinación de (2) y (4).
  6) Combinación de (3) y (4).
- Modelos de 8 y 16 estados
  1) Proceso de nacimiento y muerte.

En el caso de los modelos con más estados, se limitó notablemente la complejidad del modelo, ya que se comprobó que, en caso contrario, el algoritmo *Baum-Welch* no convergía adecuadamente.

La implementación del modelo *HMM* se ha llevado a cabo en el marco del simulador *Network Simulator*; se utilizan, como entradas para configurarlo, sendos ficheros en los que se establecen las matrices $\mathbf{A}$ y $\mathbf{B}$, con lo que otorga al modelo de una gran flexibilidad. El modelo, además, permite ser configurado, tanto a nivel de tramas como temporal; este es un aspecto fundamental, ya que en muchos trabajos en la literatura, al emplear modelos de canal basados en cadenas de *Markov* asumen incorrectamente que utilizar una frecuencia de emisión constante en la fuente es correcto; hay que tener en cuenta que la generación de información dependerá fuertemente de varios factores: modelo de tráfico (servicio empleado), carga en el canal inalámbrico, etc; por ejemplo, al utilizar aplicaciones basadas en TCP es muy posible que se produzcan periodos de inactividad relevantes, lo que invalida una configuración basada en tramas.

A la hora de configurar correctamente el modelo es necesario establecer la *función densidad de probabilidad* de permanencia en un estado. Es bien sabido que dicha *fdp* es exponencial negativa, $f_{T_i}(t_i) = \lambda e^{-\lambda \cdot t_i}$, donde $\overline{t_i} = \frac{1}{\lambda}$, es el tiempo medio de permanencia en el estado i. Para estimar $\overline{t_i}$, se calcula el número medio de tramas consecutivas para cada estado según se indica en 1, valor que se multiplica por el tiempo de transmisión medio por trama.

$$\text{Número medio tramas consecutivas estado } i = \overline{N_i} = \\ = \sum_{i=1}^{\infty} n p_i(n) = \sum_{i=1}^{\infty} n a_{i,i}^{n-1}(1 - a_{i,i}) = \frac{1}{1 - a_{i,i}} \quad (1)$$

Así, se garantiza la validez del modelo, independientemente de los modelos de tráfico y del tipo de protocolo de transporte empleado.

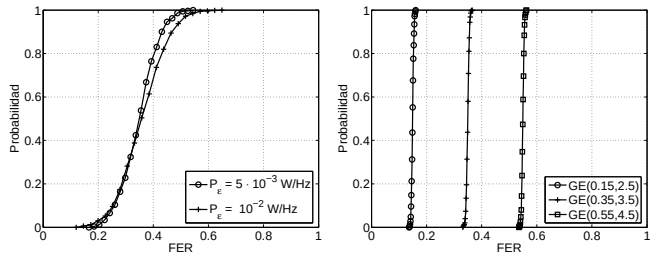
IV. Resultados

En esta sección se presentan los resultados obtenidos con los diferentes modelos de canal que se han mencionado anteriormente. Se utilizarán varias configuraciones de *BEAR*, *Gilbert-Elliot* y *HMM*, presentando asimismo los valores que se recogieron en el canal real. Para cada uno de los modelos de canal analizados se ha seguido el mismo procedimiento: se llevan a cabo 500 experimentos independientes, enviando, en cada uno de ellos, 20000 datagramas UDP entre el transmisor y el receptor y garantizando, en cualquier caso, que siempre haya paquetes esperando a ser transmitidos (saturación del canal).

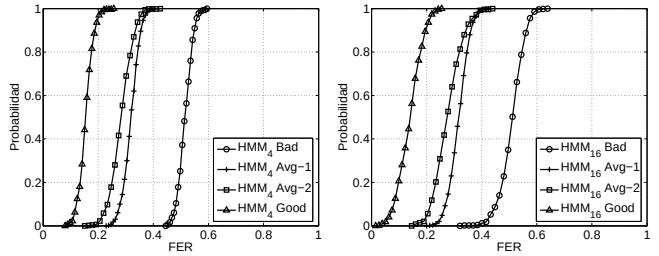
Con el objetivo de caracterizar y comparar todos los modelos de canal se utilizarán un número de métricas, que se presentan a continuación.

- *Frame Error Rate (FER).* Relación entre las tramas que llegan con error al receptor y el total de tramas recibidas.
- *Packet Error Rate (PER).* En la tecnología IEEE 802.11b se establece un mecanismo de retransmisión, mediante el cual una trama puede retransmitirse un número determinado de veces (3 en las interfaces empleadas en este trabajo) antes de darse por perdida, por lo que la tasa de pérdida de los datagramas IP no coincide con la FER.
- *Erroneous Frame Burst (EFB).* Las ráfagas de errores son una de las principales causas del deterioro que los protocolos de capas superiores (TCP y UDP) sufren sobre canales IEEE 802.11 en interiores; en este sentido se estudiarán las ráfagas, en términos de longitudes media y máxima, considerando como longitud mínima de ráfaga una trama errónea. Asimismo se presentarán las funciones de distribución de las ráfagas en medidas individuales, así como la función de autocorrelación de tramas erróneas.

De las diferentes configuraciones del modelo HMM que se han empleado, se utilizarán únicamente las de 4 y 16 estados, utilizando, en el segundo caso, una cadena de *nacimiento y muerte*, mientras que para HMM_4 se optó por emplear la configuración con mayor grado de libertad. Sin embargo, se ha comprobado que, para pocos estados, no hay una diferencia sustancial entre permitir transiciones entre cualquier pareja de estados y limitar el modelo para que sea de nacimiento y muerte. Por otro lado se ha optado por mostrar los resultados del modelo de 4 estados (similares a los obtenidos con 3) y los de 16, que ofrece algo más de variabilidad que la cadena con 8 estados. Como se ha comentado en la Sección III, se utilizaron cuatro comportamientos reales para entrenar las cadenas correspondientes. La Tabla I muestra el comportamiento

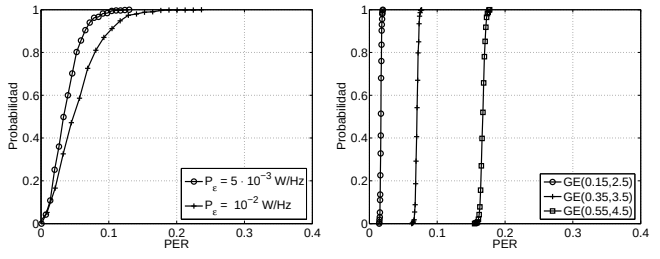


(a) Canal BEAR (b) Canal GE

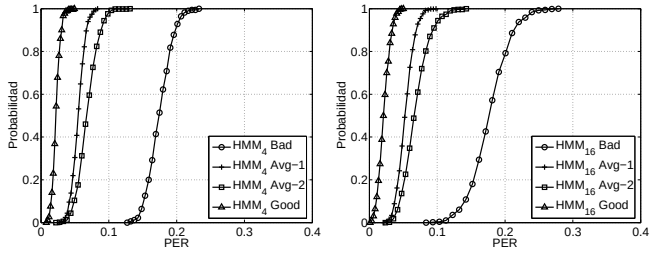


(c) Canal HMM_4 (d) Canal HMM_{16}

Fig. 1. Función de distribución de la FER para los diferentes modelos de canal



(a) Canal BEAR (b) Canal GE



(c) Canal HMM_4 (d) Canal HMM_{16}

Fig. 2. Función de distribución de la PER para los diferentes modelos de canal

que se observó en estas cuatro situaciones particulares. Por su parte, para el modelo *BEAR* se utilizarán dos potencias para el ruido blanco gaussiano de entrada al filtro AR: 10^{-2} y $5 \cdot 10^{-3}$ W/Hz; siendo este último el que se utilizó en [8], [9], [10], mientras que con el primero se pretende conseguir una mayor memoria en el canal. En lo que se refiere al canal *Gilbert-Elliot* se emplearán tres configuraciones, que reflejan situaciones similares a las utilizadas para entrenar al HMM.

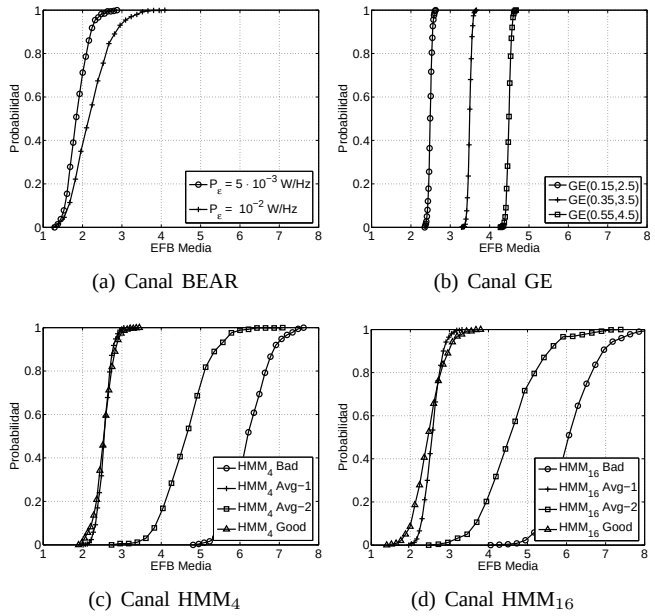
En primer lugar, la Figura 1 muestra las funciones de distribución que se obtuvieron para la FER en los cuatro modelos de canal que se están analizando. Como se puede ver, se pone de manifiesto que, en lo que se refiere a la FER, la configuración del modelo *BEAR* no tiene una relevancia notable, ya que el comportamiento es similar para los dos valores de potencia empleados; en ambos casos se comprueba que el rango de valores observado es muy elevado, variando desde 0.15 hasta 0.65 en un caso y desde < 0.2 a 0.55 en el otro. El canal *GE* ofrece un comportamiento claramente predecible, pues mantiene la FER muy constante en torno al valor empleado para su configuración. En cuanto al modelo HMM, las gráficas permiten establecer diversas conclusiones: en primer lugar, incrementar el número de estados otorga mayor variabilidad al modelo; además, las trazas empleadas para *entrenar* la cadena de *Markov* son las que determinan el comportamiento de éste; así, se observa una mayor varianza en la FER caracterizada a partir de las medidas *Bad* y *Avg-2*.

En lo que se refiere a la PER (ver Figura 2) se constata que, en esta ocasión, la configuración de *BEAR* sí que influye claramente en su comportamiento, ya que se ve que cuando se utiliza 10^{-2} como valor de la potencia de entrada al filtro AR se observan valores de PER sensiblemente mayores que con la otra configuración (a pesar de la FER era similar); se desprende, por tanto, que dicho parámetro de configuración tiene una influencia directa sobre la memoria del canal. Para el canal *GE*, se vuelve a observar un comportamiento muy predecible en torno a un valor concreto. Sin embargo, los modelos HMM consiguen una variabilidad notable, especialmente para las configuraciones más pesimistas (*Bad*); además, la variabilidad en torno al valor medio depende claramente del número de estados, como queda de manifiesto al comparar los resultados obtenidos para los modelos HMM_4 y HMM_{16}. Sin embargo, a pesar de que se logran valores elevados de PER, ninguna de las configuraciones consigue reflejar un comportamiento tan variable como el de *BEAR*, que logra emular situaciones de baja (alrededor del 1%) y elevada (mayor del 20%) PER para una única configuración.

De alguna manera, el comportamiento de los diferentes modelos de canal en cuanto a la FER y a la PER debería tener una relación directa con lo que sucede en términos de las ráfagas. Para corroborar este punto, la Figura 3 muestra la longitud media de las EFB que se observaron para los cuatro modelos de canal. El modelo *BEAR* de nuevo es capaz de reflejar (para una única configuración) un rango amplio de comportamientos, volviéndose a poner de manifiesto que la potencia de la señal de entrada al filtro AR permite determinar la memoria (*variabilidad*) del modelo. De nuevo *GE* es el que peores prestaciones ofrece, ya que su comportamiento se sitúa, de manera completamente predecible, en torno al valor utilizado para su configuración. En el caso de los canales *HMM*, vuelve a manifestarse una variabilidad mayor para las configuraciones *Bad* y *Avg-2*, así como una dependencia de la varianza observada frente al número de estados empleados. En este caso, se puede ver que con la configuración más pesimista de *HMM* se pueden lograr valores de longitudes media de

Tabla I
MEDIDAS, OBTENIDAS EN UN CANAL INALÁMBRICO REAL, UTILIZADAS PARA ENTRENAR EL MODELO *HMM*

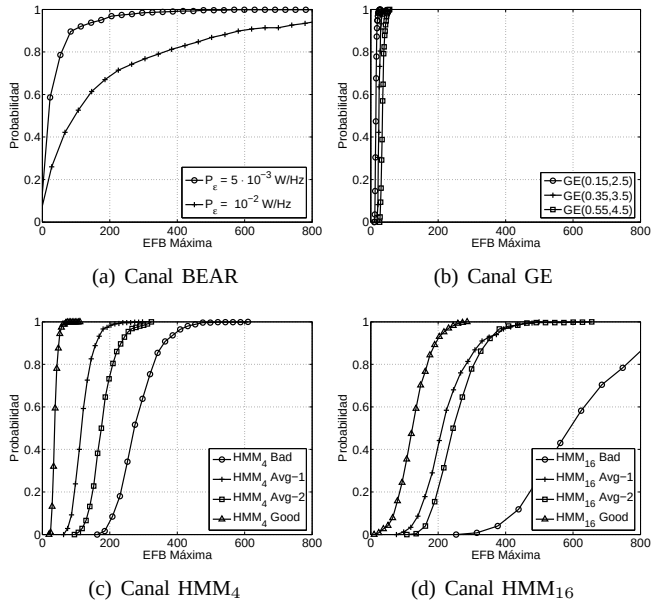
Canal	**FER**	**PER**	**Tput**	**EFB**		
			Mbps	**Avg**	**Var**	**Max**
Bad	0.517	0.179	2.33	6.22	983.66	821
Avg-1	0.331	0.058	3.58	2.60	79.53	258
Avg-2	0.298	0.127	3.80	4.84	301.49	219
Good	0.163	0.025	4.79	2.63	57.63	144



(a) Canal BEAR (b) Canal GE

(c) Canal HMM_4 (d) Canal HMM_{16}

Fig. 3. Función de distribución de la EFB media para los diferentes modelos de canal



(a) Canal BEAR (b) Canal GE

(c) Canal HMM_4 (d) Canal HMM_{16}

Fig. 4. Función de distribución de la EFB máxima para los diferentes modelos de canal

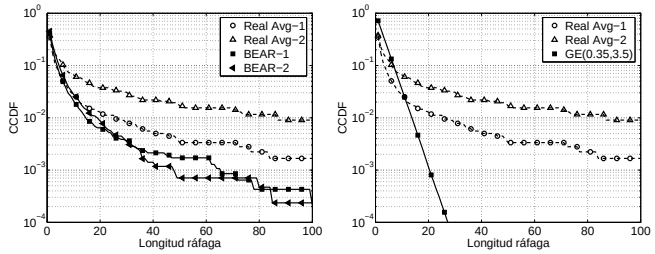
ráfagas notablemente mayores que con los otros modelos, aunque es esas circunstancias, el rango de valores obtenidos se aleja claramente del observado sobre un canal real; además, para valores de PER comparables a los obtenidos con *BEAR* (si se toma, por ejemplo, la configuración *Avg-2*), la EFB media es sensiblemente mayor (llega a valores superiores a 7, mientras que en *BEAR* apenas supera las 4 tramas.

Con el fin de analizar completamente el comportamiento en cuanto a la longitud de las ráfagas de tramas erróneas, la Figura 4 muestra las funciones de distribución obtenidas para la EFB máxima de los cuatro modelos de canal estudiados. En este caso, la ventaja de *BEAR* frente a *HMM* se puede ver de manera mucho más clara. En el comportamiento observado empíricamente, la ocurrencia de una ráfaga larga se puede considerar como un hecho más o menos aislado (la probabilidad de que haya más de 100 tramas erróneas es inferior al 0.7% [10]); como se puede comprobar, el canal *BEAR*, especialmente en la configuración que usa un ruido de potencia 10^{-2} como entrada al filtro AR, se observan ráfagas de tamaño considerable (incluso de más de 1200 tramas); estos valores también se han medido utilizando el canal *HMM*, pero con la diferencia de que la EFB media era mucho mayor en este caso que al utilizar *BEAR*; se puede concluir, por tanto, que *HMM* permite emular canales en los que la presencia de errores a ráfagas es mucho más constante. Por su parte, al utilizar cualquiera de las configuraciones del canal *GE*, se obtienen longitudes de ráfaga máxima mucho menores que con el resto de alternativas, además de ser muy predecibles, por lo que se puede concluir que su comportamiento está bastante alejado de la realidad.

El análisis llevado a cabo hasta el momento pone de manifiesto que las mayores diferencias se limitan a la variabilidad del comportamiento observado, por una parte, y a la estadística en lo que se refiere a la ocurrencia de ráfagas. Con objeto de estudiar con mayor nivel de detalle este último punto, se analizarán dos aspectos adicionales: por un lado la distribución de la longitud del tamaño de las ráfagas observadas para los diferentes modelos de canal y, por otro, la autocorrelación de medidas obtenidas con cada uno de los modelos, como otra manera de analizar la memoria que cada una de las alternativas puede aportar.

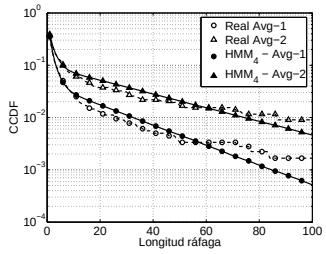
En primer lugar, la Figura 5 muestra las funciones de distribución acumulada complementaria (*ccdf*) de las longitudes de ráfagas para los cuatro modelos de canal analizados. Se representan únicamente las dos situaciones que se han venido considerando como comportamiento medio del canal real, esto es *Avg-1* y *Avg-2*. En el caso de *BEAR*, teniendo en cuenta la gran variabilidad que lo caracteriza, se han empleado dos medidas cualesquiera, cuyos resultados se acercaran a dicho comportamiento medio: FER en torno al 30% y PER cercana al 5%, para las dos configuraciones que se están estudiando a lo largo del artículo. En los otros tres modelos, se han procesado el conjunto de 500 medidas, dado que su comportamiento se ha visto que es notablemente más predecible. Hay dos conclusiones que llaman la atención a primera vista; en primer lugar, se vuelve a demostrar que las prestaciones del modelo de *Gilbert-Elliot* son bastante negativas, ya que la estadística de las ráfagas decrece rápidamente; además, se ve que el modelo *HMM* es capaz de reproducir, de manera fidedigna, el comportamiento observado sobre el canal real; además se comprueba que el hecho de incrementar la complejidad de la cadena subyacente (empleando 16 estados) incrementa, de manera apreciable, la precisión del modelo. En el caso del *BEAR* se ve que no consigue reflejar la estadística de longitudes de ráfagas para valores mayores de 20; hay que tener en cuenta, sin embargo, que la mayoría de ráfagas (aproximadamente el 99% tienen longitudes por debajo de este valor).

Otro parámetro que puede servir como indicador de la memoria de los diferentes modelos de canal es la autocorrelación del proceso de errores (a nivel de trama). Otros autores, por ejemplo Cardoso [12], ya han empleado este parámetro. La Figura 6 muestra las funciones de autocorrelación de

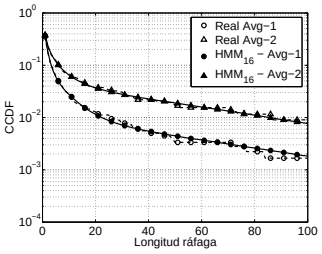


(a) Modelo BEAR

(b) Modelo GE(0.35,3.5)



(c) Modelo HMM_4



(d) Modelo HMM_{16}

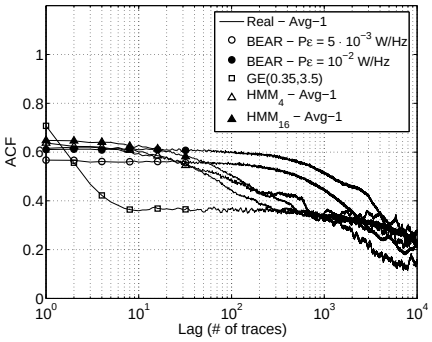
Fig. 5. Funciones de distribución complementarias de las longitudes de ráfagas para los cuatro modelos de canal

varias medidas concretas, obtenidas con todos los modelos, y comparándolas con las correspondientes a las instancias del canal real *Avg-1* y *Avg-2*. En primer lugar se vuelve a demostrar que el canal *Gilbert-Elliot* presenta un comportamiento muy diferente al que se observa empíricamente, siendo de nuevo el modelo *HMM* el que mejor refleja el comportamiento real; aunque es importante destacar el hecho de que las cadenas de *Markov* subyacentes se han *'entrenado'* con las trazas reales, por lo que es lógico que sus prestaciones se acerquen a éstas. También es importante destacar en este caso es que el modelo *BEAR* sí que refleja adecuadamente el comportamiento del canal *Avg-1* (se verá posteriormente que se trata de un ejemplo más ilustrativo de las prestaciones *medias* del canal), aunque no es capaz de replicar de manera tan precisa la autocorrelación obtenida para *Avg-2*.

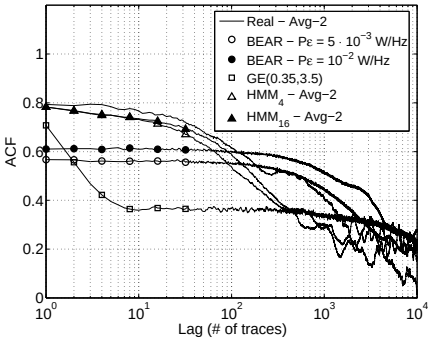
Para finalizar con el estudio que se ha llevado a cabo se analizará a continuación la relación entre la FER y la PER, que también es un indicativo claro de la memoria que presenta un canal en particular. Así, si se asume que no hay ninguna memoria (esto es, que los errores en las tramas ocurren de manera completamente independiente), se podría asegurar que la $PER = FER^4$, ya que para que se pierda un datagrama IP es necesario que haya cuatro tramas erróneas de manera consecutiva. En general se podría asegurar que la PER se puede calcular a partir de la FER, a través del exponente γ:

$$\mathrm{PER} = \mathrm{FER}^{\gamma} \tag{2}$$

en donde γ da idea de la memoria del canal. La Figura 7 permite comparar los valores observados sobre un canal real (30 puntos) frente a los obtenidos con todos los modelos que se están analizando, además de incluir la gráfica que representaría el canal sin memoria. Para obtener cada una de las curvas de los diferentes modelos se ha calculado el parámetro γ que mejor ajusta el comportamiento de las 500 simulaciones que se disponen para cada modelo de canal en particular. Una primera conclusión importante es que el modelo *BEAR*



(a) Canal *Avg-1*

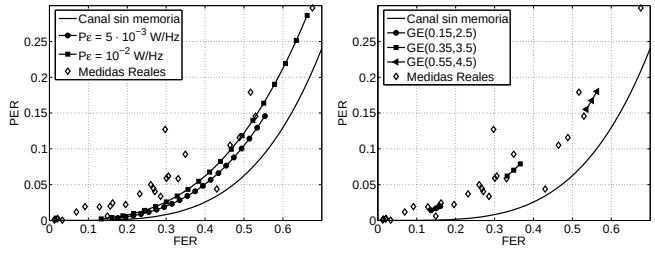


(b) Canal *Avg-2*

Fig. 6. Funciones de autocorrelación para los diferentes modelos de canal

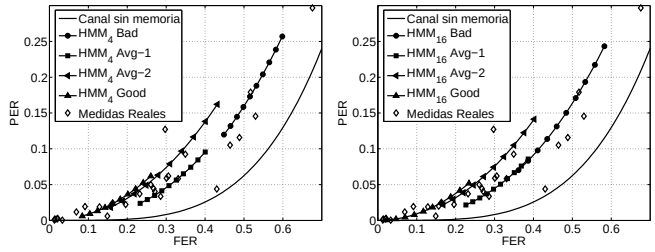
vuelve a ser el que mayor variabilidad presenta, ya que cubre prácticamente todos los valores de FER posibles para una única combinación (notar que para lograr el mismo rango en *HMM* se necesitan unir las cuatro configuraciones que se han empleado). Sin embargo, en el entorno en el que se sitúan la mayoría de los comportamientos reales, se ve que *BEAR* no ofrece el mismo comportamiento que el resto de alternativas analizadas; en este punto hay que destacar claramente las prestaciones de los modelos de canal *HMM*, que vuelven a reflejar de manera muy fidedigna el comportamiento empírico. Hay que tener en cuenta, sin embargo, que estos resultados no tienen porqué ser determinantes de la idoniedad de un modelo u otro (se puede ver, por ejemplo, que *GE* es capaz de acercarse más al canal real que *BEAR*, cuando ya ha quedado claro que las prestaciones de la cadena de *Markov* de dos estados son claramente inferiores a las del resto de modelos).

Una de las posibles razones que pueden explicar la diferencia entre los valores obtenidos con *BEAR* y los observados empíricamente es que la variabilidad que se observa con este modelo de canal tenga como consecuencia que la estimación del parámetro γ no sea muy apropiada. Para corroborar este punto, la Figura 8 muestra el conjunto de puntos que se obtuvieron con *BEAR*, comparándolo con los que se observaron al utilizar las dos configuraciones *medias* del canal HMM_4. Se ve claramente que *BEAR* tiene una variabilidad bastante mayor, fruto de la cual puede aproximarse (en diferentes instancias) al comportamiento empírico (a pesar de que en la figura anterior se pudiera desprender una conclusión diferente). Por su parte, las dos configuraciones *HMM* analizadas permiten reflejar el comportamiento real, aunque debido a su escasa variabilidad, no logran capturar situaciones que se sitúen lejos del que se podría considerar como comportamiento *promedio*.



(a) Canal BEAR

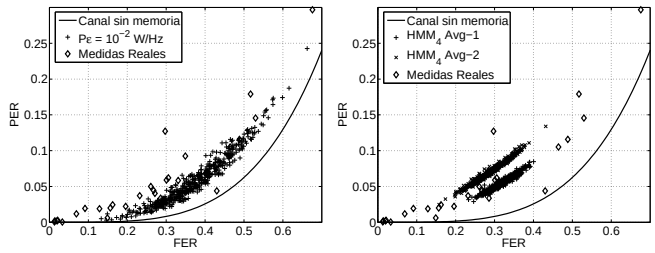
(b) Canal GE



(c) Canal HMM_4

(d) Canal HMM_{16}

Fig. 7. Relación entre la PER y la FER para los diferentes modelos de canal



(a) Canal BEAR

(b) Canal HMM_4

Fig. 8. Relación entre la PER y la FER para todas las repeticiones llevadas a cabo

V. Conclusiones

En este artículo se propone la utilización de cadenas de Markov ocultas para modelar el comportamiento de un canal 802.11b caracterizado empíricamente en términos de estadísticas de errores a nivel de trama. Dichas cadenas han sido implementadas en el simulador ns-2 para diferentes configuraciones y número de estados, siendo entrenadas mediante las propias trazas obtenidas en la campaña de medidas. De los resultados obtenidos en las simulaciones se observa que incrementar el número de estados otorga mayor variabilidad al modelo, lo que se aproxima con mayor exactitud al comportamiento real del canal. Por otra parte, las trazas empleadas para entrenar la cadena son las que finalmente determinan el comportamiento del canal simulado. Dichos resultados han sido comparados, asimismo, con los del modelo GE y con los que proporciona el modelo BEAR para dos configuraciones distintas correspondientes a dos valores de potencia de señal de entrada al filtro AR. Se observa que éste último es capaz de reflejar (para una única configuración) un amplio rango de comportamientos, lo que las cadenas HMM no consiguen en ninguna de sus configuraciones.

Por otro lado, se comprueba que las prestaciones de los modelos *HMM* son muy superiores a las del tradicional *Gilbert-Elliot* (que sigue siendo ampliamente utilizado por la comunidad científica) y que, además, en determinadas situaciones puede proporcionar un comportamiento más acorde con la realidad que *BEAR*. Hay que tener en cuenta, sin embargo, que uno de los principales valores añadidos de este último es que su funcionamiento depende de la calidad del canal (en términos de la SNR), lo que le otorga una capacidad muy interesante.

Como posibles líneas futuras de trabajo se tratarán de comparar las prestaciones de los modelos *HMM* con otras alternativas (especialmente *BEAR*) al emplear otro tipo de modelos de tráfico, prestando especial atención al posible efecto sobre las prestaciones del protocolo de transporte TCP.

Agradecimientos

Los autores querrían expresar su agradecimiento al Gobierno de España por su financiación en los siguientes proyectos: Mobilia - Programa CELTIC (Avanza I+D TSI-020400-2008-82) y “Comunicaciones Cognitivas y Cooperativas sobre Entornos Heterogéneos”, C3SEM (TEC2009-14598-C02-01)

Referencias

[1] H. Bai, M. Atiquzzaman. ‘Error Modeling Schemes for Fading Channels in Wireless Communications: A Survey’, IEEE Communications Surveys and Tutorials vol. 5, no. 2, págs 2-9, 4th Quarter 2003

[2] D. Eckhardt, P. Steenkiste, ‘Measurement and analysis of the error characteristics of an in-building wireless network’, Proceedings of the SIGCOMM Symposium on Communications Architectures and Protocols, págs 243–254, Stanford, agosto 1996

[3] G.T. Nguyen, B. Noble, R.H. Katz, M. Satyanarayanan, ‘A Trace-based Approach for Modeling Wireless Channel Behavior,’ Proceedings of Winter Simulation Conference, págs 597-604, 1996

[4] P. Ikkurthy, M.A. Labrador, ‘Characterization of MPEG-4 Traffic over IEEE 802.11b Wireless LANs’, Proceedings of the 27th Annual IEEE Conference on Local Computer Networks, LCN 2002, noviembre 2002

[5] G. Convertino, S. Oliva, F. Sigona, L. Anchora, ‘An Adaptive FEC Scheme to Reduce Bursty Losses in a 802.11 Network,’ IEEE Global Telecommunications Conference, GLOBECOM 06, noviembre 2006

[6] V.R. Gandikota, B.R. Tamma, C. Murthy, ‘Adaptive FEC-Based Packet Loss Resilience Scheme for Supporting Voice Communication over Ad hoc Wireless Networks,’ IEEE Transactions on Mobile Computing, vol.7, no.10, págs 1184-1199, octubre 2008

[7] A. Vlavianos, L.K. Law, I. Broustis, S.V. Krishnamurthy, M. Faloutsos, ‘Assessing link quality in IEEE 802.11 Wireless Networks: Which is the right metric?’, IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2008, 15-18 septiembre 2008

[8] R. Agüero, M. García, L. Muñoz, ‘Modelado de errores a ráfagas en canales inalámbricos mediante filtrado AR’, VI Jornadas de Ingeniería Telemática, (JITEL 07), págs 329-336, Málaga, septiembre 2007

[9] R. Agüero, M. García, L. Muñoz, ‘Simulación realista del comportamiento de TCP sobre canales con errores y memoria’, VII Jornadas de Ingeniería Telemática (JITEL 08), págs 33-40, Alcalá de Henares, septiembre 2008

[10] R. Agüero, M. García, L. Muñoz, ‘Accurate simulation of 802.11 indoor links: A ’bursty’ channel model based on real measurements’, EURASIP Journal on Wireless Communications and Networking, Special Issue ”Simulators and Experimental Testbeds Design and Development for Wireless Networks”, doi:10.1155/2010/380410, 2010

[11] P. Barsocchi, G. Oligeri, F. Potortì, ‘Measurement-based frame error model for simulating outdoor Wi-Fi networks’, IEEE Transactions on Wireless Communications, vol. 8, nº 3, págs 1154-1158, marzo 2009

[12] K.V. Cardoso, J. F. De Rezende, ‘Accurate hidden markov modeling of packet losses in indoor 802.11 networks,’ IEEE Communications Letters, vol.13, no.6, págs 417-419, junio 2009

[13] Lawrence R. Rabiner. ‘A tutorial on Hidden Markov Models and selected applications in speech recognition’, Proceedings of the IEEE 77 (2), págs 257-286, febrero 1998

Impacto del modelo de error en distancia en la simulación de sistemas de localización

Salvador Guardiola, Israel Martin-Escalona, Francisco Barcelo-Arroyo, Marc Ciurana
Departamento de Ingeniería Telemática
Universidad Politècnica de Catalunya (UPC)
c/ Jordi Girona 1-3, Edificio C3
imartin@entel.upc.es

Resumen- **Las redes inalámbricas han favorecido enormemente el interés de los usuarios, proveedores de servicio y operadores de red en el posicionamiento geográfico. Como consecuencia, se han propuesto mecanismos en la mayor parte de tecnologías de red inalámbrica con los que soportar la localización de usuarios. La evaluación de calidad ofrecida por dichas técnicas de localización, normalmente en términos de precisión, latencia y escalabilidad, recae en herramientas de simulación. Es esencial por tanto, que los modelos de error empleados en estas herramientas estén acordes a la realidad. Este hecho es si cabe más importante en el caso de emplear técnicas de localización basadas en medida de la distancia a partir de métricas temporales, como son el tiempo de llegada (TOA) o la diferencia entre tiempos de llegada (TDOA). Estas técnicas son especialmente sensibles a no disponer de visión directa entre los distintos elementos involucrados en la localización, por lo que la evaluación de sus capacidades suele hacerse bajo esas condiciones. El presente artículo compara bajo un mismo escenario, diversos modelos de error para las métricas empleadas en técnicas como TOA o TDOA. Los resultados concluyen que los modelos que no tienen en cuenta las distancias reales (que son los más habituales) tienden a proporcionar una estimación optimista el error de posicionamiento, cosa que no ocurre en el caso de modelos más complejos que sí tienen en cuenta esa información.**

Palabras Clave- **error en medidas de distancia, TOA, TDOA, NLOS, posicionamiento en interiores.**

I. INTRODUCCIÓN

Las redes móviles ad-hoc (MANETs) han concentrado gran parte del interés reciente por parte de la industria, principalmente debido a las grandes capacidades que ofrecen en cuanto a dinamismo y autoconfiguración. Su condición de móviles hace que este tipo de redes represente un reto en cuanto diseño y planificación, ya que los distintos protocolos deben tener en cuenta que los nodos que forman parte de la red pueden cambiar su posición y añadirse o abandonar de forma súbita la red. Debido a esto múltiples esfuerzos han sido dedicados a dotar de capacidades de posicionamiento a las distintas redes MANET. El conocimiento de la posición de los nodos en una MANET abre un mundo de posibilidades tanto en términos de servicios de valor añadido (normalmente proporcionado por terceras partes) como en términos de operación y mantenimiento de la red, tareas que pueden ser optimizadas de ser la localización un dato conocido. Este último caso es de especial relevancia en el caso de MANETs. Por ejemplo, los protocolos de encaminamiento destinados a gobernar el tráfico en este tipo de redes sólo son escalables si la posición de los nodos es conocida [1].

El ámbito en el que las MANETs se despliegan, así como su propia naturaleza, hacen que la provisión de la información de posicionamiento sea un reto importante. En la actualidad existe un gran número de técnicas y algoritmos para el posicionamiento en redes ad hoc, como las basadas en huellas de señal [2, 3], en tecnologías Ultra Wide Band [4, 5] o en el ángulo de llegada [6]. Las técnicas basadas en métricas temporales proporcionan un excelente compromiso entre precisión, escalabilidad y coste de desarrollo y mantenimiento, por lo que son muy estimadas en el ámbito ad hoc.

El presente artículo se centra en dos de esas técnicas: tiempo de tránsito de ida y vuelta (2-way TOA) [7, 8] y diferencias de tiempos de llegadas (TDOA) en modo pasivo [9]. Ambas obtienen la posición de los distintos nodos aplicando algoritmos de multilateración a distancias estimadas a partir de métricas temporales. Estas técnicas presentan la ventaja de que habitualmente no requieren del desarrollo de hardware específico, ni de etapas previas al despliegue del sistema de localización. Sin embargo, las medidas temporales no siempre reflejan con la suficiente precisión la distancia entre los nodos implicados. Esta divergencia entre la distancia real y la estimada tiene su origen en múltiples causas. Entre otros, el ruido, obstáculos y propagación multicamino. Este último fenómeno, inherente a las comunicaciones inalámbricas, es de especial relevancia en el ámbito de redes ad hoc. Este tipo de redes con frecuencia es desplegado en escenarios donde la visibilidad directa entre nodos no existe (NLOS). En este tipo de situaciones la distancia estimada corresponde a un camino alternativo y no el directo entre los dos nodos, lo cual se traduce en una estimación de la distancia sensiblemente superior a la medida real.

Son múltiples los modelos presentados con el objetivo de reproducir el impacto de las condiciones NLOS en la estimación de la distancia (o del tiempo de tránsito). Dichas propuestas pueden agruparse en dos grandes bloques: los modelos que dependen de la distancia entre los dos nodos y los que no tienen en cuenta esta dependencia. Cada una de estas propuestas ha sido presentada en un contexto particular y por lo tanto su comparación resulta cuanto menos complicada. El presente artículo pretende cubrir este vacío y evaluar el impacto del modelo de error en las distancias estimadas. De esta forma se implementará un conjunto amplio de modelos y se cuantificará, bajo las mismas

condiciones, su impacto en técnicas 2-way TOA y passive-TDOA.

El resto del artículo se ha estructurado de la siguiente forma. La sección II presenta un breve estado del arte sobre los modelos de error de distancia. En la sección III se describen los modelos empleados en la evaluación y los escenarios sobre los que se procederá a simular dichos modelos. La sección IV por su parte presenta los resultados alcanzados en la evaluación del impacto de los distintos modelos en el cómputo de la distancia entre nodos y por ende de la posición del nodo. Finalmente, en la sección V se exponen las principales conclusiones alcanzadas en este estudio.

II. MODELOS DE ERROR EN DISTANCIA

Existen múltiples propuestas para modelar el error en la estimación de la distancia entre dos nodos. Todos ellos terminan proporcionando una expresión como

$$e_r = \hat{d} - d, \quad (1)$$

donde d es la distancia real entre los nodos implicados, $\hat{d}$ es la distancia estimada y e_r es el error cometido en la estimación. Debe tenerse presente que la Ecuación 1 puede expresarse tanto en términos de distancia como de tiempo, tan sólo con dividir por la velocidad de propagación (habitualmente la velocidad de la luz).

Una de las propuestas más simples es la presentada en [10], la cual consiste en modelar el error en distancia de forma uniforme. Sin embargo esta presunción de uniformidad parece muy alejada de la realidad. Es por ello que numerosos modelos aparecieron con posterioridad, con el objetivo de acercarse más al comportamiento esperado. Alavi *et al.* [11] propone un modelo de error en distancia basado en las condiciones de visibilidad entre nodos, hipótesis muy habitual en el ámbito del posicionamiento. La solución planteada consiste en una suma de dos variables aleatorias, con las que se pretende el modelado de las condiciones de visión directa (LOS) y no directa (NLOS). En el caso de LOS, el error viene caracterizado únicamente por la variable gausiana, que presenta una media nula y una desviación típica σ a definir según las condiciones. Para el caso de NLOS, el error se computa mediante una suma ponderada de dos variables aleatorias. La primera de ellas es una gausiana, que pretende caracterizar errores principalmente derivados del sistema de medidas. La segunda es una variable aleatoria exponencial, que pretende reproducir las condiciones derivadas del escenario NLOS. Sin embargo el modelado de NLOS mediante una variable exponencial presente una importante deficiencia: el efecto cero. Este efecto consiste en que existe una alta probabilidad de obtener un error igual a cero, es decir, el esperado en situaciones LOS y por tanto absolutamente contrarias a las condiciones que se desean modelar. Con el objetivo de evitar este problema, Alavi et al. [12] y Xu et al. [13] proponen el uso de una variable gausiana en lugar de la exponencial para el modelado de la componente NLOS del error en distancia.

Los trabajos mencionados se basan en la suposición común de que el error en distancia puede ser modelado mediante una variable aleatoria estacionaria, es decir, independiente del tiempo o la distancia. Sin embargo, propuestas recientes [12-16] muestran que se alcanzan modelos más realistas si la distancia real es tenida en cuenta para el cálculo del error, especialmente en el caso de pretender la reproducción de condiciones NLOS. De esta forma, Xu et al. [13] propone ponderar la dependencia de la distancia en el error mediante la varianza de la variable gausiana correspondiente a la componente LOS.

Marco et al. evalúan en [14] una técnica de localización empleando un modelo de error de distancia basado en una variable aleatoria exponencial cuya media es proporcional a la dispersión de retardo *(delay spread)*. Dicha dispersión es modelada como una variable aleatoria logonormal cuya mediana aumenta conforme se incrementa la distancia de separación entre los nodos implicados en la medida. De acuerdo al modelo presentado en [17], la dispersión del retardo se expresa como

$$\tau_{rms} = T_1 d^{\varepsilon} y, \quad (2)$$

donde T_1 es la mediana de la dispersión de retardo a 1 km de distancia, d es la distancia en kilómetros e y es una variable aleatoria logonormal, construida sobre una gausiana de media 0 y desviación típica σ_y. De esta forma, cuanto más alejados se encuentre los nodos el uno del otro, mayor será el error cometido al estimar la distancia. Un mecanismo similar se propone en [15] para modelar el error en distancia, aunque en esta ocasión se emplea un valor determinista para caracterizar la dispersión de retardo (es decir, se elimina la variable y de la Ecuación 2).

Una aproximación distinta se sigue en [16], donde se definen tres tipos de entorno: LOS, $NLOS^1$ y $NLOS^2$. Los dos últimos representan dos niveles de restricción en cuanto a propagación de señal en escenarios NLOS, siendo el escenario $NLOS^2$ mucho más restrictivo que el $NLOS^1$. Los tres escenarios descritos son ajustados de acuerdo a medidas procedentes de estudios de campo. El modelo de error en distancia utilizado en [16] consiste en una suma ponderada del error cometido en cada uno de los tres escenarios, donde el peso de cada uno depende tanto de la probabilidad de que un nodo esté en un entorno de ese tipo como de la distancia real que separa a los nodos involucrados en el cálculo de la distancia. De esta forma, cuanto mayor sea la separación entre nodos, mayor será la probabilidad de incurrir en un escenario NLOS, aunque el error derivado del escenario NLOS siga siendo el mismo. En [12] se sigue con esta aproximación, definiendo dos escenarios: LOS y NLOS. El modelo asociado con LOS presenta una dependencia logarítmica con la distancia real, mientras que el modelo propuesto para NLOS no tiene en cuenta la dependencia con la distancia. El error final es una suma ponderada de los dos escenarios, donde la probabilidad de pertenecer a cada uno de los escenarios es nuevamente dependiente de la distancia real.

De esta forma, múltiples propuestas han sido presentadas para el modelado del error en distancia, si bien no se ha procedido a evaluar el impacto de cada una de ellas en el cálculo de la posición de una forma comparativa. Este artículo pretende cubrir esta carencia y cuantificar las diferencias en cuanto a precisión derivadas del uso en simulación de distintos modelos de error para la distancia.

III. SIMULACIÓN Y ESCENARIOS

Los modelos de error en distancia planteados en este estudio son evaluados mediante simulación. Se han empleado dos técnicas de localización para el posicionamiento: tiempo de tránsito de ida y vuelta y TDOA pasivo [9]. El escenario simulado está formado por cuatro puntos de acceso

dispuestos en las esquinas de un área de simulación cuadrada, hipótesis muy habitual en evaluaciones de sistemas de posicionamiento. Sobre esta área se sitúan dos nodos, uno de ellos empleando una técnica de posicionamiento basada en el tiempo de tránsito de ida y vuelta (TOA); y otro implementando la técnica de TDOA pasivo. Ambas técnicas emplearán el algoritmo de mínimos cuadráticos no lineales propuesto por *Levenberg-Marquard* para estimar la posición del nodo. Debe tenerse presente que los errores derivados de la geometría (DOP) caen fuera del propósito de este estudio.

Tres son los modelos de error que han sido evaluados en este estudio: exponencial independiente de la distancia, exponencial dependiente de la distancia y gausiano dependiente de la distancia. En el primero de ellos, el error en distancia se calcula mediante

$$e_{r_1} = w_1 N(0,\sigma) + w_2 Exp(\lambda), \quad (3)$$

donde $N(0,\sigma)$ es una variable aleatoria gausiana de media cero y desviación típica σ; $Exp(\lambda)$ representa una variable aleatoria exponencial de media λ^{-1} y w_1 y w_2 son los pesos de cada uno de esos dos componentes. Por su parte, los errores producidos por el modelo exponencial dependiente de la distancia se calculan mediante

$$e_{r_2} = w_1 N(0,\sigma) + w_2 Exp(\beta), \quad (4)$$

donde el valor medio β se calcula como

$$\beta = cT_1 d^{\varepsilon} y. \quad (5)$$

Finalmente, el modelo gausiano dependiente de la distancia genera errores según

$$e_{r_3} = w_1 N(0,\sigma) + w_2 N(\beta, \rho \cdot \beta), \quad (6)$$

donde ρ representa el coeficiente de variación de la gausiana, es decir, el ratio entre la desviación estándar y el valor medio de la variable aleatoria en cuestión. Tal y como puede observarse, todos los modelos planteados sólo difieren en el componente empleado para caracterizar la contribución en escenarios NLOS. De esta forma, se ha optado por seguir la tendencia marcada en otros estudios [9, 16] y dotar de más relevancia a la componente NLOS, adoptando 0.26 y 0.74 como valores para los pesos w_1 y w_2.

La Tabla 1 presenta el resto de los parámetros empleados para los distintos modelos de error en distancia, donde σ_{ly} representa la desviación típica de la variable logonormal y en la Ecuación 2. Esos valores han sido tomados de distintos estudios [9, 12, 15] y adaptados a condiciones de interior, puesto que dichas condiciones representan uno de los escenarios más restrictivos en términos de propagación de señal y por ende más perjudiciales para el sistema de localización. Bajo este escenario base, se ha procedido a alterar los valores de λ y β. Con ello se consigue alterar la raíz del valor cuadrático medio (RMS) del error en distancia (a través del valor del parámetro T_1). Se han considerado valores de RMS para el error en distancia desde 0.1 hasta 2 metros, cifras normalmente propuestas para sistemas de localización en interiores (por ejemplo los basados en *ultra wide band*).

Para la simulación se utilizó el método de Montecarlo, calculándose la posición de los dos nodos anteriormente indicados en cada una de las iteraciones. El procedimiento seguido es el mismo que se detalla en [9] y que se resume a continuación:

σ	λ^{-1}	T_1	ε	σ_{ly}	ρ
0.0129 m	0.1185 – 0.5561 m	1.57 – 23.41 ns	0.3	4.0	0.94

Tabla 1. Parámetros de simulación.

i. Se sitúa el nodo TOA de forma aleatoria en el área de simulación.
ii. Se sitúa el nodo TDOA de forma aleatoria en el área de simulación.
iii. Se calculan la posición de cada uno de los nodos y el valor de los distintos errores que ellas se derivan.
iv. Volver al paso ii) 1000 veces, es decir, manteniendo la posición del nodo TOA, obtener resultados para 1000 posiciones aleatorias del nodo TDOA.
v. Volver al paso i) 1000 veces, es decir, repetir todo el proceso para 1000 posiciones aleatorias del nodo TOA.

Se emplearon áreas de simulación cuadradas desde 10 a 50 metros de lado. Debido a la similitud en los resultados y la restricciones de espacio, se ha decido mostrar únicamente los resultados derivados del escenario de 20 metros de lado, que es una dimensión adecuada a los despliegues de red actuales con una densidad moderada de nodos.

IV. Evaluación de los modelos de error

En esta sección se evalúa el impacto del modelo de error en distancia sobre el cálculo de la posición empleando técnicas basadas en métricas de distancia temporal, como son TOA y TDOA. La Fig. 1 muestra la evolución del RMS del error de posicionamiento con respecto al RMS del error en distancia. Las menciones a *Exponencial* y *Gausiano* en la Fig. 1 hacen referencia a los modelos dependientes de la distancia en los que la componente NLOS viene modelada por una variable aleatoria de ese tipo. Por su parte, *Independiente* hace referencia al modelo de error no dependiente de la distancia. Las posiciones son estimadas mediante el algoritmo de mínimos cuadráticos no lineal de *Levenberg-Marquardt* (LM) [18]. Para su inicialización se empleará la posición obtenida mediante el algoritmo de mínimos cuadráticos lineal (LLS).

La Fig. 1 recoge la precisión obtenida con cada una de estas posiciones. Tal y como puede observarse, en el caso de la técnica TOA, el modelo de error en distancia impacta de forma notable en el error de posicionamiento obtenido. Las líneas discontinuas en la Fig. 1 (a, b) representan el intervalo de confianza al 95% para las presiones obtenidas. Nótese como las diferencias son apreciables incluso teniendo en cuenta el margen suscitado por el intervalo de confianza, lo que subraya la importancia del modelo de error en distancia en el cálculo de la posición para este tipo de técnicas. Las técnicas basadas en TDOA por otro lado se muestran más insensibles al modelo de error en distancia, ofreciendo valores muy similares en los distintos modelos de error. El intervalo de confianza no ha sido incluido en el caso de técnicas TDOA puesto que ha resultado ser despreciable (menor que el 0.1% del valor obtenido en cada caso).

Cuando se emplea TOA como técnica de posionamiento, el modelo de error independiente de la distancia produce errores menores a los derivados del resto de modelos

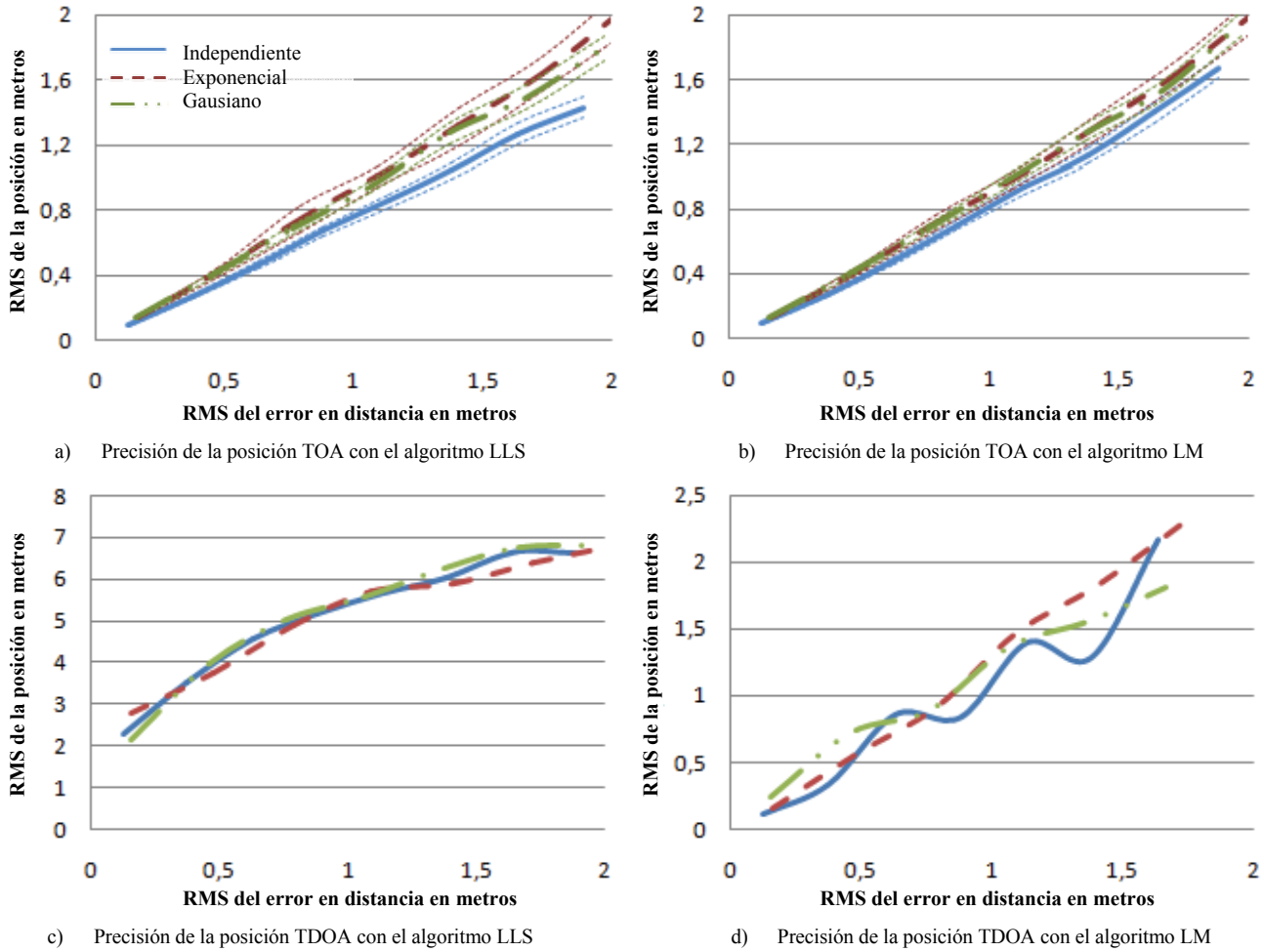


Fig. 1. Precisión alcanzada mediante las técnicas TOA (ida y vuelta) y TDOA y algoritmos de mínimos cuadráticos

dependientes de la distancia, más cercanos a la realidad [12-16]. Es decir, proporciona resultados optimistas en términos de precisión. Además, esta diferencia entre el modelo independiente y los dependientes se muestra mayor cuanto mayor es el RMS del error en distancia. En cuanto a los modelos que tienen en cuenta la distancia real entre nodos, la diferencia entre los errores proporcionados por uno u otro es escasa, probablemente porque ambos modelos presentan momentos muy similares (misma media y desviación típica prácticamente idéntica). De esta forma, para el caso de la técnica *2-way TOA*, se puede afirmar que la precisión expresada en términos de RMS del error de posicionamiento no es sensible a la distribución de la componente NLOS del modelo de error en distancia.

Lo anterior no aplica al caso del TDOA pasivo, donde la técnica se muestra muy poco sensible al modelo de error en distancia seleccionado. Son escasas las diferencias entre los resultados derivados de cada uno de los modelos, con independencia de que consideren la distancia real o no. El motivo principal de la cercanía en resultados, así como de la variabilidad al aumentar la magnitud del error en distancia, estriba en el hecho de que el TDOA pasivo opera con medidas más ruidosas que la técnica TOA en la que se apoya. Es así ya que uno de los nodos de referencia tiene asociada una posición con un cierto error, cosa que no sucede en TOA. Ese error en la posición del nodo de referencia enmascara al resto, haciendo mínimas las diferencias entre los modelos de error en distancia.

Los resultados en cuanto a precisión obtenidos mediante los algoritmos LLS y el LM empleando la técnica TOA son muy cercanos entre sí. Esta similitud viene explicada por el hecho de que los observables son suficientemente buenos como para operar de forma óptima empleando ambos algoritmos, de forma que sólo se producen diferencias entre ellos catalogables como estadísticas (es decir, derivadas del propio análisis). Este comportamiento sin embargo no es extensible a la técnica de TDOA pasivo, donde el algoritmo LLS muestra una evolución mucho más estable que para vislumbrada para el caso de LM. La explicación a este fenómeno fue ya introducida en párrafos anteriores y es el hecho de que el TDOA pasivo opera con medidas más ruidosas. Por lo tanto, aunque el resultado del LLS muestra una evolución muy consistente, el error cometido en el posicionamiento es muy superior al observado en técnicas TOA. Al alimentar al algoritmo de LM con un valor más pobre, se aumenta la probabilidad de que el algoritmo no alcance el valor óptimo en el número de iteraciones marcadas, observándose por tanto una evolución menos estable que en el caso del LLS o la reportada en el caso de TOA. Dependiendo de la situación, el valor óptimo no puede alcanzarse, aún aumentándose el número de iteraciones. En esos casos el algoritmo se limita a proporcionar un mínimo local, frecuentemente alejado del mínimo global buscado.

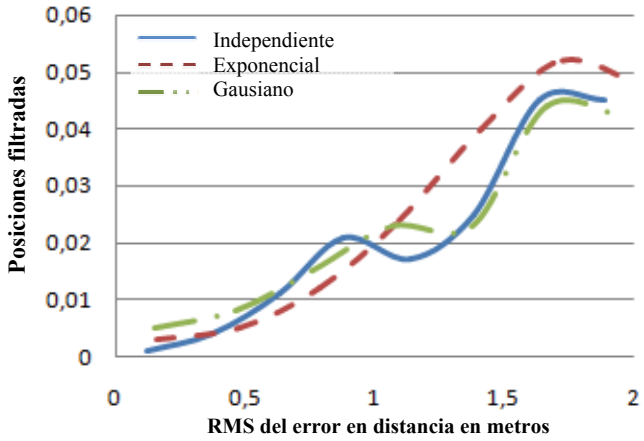


Fig. 2. Porcentaje de posiciones filtradas en TDOA pasivo empleando el algoritmo LM

Percentil	Modelo de error	Coeficientes		
		b_0	b_1	R^2
66% (TOA)	Independiente	- 0,0789	0,8771	0,9900
	Exponencial	- 0,0757	0,9027	0,9933
	Gausiano	- 0,0766	0,9821	0,9948
66% (TDOA)	Independiente	- 0,0306	0,8839	0,9975
	Exponencial	- 0,0146	0,8916	0,9984
	Gausiano	- 0,0202	0,9546	0,9990
95% (TOA)	Independiente	- 0,1381	1,6871	0,9951
	Exponencial	- 0,1598	1,9425	0,9958
	Gausiano	- 0,0699	1,7544	0,9986
95% (TDOA)	Independiente	- 0,0788	1,7663	0,9927
	Exponencial	- 0,0334	1,8206	0,9959
	Gausiano	- 0,1752	1,9877	0,9835

Tabla 2. Regresión lineal de los percentiles de acuerdo al modelo de error en distancia

Para evitar los errores aberrantes, se han eliminado todas aquellas posiciones cuyo error asociado era superior a la distancia entre dos puntos de referencia (es decir 20 metros). Este umbral coincide con dos veces el error proporcionado por técnicas basadas en la identificación de celda y por lo tanto puede ser considerado como parte de una hipótesis conservadora. La Fig. 2 muestra el porcentaje de posiciones TDOA que han sido rechazadas bajo este criterio (dicho porcentaje en la técnica TOA es 0 para todos los escenarios y modelos simulados). Tal y como se puede apreciar, la tasa de posiciones con consideradas es similar en los tres modelos der error. Sin embargo, el modelo exponencial dependiente de la distancia tiende a divergir con una mayor facilidad que el resto de modelos al aumentar el RMS del error en distancia.

Dos métricas ampliamente utilizadas en la evaluación de técnicas de localización son el percentil al 66% y al 95%. Los datos recogidos respecto a dichos percentiles muestran una evolución lineal con respecto al RMS del error en distancia. De esta forma, se puede llevar a cabo una regresión lineal sobre los datos recogidos de tal forma que pueda definirse el percentil como

$$, \qquad (7)$$

donde e_p es el percentil del error de posicionamiento, RMS_r es el RMS del error en distancia y b_0 y b_1 son los parámetros que definen la regresión. La Tabla 2 muestra los parámetros derivados de la regresión lineal aplicada a los percentiles del 66% y 95% del error de posicionamiento en TOA y TDOA, así como el coeficiente de determinación R^2 producto de la regresión. Tal y como puede apreciarse, la mayor parte de la variabilidad de los datos defiende la hipótesis de aproximación lineal para los distintos percentiles, con independencia del modelo de error seleccionado. Sin embargo, sí existen diferencias en los resultados de cada uno de los modelos. Concretamente, los modelos que tienen en consideración la distancia real entre nodos proporcionan percentiles con un valor mayor que el modelo que no contempla la distancia real, factor que indica que los modelos dependientes de la distancia aportan cifras más conservadoras en cuanto a error de posicionamiento. Esta aseveración está en consonancia con los resultados presentados con anterioridad para el RMS del error de posicionamiento. En cuanto a las diferencias entre los modelos dependientes de la distancia, puede observarse como para percentiles bajos (ej. 66%), el modelo gausiano parece expresar mejor la evolución lineal con respecto al RMS del error en distancia (es decir presenta R^2 mayores). Para el percentiles mayores (ej. 95%), esta diferencia queda diluida. En cualquier caso, las diferencias entre uno y otro no son significativas.

La Fig. 3 muestra una estimación de la función de densidad de probabilidad del error de posicionamiento para los tres modelos de error simulados, de acuerdo a los valores recogidos. Tal y como puede apreciarse, todos los modelos tienen a producir formas similares en cuanto a la densidad de probabilidad. Sin embargo, existen diferencias notables si se comparan las funciones derivadas de los modelos dependientes de la distancia con los que no lo son. El modelo independiente de la distancia entre nodos tiende a concentrar la probabilidad de error en los valores más pequeños, presentando además una mayor variabilidad en cuanto a probabilidad que los modelos dependientes de la distancia. Este fenómeno es especialmente notable en el caso de la técnica TOA. Los modelos dependientes de la distancia presentan funciones de densidad de probabilidad más suaves en cuanto a transiciones se refiere, con formas más definidas y estables, que tienen a tener una caída más suave y prolongada que la mostrada para el caso del modelo no dependiente de la distancia. Este hecho no hace sino confirmar lo ya observado con anterioridad: el modelo independiente tiende a aportar valores más optimistas en cuanto a error de posicionamiento que los modelos dependientes en distancia, por lo que su uso debería ser relegado a tareas de evaluación o pruebas de concepto en favor de modelos más ricos como los dependientes de la distancia aquí presentados.

V. Conclusiones

Este artículo presenta una comparativa entre distintos modelos de error en distancia, empleados en el ámbito de la simulación para producir errores con los que evaluar diferentes técnicas de localización basadas en métricas temporales (ej. TOA de ida y vuelta y TDOA pasivo). Se han evaluado tres modelos de error bajo las mismas condiciones. En concreto se ha definido un escenario de interior al que se le han aplicado los distintos modelos y diversos valores de RSM para el error en distancia. Se han realizado simulaciones de Montecarlo, centrando el interés en

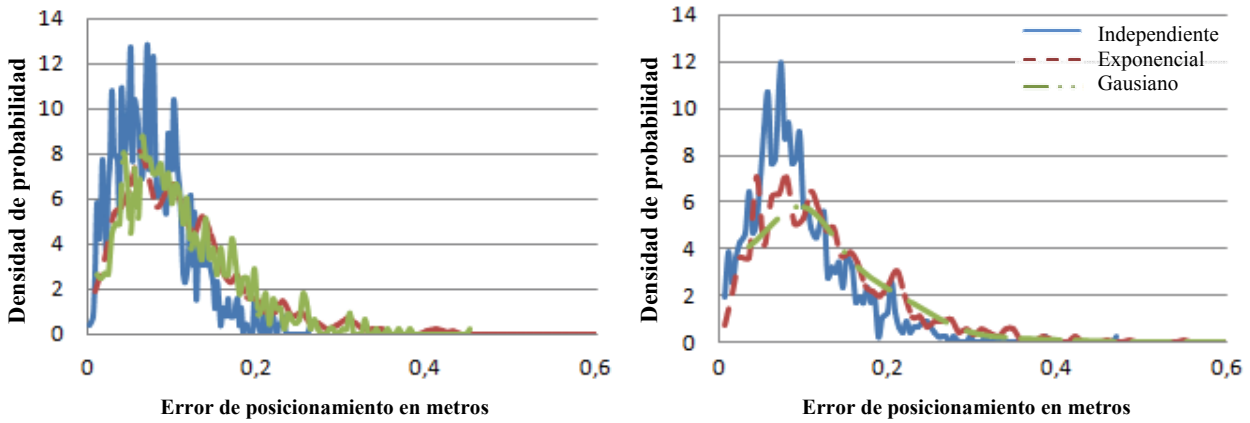


Fig. 3. Función de densidad de probabilidad empírica del error de posicionamiento en TOA (izquierda) y TDOA pasivo (derecha) con un RMS del error en distancia de 0.12 metros

cuantificar las diferencias entre modelos dependientes de la distancia entre nodos y aquellos que no lo son. Los resultados muestran como los errores derivados del modelo independiente de la distancia tienden a ser optimistas, proporcionando valores inferiores a los derivados del uso de modelos de error que tienen en consideración la distancia real entre nodos. Este hecho es especialmente notable en técnicas TOA, mientras que la técnica de TDOA pasivo parece no ser especialmente dependiente del modelo de error en distancia seleccionado.

Dado que el uso de modelos dependientes de la distancia no responde únicamente a un acto intuitivo, sino que está corroborado por múltiples estudios, puede concluirse que los modelos no dependientes de la distancia proporcionan métricas de rendimiento superiores a las que cabría esperar en despliegues reales del sistema. Por lo tanto se aconseja el uso de modelos dependientes de la distancia, a costa de un pequeño incremento en el coste computacional de la simulación.

AGRADECIMIENTOS

Este artículo ha sido parcialmente financiado por el gobierno español mediante el proyecto TEC2009-08198.

REFERENCIAS

[1] I. Stojmenovic, "Position-based routing in ad hoc networks", IEEE Communications Magazine, vol. 40, no. 7. pp. 128-134, July 2002.

[2] M. Brunato, R. Battiti, "Statistical learning theory for location fingerprinting in wireless LANs", Elsevier Computer Networks, vol. 47, issue 6, pp. 825-845, November 2004.

[3] Widyawan, M. Klepal, D. Pesch, "Influence of Predicted and Measured Fingerprint on the Accuracy of RSSI-based Indoor Location Systems", 4th Workshop on Positioning, Navigation and Communication (WPNC), pp. 145-151, March 2007.

[4] A. Hatami, K. Pahlavan, "Performance Comparison of RSS and TOA Indoor Geolocation Based on UWB Measurement of Channel Characteristics", IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-6, September 2006.

[5] K. Yu, I. Oppermann, "Performance of UWB position estimation based on time-of-arrival measurements", International Workshop on Ultra Wideband Systems 2004, pp. 400-404, May 2004.

[6] S. Venkatraman, J.Jr. Caffery, "Hybrid TOA/AOA techniques for mobile location in non-line-of-sight environments", IEEE Wireless Communications and Networking Conference (WCNC 2004), vol. 1, pp. 274-278, March 2004.

[7] M. Ciurana, F. Barcelo-Arroyo, F. Izquierdo, "A ranging system with IEEE 802.11 data frames", Wireless Communications and Networking Conference (WCNC), pp. 2092-2096, March 2007.

[8] D. Kang, Y. Namgoong, S. Yang, S. Choi, Y. Shin, "A simple asynchronous UWB position location algorithm based on single round-trip transmission", International Conference on Advanced Communication Technology (ICACT). vol. 3, pp. 20-22, 2006.

[9] I. Martin-Escalona, Francisco Barcelo-Arroyo, "A new time-based algorithm for positioning mobile terminals in wireless networks", EURASIP Journal on Advances in Signal Processing, vol. 2008, pp. 1-10, 2008.

[10] C. Yiu-Tong, T. Wing-Yue, S. Hing-Cheung, C. Pak-chung, "Time-of-Arrival Based Localization Under NLOS Conditions", IEEE Transactions On Vehicular Technology, vol. 55, no. 1, January 2006.

[11] B. Alavi, K. Pahlavan, "Modeling of the Distance Error for Indoor Geolocation", IEEE Wireless Communications and Networking Conference (WCNC), vol. 1, pp. 668-672, March 2003.

[12] B. Alavi, K. Pahlavan, "Modeling of the TOA-based Distance Measurement Error Using UWB Indoor Radio Measurements", IEEE Communications Letters, vol. 10, No. 4, April 2006.

[13] J. Xu, M. Ma, C. L. Law, "Theoretical Lower Bound for UWB TDOA Positioning", IEEE Global Telecommunications Conference (Globecom), pp. 4101-4105, Nov. 2007.

[14] A. Marco, R. Casas, A. Asensio, V. Coarasa, R. Blasco, A. Ibarz, "Least Median of Squares for Non-Line-of-Sight Error Mitigation in GSM Localization", IEEE Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-5, Sept. 2008.

[15] J. Schroeder, S. Galler, K. Kyamakya, K. Jobmann ,"NLOS detection algorithms for Ultra-Wideband localization", Positioning, Navigation and Communication, 4th Workshop on Positioning, Navigation and Communication (WPNC), pp. 159-166, March 2007.

[16] B. Denis, N. Daniele,"NLOS Ranging Error Mitigation in a Distributed Positioning Algorithm for Indoor UWB Ad-Hoc Networks" , IEEE International Workshop on Wireless Ad-Hoc Networks, pp. 356- 360, June 2004.

[17] L.J. Greenstein, V. Erceg, Y. Shuan Yeh, M.V. Clark, "A New Path-Gain/Delay-Spread Propagation Model for Digital Cellular Channels", IEEE Transactions On Vehicular Technology, vol. 46, no. 2, May 1997.

[18] D.W. Marquardt, "An Algorithm for Least-Squares Estimation of Nonlinear Parameters", SIAM Journal on Applied Mathematics, vol. 11, no. 2. pp. 431-441, 1963.

Implementation and evaluation of Multi-hop routing in 6LoWPAN

Alessandro Ludovici, Anna Calveras

Wireless Networks Group (WNG), Universitat Politècnica de Catalunya, C/ Jordi Girona, 1-3, Mòdul C3 – Campus Nord.
08034 Barcelona, Spain
alessandro.ludovici@entel.upc.edu,

***Abstract*- 6LoWPAN enables the transmission of IPv6 packets over LoWPAN networks. In order to make it possible, 6LoWPAN introduces an adaptation layer between network and link layers. This layer allows IPv6 packets to be adapted to the lower layers constraints. It provides fragmentation and reassembling of packets and header compression. It also can be involved in routing decisions. Depending on which layer is responsible of routing decisions 6LoWPAN divides routing in two categories: mesh under if the interested layer is the adaptation layer, route over if it is the network one. In this paper we compare the two routing solutions evaluating their performances in terms of end-to-end delay and round-trip time. All the performance evaluation has been realized in a real implementation of 6LoWPAN.**

***Key Words*- 6LoWPAN, *route over*, *mesh under*, blip, sensors networks**

INTRODUCTION

Wireless Sensor Networks (WSN) represents a low-cost and distributed solution for network applications in environments where wired networks cannot be applied or their deployment is not feasible. WSN are composed by many devices (sensors/actuators) usually embedded in a physical environment to monitor its conditions (e.g. temperature, pollution).

WSN are typically composed by a number of low-power devices having a short communication range. Depending on the application environment, physical obstacles can mask the wireless link between them. This scenario suggests the adoption of multi-hop routing solutions. Furthermore, multi-hop routing helps to broaden the communication range and to use alternative links.

Although a WSN can be based on various protocol stacks, it would be preferable to adopt a standard solution as the one provided for physical and data link layers by the IEEE 802.15.4 standard [1]. Concerning the upper layers, it is possible to find a number of protocols developed as a proprietary solution. As consequence, the integration of WSN with external networks or the interoperability of different WSN become more difficult. WSN would result as stand-alone networks while it would be useful to integrate them in external networks like IP based networks. In this sense, the adoption of IP as network layer protocol would give a chance to integrate embedded wireless network with Internet. In particular, the adoption of IPv6 will provide enough space to address large WSN. The specification on how to enable IPv6 over WSN based on IEEE 802.15.4 are carried out by a specific IETF WG called 6LoWPAN [8] (IPv6 over Low power Wireless Personal Area Networks). Its aim is to provide mechanisms and architectural solutions to ease the integration of the IPv6 in constrained networks environments specified as Low power Personal Area Networks (LoWPAN).

IEEE 802.15.4

LoWPAN are defined by the IEEE 802.15.4 standard. Following the OSI reference model, it specifies the physical and the Medium Access Control (MAC) sub-layer of the data link layer. LoWPAN are characterized to be resource constrained. Devices forming them typically have an 8-bit or 16-bit CPU, 4 KB to 8 KB of RAM and 48 KB to 128 KB of ROM. Due to the limitation in processing and in storage capabilities, the software components developed for these networks have to be very simple and light-weight. Since devices are mainly battery powered, it has to be considered the energy consumption as key aspect when developing such constrained networks. Usually, these devices alternate between being awake for a short amount of time and then entering a sleep mode in which they consume less energy.

A LoWPAN network has also limitation in the available bandwidth. Depending on the frequency band it operates the resulting data-rate are of 250 Kbps (2.4 GHz), 100 Kbps, 40 Kbps or 20 Kbps. Furthermore, LoWPAN networks are self-healing and self-organizing meaning that a node is able to recover from errors and to join a network without external intervention.

IEEE 802.15.4 defines the use of 16-bit short or 64-bit extended link layer addresses and a MTU of 127 bytes. Short addresses are preferable in order to reduce overhead in the MAC frame.

6LoWPAN

The transmission of IPv6 packets over IEEE 802.15.4 links introduces several challenges. Besides the low capabilities in terms of processing, memory and bandwidth of 802.15.4 devices, the IPv6 adoption as network layer protocol does not fit with its MTU (Maximum Transferable Unit) specifications. IPv6 requires at least a MTU of 1280 bytes that is ten times the one specified for 802.15.4 networks. The 40-bytes length IPv6 header imply a huge overhead that, considering the presence of transport layer header (8 bytes for UDP), MAC header (25 bytes) and link-layer security (21 bytes), would leave only 33 bytes available for application data payload. Both problems are addressed in the 6LoWPAN specification [2]. In order to satisfy the MTU requirements of IPv6 and reduce the overhead, 6LoWPAN implements an adaptation layer placed between network and data link layers. This layer provides a mechanism for packet fragmentation, header compression and support for data link layer forwarding of IP packets [3].

IPv6 header compression in 6LoWPAN is possible since the information contained in the header can be inferred from lower layers or by assuming a shared context between network nodes. It can be supposed that a number of 6LoWPAN application scenarios would require packet size considerable smaller than the IPv6 MTU. Consequently, the application payload in addition with the IPv6 compressed header would fit with the MTU requirements of 802.15.4. However, the introduction of further overhead from higher layer protocols or routing headers would require fragmentation of IPv6 packets into multiple MAC frames.

The adaptation layer can also be responsible to take routing and forwarding decisions instead of the network layer. Depending on which layer is in charge of routing and packet forwarding, 6LoWPAN divides routing in two schemes: *mesh under* if routing is done at the adaptation layer and *route over* if done at the network layer.
In fig. 1 and 2 are showed the 6LoWPAN protocol stacks for *mesh under* and *route over*.

The network topology of LoWPAN is expected to be a star or either a mesh topology. However, even if a mesh routing protocol is expected to run over LoWPAN, the 802.15.4 specification does not define such capability [2].

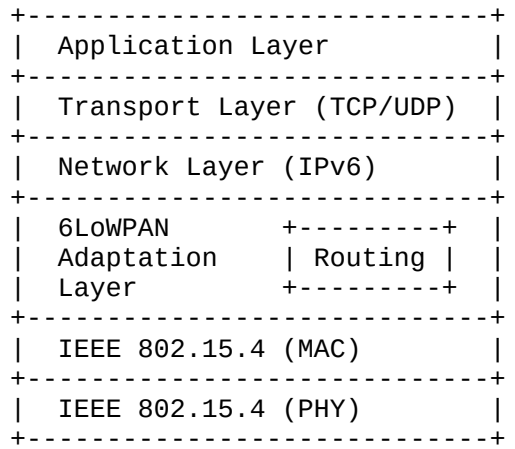


Fig.1 6LoWPAN *mesh under* protocol stack [4]

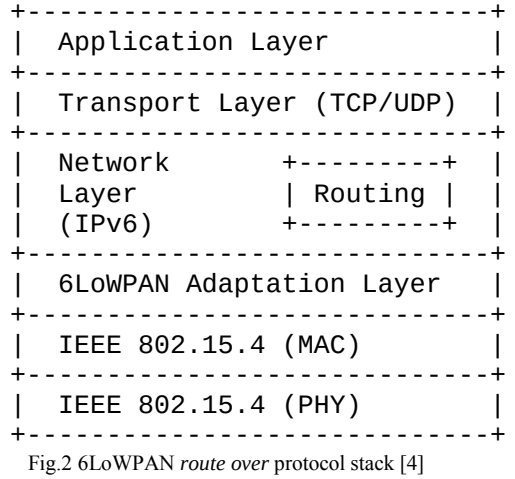


Fig.2 6LoWPAN *route over* protocol stack [4]

The work presented in this paper is to analyse the characteristics of both routing schemes and test their performances in a real 6LoWPAN implementation. We will show how *mesh under* and *route over* performs in terms of latency in a multi-hop 6LoWPAN network.

The rest of the paper is organized as follow: In the next section we present previous research and discussions on *mesh under* and *route over*. Then we will explain how the two routing schemes work and differs. Subsequently, we will introduce the implementation and the test-bed used for their performance evaluation. Finally, we will present the main results of our research and give guidelines for future works.

Related Work

Discussions on *mesh under* and *route over* are presented in [3] and [4]. In [4] there are specified a series of guiding principle for 6LoWPAN routing including both *mesh under* and *route over* solutions. In [3] an extended explanation of the adaptation layer and issues of *mesh under* and *route over* are given.

To our best knowledge, there are no performance analyses of *mesh under* and *route over* but an analytical analysis on a comparison of both routing schemes [5]. Chowdury et al. show in their work how *mesh under* and *route over* differs in terms of packet arrival probability, retransmission policies and latency. A probabilistic model has been used to compare the routing schemes. Considering a transmission of IP fragmented packets in a multi-hop 6LoWPAN network, they demonstrate how *route over* has a higher fragment arrival probability than *mesh under*. In fact, in *route over* the packet is reassembled at each hop before being fragmented again and forwarded. If a fragment gets lost, the previous hop resends the whole IP packet. In *mesh under* the packet is reassembled at destination and each fragments can be forwarded trough a different path. If a packet gets lost the source resend the whole packet. Furthermore, they have shown how in *route over* there is the possibility of buffer overflow when a node is reconstructing a packet. Analysis on latency has demonstrated that it is higher in *route over* due to the time spent in reassembling and fragmenting the packet at each hop. In the next section we explain in more detail the 6LoWPAN routing schemes.

6LoWPAN Routing

Since in *route over* decisions are taken at network layer, the addresses carried in the IPv6 headers are used to forward the packet to next hop. IPv6 source address represents the node that has initiated the communication while the destination address is the final node. When a node receives a packet, it unpacks the IPv6 header and uses the destination address to determine whether or not the packet is for itself. If not, it decrements by one unit the hop limit field and, if not zero, it checks its routing table to determinate the next hop. Intermediates nodes addresses are specified as link layer addresses. In *route over* each hop is considered as an IP hop and each node acts as an IPv6 router as well as the edge router. An example of network topology in route over is reported in Fig.6, while in Fig.7 it is showed an example for *mesh under*.

Route over protocols could use routing headers included in the IPv6 payload as an IP extension header. The header chain for *route over* is reported at Fig. 3.

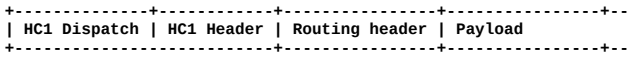


Fig.3 Header encapsulation in *route over*

In *mesh under*, packets are routed at adaptation layer. As well as for *route over*, addresses of intermediates hops are specified as link layer addresses. To realize *mesh under* it is defined the use of a mesh header. In Fig.4 it is showed the mesh header pattern and in Fig.5 how it is encapsulated in the 6LoWPAN frame.

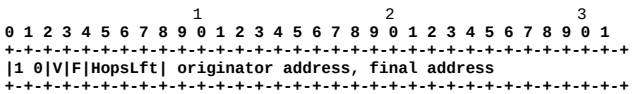


Fig.4 mesh header

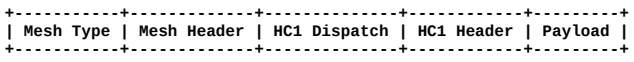


Fig.5 header encapsulation in *mesh under*

The mesh type is specified by the first two bits settled to 1 and 0. The length of originator and final addresses are specified respectively by the V and F bits. If they have the value of 0, the addresses are IEEE extended 64-bit addresses; if 1 they are short 16-bit addresses. The originator and final addresses are in that order the address of the node starting the communication and its destination. Four bits of the first octet are used to specify the number of hops. It can be defined up to 14 hops. An extra byte can be added to define a number of hops greater than 14 by setting the Hops Left to 0xF.

When a node receives a packet with a mesh header, it checks the final address to decide whether or not the packet is destined to itself and update the hops left field in case of forwarding.

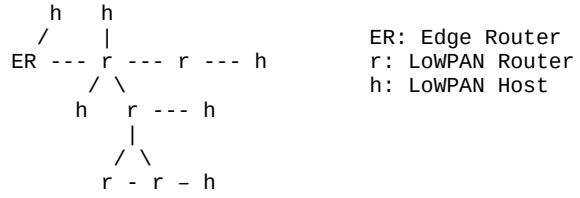


Fig.6 *route over* topology [4]

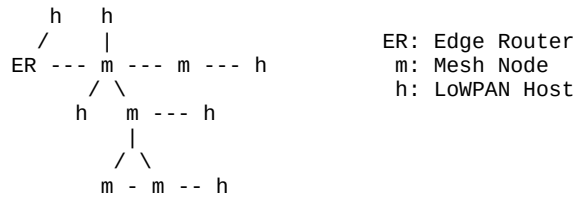


Fig.7 *mesh under* topology [4]

The use of mesh header introduces further overhead. If using IEEE 16-bit short addresses and a number of hops lower than 14, the mesh header length will be of 5 bytes. However, using a mesh header it is possible to compress the IPv6 addresses down to 0 bytes and to elide the hop limit field of the IPv6 header. In that way, the presence of mesh header does not increase the overhead.

IMPLEMENTATION

In this section we describe the implementation of *mesh under* and *route over* in a real 6LoWPAN network environment. We start presenting the protocol stack and the hardware used for our studies. Finally, we will give details on how tests have been done and the network topology used to realize them.

Protocol Stack

We adopted an open-source TinyOS based 6LoWPAN implementation developed by the University of California at Berkeley. It is called Berkeley IP (blip) [4]. Blip consists of TinyOS and ANSI-C code that implements the 6LoWPAN stack on the motes. A Unix daemon translates 6LoWPAN packets reaching the base station mote to IPv6 packets. IPv6 router advertisement messages are generated by standard daemon RADVD. As IPv6 header compression, it uses the 6LoWPAN standard compression HC1 [2].

Blip implements an hybrid routing protocol called HYDRO [5]. Routing decisions as well as packets forwarding are taken at network layer. However, fragmented packets are forwarded trough the destination without the hop-by-hop reassembling required by *route over*.

Blip has libraries to add *mesh under* header but it is not implemented any mesh handler routine. In this work we have developed proper code and modified some of the existing to give to blip the necessary *mesh under* and *route over* capabilities.

Hardware Platform

The Crossbow's TelosB mote is the hardware platform we used four our experiments [9]. It is an open source, low-power wireless sensor module. TelosB motes have a 16-bit RISC MCU at 8 MHz and 16 registers. The platform offers 10 kB of RAM, 48kB of flash memory and 16 kB of EEPROM. Requiring at least 1.8 V, it draws 1.8 mA in the active mode and 5.1 μA in the sleep mode. The MCU has an internal voltage reference and a temperature sensor. Further sensors available on the platform are a visible light sensor (Hamamatsu S1087), a visible to IR light sensor (Hamamatsu S1087-01) and a combined humidity and temperature sensor (Sensirion SHT11).

TelosB motes can be plugged via a USB port to a computer through which the motes can be programmed.

Test-bed

A performance analysis of *route over* and *mesh under* has been done taking into account the average end-to-end delay in packets transmission within the sensor network and the average round-trip delay time. Both tests have been done in a multi-hop network topology. The number of hops for end-to-end delay measurements ranges from a minimum of 2 to a maximum of 14. Regarding RTT, measurements have been done with a number of hop ranging from 2 to 5. The network topology was composed by a number of nodes varying according to the number of hops. In Fig.9 it is showed the topology for a 2 hops network. The network was composed by the followings elements:

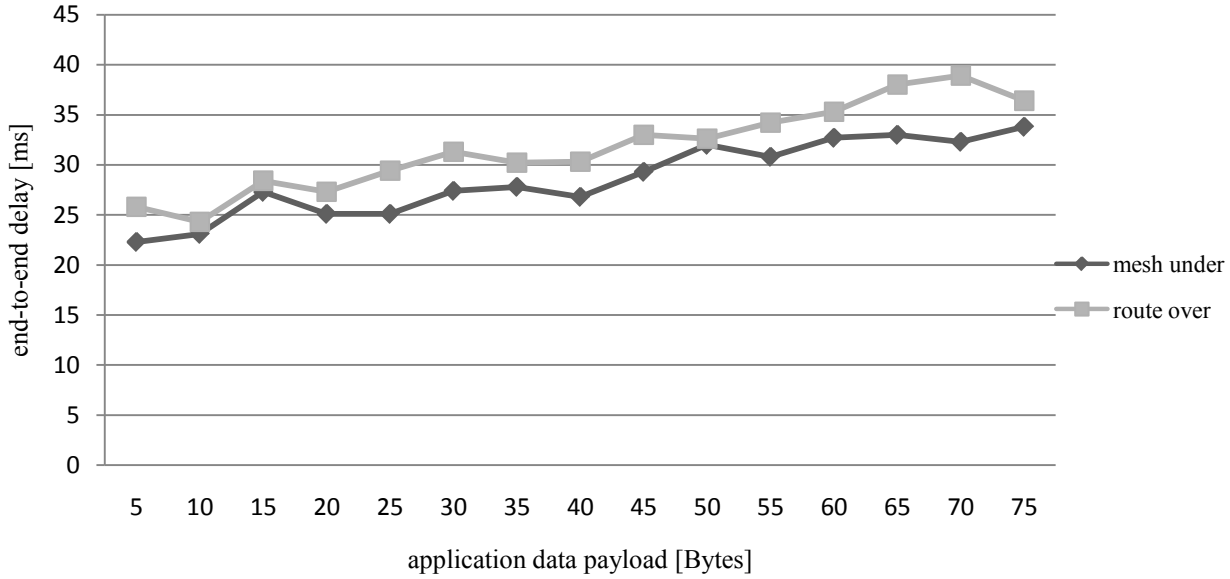


Fig.8 end-to-end delay variation according to application data payload

1) A border router called IP Base Station acting as destination node in end-to-end tests and source in case of round-trip time.
2) A sensor node that transmits UDP packets to the IP Base Station. This is considered the source node in end-to-end tests while it is the destination in case of round-trip time.
3) A variable number of relay nodes acting as packets forwarders.

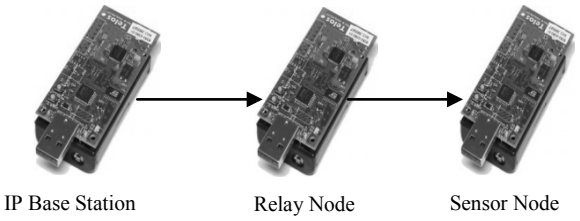


Fig.9 Network topology for a 2 hop scenario

RESULTS

End-to-end delay has been analysed considering two different situations. Firstly, we was interested in evaluating delay for *mesh under* and *route over* according to the application data payload while the number of hops was kept constant. Then, we have observed the delay evolution according to the number of hops keeping the application data payload fixed to a constant value.

In Fig.8 it is showed the end-to-end delay time (in ms) for a 6LoWPAN communication in a network with 4 hops and an application data payload ranging from 5 to 75 bytes, reaching the limit to do not fragment the packet. Nodes were at a constant distance of 25 cm from each other. This distance results enough to avoid direct connectivity between the base station and the destination node. To avoid that the blip routing protocol has influence on results, we used static routes to forward packets trough the network.

For each different application data payload, it has been taken 10 observations of nodes processing and propagation time. This number results to provide a reliable evaluation since we noticed that propagation and processing had no significant variations. The sum of the obtained times gives the delay for the observation. The mean value of the 10 observation taken for each payload size is the resulting end-to-end delay time.

As shown in Fig.8, *mesh under* improves the end-to-end delay trend. It can be explained considering that the processing time of the nodes is lower because the hop-by-hop decompression and compression of the IPv6 header is avoided. The transmission time has no influence on the enhancement of performances since it has the same value in both routing schemes. Considering the difference between the average end-to-end delay times obtained for *mesh under* and *route over*, the first one has an average improvement of 3,1 ms with a peak of 6,6 ms for 70 bytes and a minimum of 0,6 ms for 50 bytes of application data payload.

Fig.10 shows the average end-to-end delay evolution according to the number of hops between source and destination. The application data payload has been fixed to 75 bytes, which is the maximum we can have to avoid fragmentation. The average values from 2 to 5 hops have been obtained in the same way used for the previous delay computation through a real 6LoWPAN communication. The average end-to-end delay obtained from 6 to 14 hops has been obtained simulating a 6LoWPAN communication. In fact, we observed that the delay trend for both *mesh under* and *route over* followed a linear evolution:

$$y = n \times x \tag{1}$$

Considering that the transmission time was constant in each hop and the node processing time was independent from the number of hops, we can calculated the mean value of the processing time for each node. The function expressing the end-to-end delay is:

$$T = n \times (t_t + t_p) \tag{2}$$

Where T is the end-to-end delay, n the number of hops, t_t and t_p stands respectively for the transmission time and average node processing time.

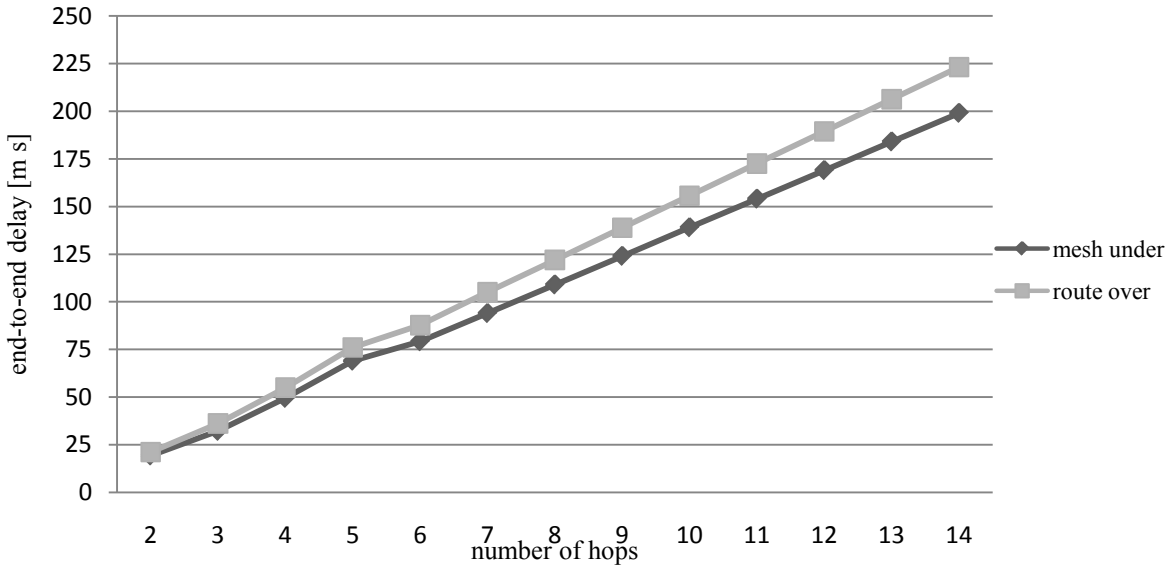


Fig.10 Throughput variation according to the number of hops

Mesh under outperforms *route over* also in this case. Increasing the number of hops the differences between them becomes bigger. For a 2 hops network, delay for *mesh under* is 1,9 ms lower respect to *route over*, considering 14 hops the difference between them is approximated to 24,05 ms. It can be estimated that the introduction of a new hop augment by 1,84 ms the differences between end-to-end delay for *mesh under* and *route over*. Differences in terms of delay between *mesh under* and *route over* are big as we could expect.

A further interesting analysis is in the differences in the time spent by a node to process and forward a packet. It has to be noticed that *mesh under* forwards packets from the adaptation layer avoiding the decompression and compression of the IPv6 packets done in *route over*. For *mesh under* the mean value of node processing time is 11 ms with a standard deviation of 2,1 ms. Regarding *route over* the node processing time is 12,85 ms with a standard deviation of 2,3 ms. The difference between the mean value of processing time of *mesh under* and *route over* gives an estimation of the time spent in both compression and decompression routines, that is 1,85 ms.

It has to be noticed that transmission and node processing time includes DIFS and SIFS time interval defined in the CSMA\CA mechanism used by LoWPAN. In [1] are defined minimum DIFS and SIFS period expressed in number of symbols. According to [10] for the 2.4 GHz band 2 symbols are correspondent to 32µs. DIFS is fixed to 40 symbols and it is equivalent to 640 µs while SIFS to 192 µs since it is set to 12 symbols. DIFS period has to be included in the node processing time while SIFS in the transmission time.

A further analysis has been done taking into account the round-trip time delay. Table 1 shows the results obtained for *mesh under* while Table 2 for *route over*. The round-trip time delay has been measured using the ping6 command. For each number of hops it has been sent 1000 packets with a payload size of 60 bytes. However, the performances obtained for end-to-end delay and round-trip-time are not comparable. In fact, end-to-end delay take in account only the time spent by the packet to reach the destination node without taking into account the processing time of the final node. Instead, in round-trip-time results it is included the time needed to process ping response and presents the results.

Number of hops	Average RTT (ms)	Max RTT (ms)	Min RTT (ms)	Standard deviation (ms)
2	117,72	131,01	103,53	5,78
3	148,83	168,07	129,51	7,03
4	175,68	192,07	152,09	7,83
5	202,51	224,1	181,12	8,41

Table 1: Round-Trip Time (RTT) statistics for mesh under

Number of hops	Average RTT (ms)	Max RTT (ms)	Min RTT (ms)	Standard deviation (ms)
2	118,47	133,03	104,9	6,03
3	149,39	184,09	131,03	7,53
4	178,82	245,04	164,06	8,34
5	213,91	252,12	190,12	9,37

Table 2: Round-Trip Time (RTT) statistics for route over

Comparing round-trip time statistics for *mesh under* and *route over*, it can be appreciated how *mesh under* outperforms *route over*. The lower time spent to forward the packet in a *mesh under* node respect to a *route over* one, is the key to keep latency low.

In a multi-hop scenario, the use of *mesh under* would decrease the node occupancy time having an important reflection in the node's energy consumption. In fact, less time a communication lasts and more energy can be saved by nodes.

CONCLUSION

The contribution of this paper has been the examination of *mesh under* and *route over* routing schemes in 6LoWPAN. Our attention has been focused on the end-to-end delay and round-trip time performance evaluation. All the tests have been done on a real 6LoWPAN network. A TinyOS based open-source implementation of 6LoWPAN protocol stack named blip has been used for our studies. We adapted it in order to implements correctly the mesh under capabilities and installed in TelosB motes. For our tests, we have considered only 6LoWPAN communications not requiring packet fragmentation. As expected, to forward packets from the adaptation layer instead of the network one has reduced the time spent in packet processing. This allowed *mesh under* to have better performance in both end-to-end delay and round-trip time. We have tested both routing techniques in a multi-hop network according to different size of application data payload and number of hops.

FUTURE WORK

The tests made in this work have been done in absence of packet fragmentation. We will include in future work the evaluation of both *mesh under* and *route over* in 6LoWPAN communications with fragmented packets. Besides the repetition of end-to-end delay and round-trip time performance evaluation, we will take in account also to test the energy consumption of both routing schemes. Future work will be based on the same 6LoWPAN protocol stack implementation and hardware used in this work.

ACKNOWLEDGEMENTS

This work has been supported by Spanish Government through project TEC2009-11453, and by the Catalan Government (Comissionat per a Universitat i Recerca del DIUE) and the Social European Budget.

REFERENCES

[1] IEEE Computer Society. IEEE Standard 802.15.4-2006. Part 15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). 2006.

[2] Montenegro, G.; Kushalnagar, N.; Culler, D.E. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. IETF RFC 4944. 2007

[3] Hui, J.W.; Culler, D.E. Extending IP to Low Power, Wireless Personal Area Networks. IEEE Internet Computing 2008, vol.12, no.4, 37-45.

[4] Kim, E.; Kaspar, D.; Gomez, C.; Bormann, C. Problem Statement and Requirements for 6LoWPAN Routing. draft-ietf-6lowpan-routing-requirements-04. July 2009.

[5] Chowdhury, A. H. et al. "Route-over vs Mesh-under Routing in 6LoWPAN", IWCMC '09, June 2009.

[6] Blip. Available online: http://smote.cs.berkeley.edu:8000/tracenv/wiki/blip (accessed on 30 June 2010).

[7] Tavakoli, A.; Dawson-Haggerty, S.; Hui, J.; Culler, D. HYDRO: A Hybrid Routing Protocol for Lossy and Low Power Networks. draft-tavakoli-hydro-01.

[8] 6loWPAN IETF Working Group. Web page: http://datatracker.ietf.org/wg/6lowpan/charter/ (accessed on 30 June 2010).

[9] Crossbow Technology Inc. TelosB Datasheet: http://www.willow.co.uk/TelosB_Datasheet.pdf (accessed on 30 June 2010).

[10] Scheers, B.; Mess, W.; Lauwens, B. Developments on an IEEE 802.15.4-based wireless sensor network. Journal of Telecommunications and Information Technology, pp. 46-53, 2008.

Dependencias estadísticas en servicios de vídeo de alta calidad en Internet

Ana Lobo, Roberto García, Xabiel G. Pañeda, David Melendi, Sergio Cabrero, Victor G. Garcia
Departamento de Informática,
Universidad de Oviedo
Campus de Viesques, sn, 33204, Gijón-Asturias, España.
{loboana, garciaroberto, xabiel, melendi, cabrerosergio, victor}uniovi.es

***Resumen*- En este artículo se propone un modelo de un servicio real de vídeo bajo demanda en Internet (LNE TV, http://tv.lne.es). El modelo considera tanto el comportamiento del usuario como las características del tráfico intercambiado entre el servidor y los clientes del sistema. Para caracterizar las interacciones de los usuarios se han analizado más de 300.000 peticiones de, aproximadamente, 1.500 vídeos en el sistema real. Como mejora a otros trabajos anteriores, el modelo considera la existencia de dependencias estadísticas en las interacciones del usuario, ya que tiene en cuenta las distribuciones estadísticas individuales y la estructura de correlación entre las mismas. Otra de las mejoras que presenta el modelo diseñado es la transmisión de audio y vídeo de alta calidad, teniendo en cuenta la creciente demanda de este tipo de contenidos. Los resultados de los experimentos realizados han permitido validar el modelo implementado.**

***Palabras Clave*- Vídeo bajo demanda (*VoD*), sistemas multimedia (*multimedia systems*), aproximación estadística (*stochastic approximation*), modelado del usuario (*user modeling*)**

I. INTRODUCCIÓN

Los sistemas de vídeo bajo demanda permiten al usuario seleccionar y reproducir los contenidos solicitados en el momento en que se quieran visualizar. Esta descripción conceptual tan simple esconde una complejidad de implementación cuando los contenidos a visualizar deben transmitirse a través de la red provenientes de servidores localizados en diferentes puntos la misma. Los servicios de audio y vídeo en Internet son cada vez más populares y los usuarios demandan contenidos de mayor calidad. Estas circunstancias, unidas a los grandes volúmenes de tráfico que soportan las actuales redes de comunicaciones, pueden dar lugar a situaciones problemáticas que afectan a su rendimiento y al del resto de aplicaciones que comparten con ellos la red.

La utilización de modelos o de generadores de carga precisos constituye una herramienta fundamental a la hora de determinar el rendimiento de los nuevos servicios en las redes de comunicaciones. Un modelo preciso del servicio multimedia permitiría evaluar no solamente las prestaciones del servicio modelado, sino también la influencia que su incorporación tiene sobre la red de datos y el resto de servicios que ya están implantados.

El objetivo de este artículo es la implementación de un modelo de un servicio de vídeo bajo demanda con contenidos de alta calidad. Una vez validado, el modelo permitirá la evaluación de prestaciones del servicio multimedia ante diferentes configuraciones tanto del servicio modelado como de la red de comunicaciones. Para la implementación del modelo se han tenido en cuenta todas las interacciones del usuario con el sistema, los flujos de datos intercambiados entre clientes y servidor, así como los protocolos encargados del control y la transmisión del tráfico multimedia.

Como paso previo al diseño del modelo se han capturado datos para caracterizar el comportamiento de los usuarios en un servicio multimedia real. El servicio analizado es LNE TV (http://tv.lne.es), que constituye la sección multimedia del periódico digital La Nueva España (http://www.lne.es). El análisis se ha realizado examinando más de 300.000 peticiones sobre, aproximadamente, 1.500 vídeos del servicio. Se trata de un servicio comercial y de entretenimiento, de libre acceso a todo tipo de usuarios, que se diferencia claramente de otros trabajos de investigación en este campo, centrados en entornos educacionales, en los que el comportamiento de los usuarios estaba claramente condicionado por la consecución de unos objetivos predeterminados.

Por otra parte, el análisis realizado no se ha limitado a encontrar la distribución estadística que mejor se ajusta a los datos empíricos observados. A diferencia de otros trabajos revisados en este campo [1-6], se ha tenido en cuenta la correlación entre las diferentes interacciones para estudiar sus dependencias, generando distribuciones multivariante y mejorando así la precisión de los modelos desarrollados.

Para la caracterización del tráfico intercambiado entre clientes y servidor de vídeo se ha monitorizado la transmisión de audio y vídeo de alta calidad a partir de experimentos de laboratorio. Además de los volúmenes de audio y vídeo intercambiados se ha caracterizado la dinámica de los protocolos RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol) y RTSP (Real-Time Streaming Protocol) para el intercambio de tráfico multimedia.

Con respecto a otros modelos existentes, nuestra contribución ha sido considerar la existencia de dependencias estadísticas en las interacciones del usuario con el servicio de vídeo multimedia. De esta forma, se mejora la caracterización del comportamiento del usuario en el modelo del cliente, ya que tiene en cuenta las distribuciones estadísticas individuales de las variables implicadas y proporciona una estructura de correlación entre las mismas. Asimismo, el modelo diseñado permite representar la transmisión de contenidos de alta calidad, con lo que se adapta a la demanda cada vez más creciente de este tipo de contenidos por parte de los usuarios de Internet.

Este artículo está organizado de la siguiente forma. En el apartado II se muestra el estado del arte. Las secciones III y IV están dedicadas a presentar el caso de estudio y describir los análisis del comportamiento del usuario y de la carga del servidor. Estos análisis permiten, en el apartado V, la realización de un modelo del sistema. Los resultados del modelo se muestran en la sección VI y las conclusiones y trabajos futuros en la sección VII.

II. TRABAJOS RELACIONADOS

El número de servicios de vídeo bajo demanda ofrecidos en Internet ha ido creciendo en los últimos años. Este hecho ha llevado a los investigadores a trabajar cada vez más en analizar algunos de sus aspectos, como el comportamiento del usuario, las interacciones de éste con el sistema y la carga de tráfico ofrecida por el servidor. Se revisan aquí algunos de estos trabajos relacionados con el que se presenta en este artículo.

En [1] y [2] se analizan el comportamiento del usuario y sus interacciones cuando el servidor ofrece contenidos relativos a una única temática. [1] trabaja en un entorno educacional, mientras que [2] se mueve en el mundo del deporte y la música, añadiendo además interacciones especiales como el *bookmarking* (enlaces directos a puntos más interesantes del vídeo). Estas últimas interacciones y el tipo de contenidos ofrecidos condicionan claramente el comportamiento del usuario, por lo que los resultados obtenidos en estos trabajos no serían extrapolables a servicios más generales. Sin embargo, el servicio analizado en este artículo ofrece una gran variedad de contenidos y duraciones de los vídeos, lo que refleja un comportamiento del usuario más real, no condicionado por los contenidos.

En [3] se trabaja con vídeos de baja calidad y [4] analiza el tráfico propietario *RealMedia*. Sin embargo, el trabajo presentado aquí analiza vídeos de alta calidad (superior a 1Mbps), que es a lo que tienden los contenidos ofrecidos en Internet, enviados por el servidor streaming mediante los protocolos estándares RTP y RTCP.

En ninguno de los trabajos revisados se tienen en cuenta las posibles dependencias estadísticas que pueden existir entre las interacciones del usuario, sino que se modelan éstas con distribuciones independientes entre sí. Estas consideraciones pueden ser erróneas y llevar a resultados imprecisos en la simulación de los modelos implementados [5,6]. Sin embargo, [7] demuestra que efectivamente sí que existen dichas dependencias, las cuales serán integradas en el modelo que va a ser descrito en el presente artículo, mediante el método de las cópulas. Las cópulas son funciones que permiten crear distribuciones multivariantes, a partir de las distribuciones univariantes y los correspondientes coeficientes de correlación. Estas funciones ya han sido utilizadas en otros campos de investigación como el análisis de los riesgos financieros [8] o los efectos de los fenómenos hidrológicos [9], aunque no en el campo de los servicios streaming, hasta donde se ha podido comprobar.

III. ANÁLISIS DEL COMPORTAMIENTO DEL USUARIO

En este artículo se presenta el modelo implementado a partir del análisis realizado del servicio de vídeo bajo demanda de La Nueva España Digital (http://tv.lne.es). Este servicio lleva en funcionamiento desde el año 2001 y su número de visitas ha ido creciendo considerablemente año a año. Concretamente, para realizar el análisis se han examinado más de 300.000 peticiones. A continuación, se resume el comportamiento identificado en las mismas.

En cada sesión o acceso al servicio el usuario puede realizar una o varias reproducciones. Cada una de las reproducciones de una sesión comienza con la interacción *play* del usuario y finaliza cuando se termine de enviar el vídeo o se produzca la interacción *stop*.

Durante cada reproducción el usuario puede realizar interacciones intermedias (pausas, avances, retrocesos, *play* y *stop*).

El estudio realizado se divide en dos partes. Por un lado, se realiza el análisis de cada sesión de un usuario, caracterizando su comportamiento en cuanto al número de reproducciones realizadas por sesión y al tiempo que deja pasar entre reproducción y reproducción. Por otro lado, se analiza cada reproducción y las diferentes interacciones realizadas durante ésta (duración de la reproducción, número de pausas, duración de las pausas, número de avances y de retrocesos, duración de los avances y de los retrocesos).

El estudio se ha hecho además diferenciando entre vídeos cortos y vídeos largos. La diferenciación se realizó gracias a la observación de un comportamiento diferente de los usuarios según la duración del vídeo sea menor o mayor que 5 min. Los vídeos de duración menor que 5 min (cortos) son bastante más demandados que los vídeos de duración mayor que 5 min (largos). Además, los vídeos cortos se suelen reproducir completos con mayor frecuencia que los vídeos largos.

El modelo del cliente que será descrito en apartados posteriores tiene en cuenta, por tanto, todos los parámetros comentados anteriormente: caracterización de la sesión (con una o más reproducciones), caracterización de la reproducción (con todas las interacciones posibles) y la distinción de todo el análisis según la duración del vídeo.

La caracterización de todos estos parámetros se hizo en [7] mediante funciones de distribución estadísticas estimadas a partir de los datos reales. Para ello, se utilizaron estimadores MLE (Maximum Likelihood Estimators) [10] y, con el fin de determinar la distribución que mejor se ajusta, de entre las familias paramétricas de distribuciones consideradas (beta, exponencial, pareto, normal, lognormal, gamma, uniforme, Weibull, ley Zipf), a los datos reales y validar así los resultados, se realizó el test de Kolmogorov-Smirnov (K-S) [10] con nivel de confianza del 95%. De esta manera, se comparan las distribuciones de los datos reales y los datos simulados, siendo la mejor elección la que menor valor estadístico del test K-S obtenga.

Se resumen aquí los resultados obtenidos de esta caracterización que, posteriormente, serán validados en el modelo.

Por un lado, del análisis de las sesiones resulta que las distribuciones estadísticas que mejor se ajustan al número de reproducciones por sesión y al tiempo entre reproducciones son la Zipf-like y la lognormal, respectivamente.

Por otro lado, en cuanto a las interacciones realizadas por el usuario durante cada reproducción, se determinan tanto las distribuciones estadísticas que siguen los valores reales, como el coeficiente de correlación existente entre los valores de las interacciones y la duración del vídeo. Esto último es la principal contribución de este trabajo, ya que todos los trabajos revisados sobre los sistemas multimedia y el análisis de las interacciones del usuario en una reproducción

caracterizan cada una de éstas mediante una distribución univariante. Es decir, que no se tiene en cuenta la dependencia que pueden tener los valores de estas interacciones respecto a la duración del vídeo en cuestión. Los resultados de [7] demuestran que efectivamente sí que algunas interacciones pueden tener una estructura dependiente de la duración del vídeo.

Los resultados de las distribuciones estimadas, los parámetros MLE y los coeficientes de correlación obtenidos para todas las interacciones del usuario, distinguiendo entre vídeos cortos y largos, se detallan completamente en [7].

IV. ANÁLISIS DE LA CARGA DEL SERVIDOR: VÍDEOS DE ALTA CALIDAD

Para terminar con la caracterización del sistema de vídeo bajo demanda, se analiza la carga de tráfico multimedia enviada por el servidor. Para ello, se van a utilizar vídeos de alta calidad (superior a 1Mbps) transmitidos mediante el servidor Darwin Streaming Server (DSS) [11].

En los siguientes apartados se detallan los protocolos utilizados durante la comunicación, el formato de los vídeos analizados, así como la caracterización de todo el tráfico de audio y vídeo enviado.

A. Comunicación streaming

El servidor streaming DSS utiliza los protocolos estándar RTP/RTCP y RTSP para enviar tráfico multimedia a los clientes a través de la red. El protocolo RTSP (Real-Time Streaming Protocol) controla la sesión streaming, permitiendo al cliente interaccionar con el servidor y así poder solicitar la reproducción o pausa de un vídeo, hacer saltos hacia adelante y hacia atrás y terminar la reproducción. El envío y monitorización del tráfico de audio y vídeo se hace mediante los protocolos RTP (Real-time Transport protocol) y RTCP (RTP Control Protocol), respectivamente. RTP utiliza normalmente el protocolo de transporte UDP para el envío de los datos de audio y vídeo. Cada flujo de datos tiene asociado un flujo de paquetes de control enviados mediante RTCP. Estos paquetes permiten monitorizar la calidad del servicio mediante, por ejemplo, envíos de informes sobre los datos recibidos por parte del cliente (*Receiver Reports*, RR) o informes sobre los datos enviados por parte del servidor (Sender Reports, SR).

B. Vídeos de alta calidad

Con el objetivo de simular en el modelo el envío de vídeos de alta calidad, para estudiar el impacto que tendrá esta carga de tráfico en la red, se caracterizó un mismo vídeo codificado en tres calidades: 1Mbps, 2.5 Mbps y 8.2 Mbps. Se ha utilizado el códec H.264 para codificar el vídeo y formato AAC para el audio. En la Tabla 1 se muestra la información más representativa de la codificación de las tres calidades para un vídeo de duración 123 segundos.

Calidad y parámetros	Audio	Vídeo
1Mbps:		
Nº paquetes	3799 paq.	9173 paq.
Tam. medio paq.	1064.8 bytes	1165.4 bytes
Tasa bit media	258 kbps	687 Kbps
2.5Mbps:		
Nº paquetes	3769 paq.	25113 paq.
Tam. medio paq.	1063.6 bytes	1353.8 bytes
Tasa bit media	258 kbps	2239 Kbps
8.2Mbps:		
Nº paquetes	3652 paq.	84925 paq.
Tam. medio paq.	1062.9 bytes	1373.3 bytes
Tasa bit media	258 kbps	7979 Kbps

Tabla 1. Información del vídeo codificado en tres calidades.

C. Captura del tráfico

Para poder analizar la carga de tráfico generada en la red con el envío de cada vídeo, se transmite cada uno de ellos desde el servidor DSS a un único cliente, ambos situados en la misma red local para tener una situación ideal. Mediante el analizador de protocolos Wireshark se capturan todos los paquetes introducidos en la red durante cada comunicación entre cliente y servidor. De esta manera, se puede analizar el comportamiento de los protocolos RTSP, RTP y RTCP, identificando los paquetes de control de la sesión, los paquetes de cada flujo de datos y los que monitorizan cada uno de estos flujos. Con el objetivo de implementar posteriormente el modelo del servidor, se caracteriza la transmisión de cada uno de estos paquetes.

D. Caracterización del tráfico RTSP

Independientemente de la calidad del vídeo a enviar, la comunicación entre cliente y servidor comienza con el establecimiento de una conexión TCP para el envío de los paquetes de control RTSP.

Cliente y servidor mantienen una negociación inicial durante la que se intercambian 5 parejas de paquetes. Estos son 5 peticiones por parte del cliente (OPTIONS, DESCRIBE, SETUP, SETUP, PLAY) y las correspondientes respuestas del servidor (REPLY). Esta negociación sirve para que, entre otras cosas, el cliente obtenga información sobre los datos que va a recibir, así como para establecer los parámetros de las sesiones UDP mediante las cuales RTP enviará posteriormente cada flujo de datos, y finalmente para comenzar la reproducción.

Durante el transcurso de la reproducción el cliente puede solicitar una pausa, un avance o un retroceso de ésta, mediante los mensajes RTSP correspondientes.

Una vez se dé por finalizada la reproducción, bien porque se termina de enviar el vídeo, o bien porque el cliente solicita su interrupción, la desconexión final se hace mediante el intercambio de un mensaje TEARDOWN (cliente) y el correspondiente REPLY del servidor.

E. Caracterización del tráfico RTCP

Por cada flujo de datos audio o vídeo RTP se establece una sesión RTCP que monitoriza el envío de dichos datos. La caracterización de dichas sesiones RTCP se resume a continuación.

Una vez solicitado el PLAY RTSP comienza la transmisión de paquetes de audio y vídeo vía RTP. Justo a continuación de enviar el primer paquete de datos de cada flujo, el servidor envía sendos paquetes RTCP (uno por flujo) identificados como SR (*Sender Report*) con información de los datos enviados hasta el momento (un solo paquete en este caso). Durante el resto de la comunicación se sucederán los paquetes SR de forma periódica cada aproximadamente 7 segundos. Por otro lado, el cliente también envía sus paquetes RTCP de control. Concretamente, a los aproximadamente 2 segundos del PLAY, envía un RR (*Receiver Report*) por cada flujo con información de los paquetes de datos recibidos hasta el momento. Los tiempos transcurridos entre la transmisión de cada uno de los sucesivos RR no son constantes, pero si fueron caracterizados mediante una distribución estadística.

La distribución que mejor se ajusta a los valores de estos tiempos es una Weibull con parámetros MLE forma = 7.3405, escala = 5.3382. Su valor medio es de 4.96 seg. El test K-S valida esta estimación con un valor estadístico de 0.0765 y un p-valor de 0.7003.

Concatenado con cada RR y cada SR se añade también un paquete SDES (*Source Description*) que identifica la fuente que generó ambos paquetes RTCP. El tamaño de todos estos paquetes es constante: 84 bytes para el SR+SDES y 60 bytes para el RR+SDES.

Tras el TEARDOWN RTSP cliente y servidor también terminan sus sesiones RTCP enviando sus últimos paquetes RR y SR. Concatenado con los últimos RR se añade también un paquete BYE que indica que ese cliente ya no va a permanecer más activo.

F. Caracterización del tráfico RTP

Por último, se caracteriza RTP-UDP, tráfico que supone la mayoría de la carga introducida en la red. Hay que diferenciar una sesión RTP para cada flujo de datos, audio y vídeo. La diferenciación se puede hacer también gracias a que los paquetes de cada flujo llevan diferente identificador PT (*Payload Type*) en la cabecera del paquete RTP.

En las Fig. 1 y 2 se muestran los consumos de ancho de banda de audio y vídeo para las calidades analizadas. En ellas se pueden distinguir diferentes fases. En el caso del audio se observa una primera fase que dura unos 5 segundos, durante la cual la tasa de bit mantiene una media aproximada de 30 Kbps. A continuación, esta tasa sufre una brusca subida durante unos 10 segundos y finalmente se estabiliza en torno a los 270 Kbps. Se puede decir que las tres calidades tienen un comportamiento muy parecido en este caso, ya que la codificación del audio se hace igual para las tres. En cuanto al vídeo, se distinguen dos fases. La primera de ellas dura unos 6 segundos, con tasas en torno a 400 Kbps. A continuación, la tasa va subiendo hasta alcanzar valores muy diferentes según la calidad: hasta unos 850 Kbps para la calidad más baja, 2.7 Mbps para la media y 9 Mbps para la más alta.

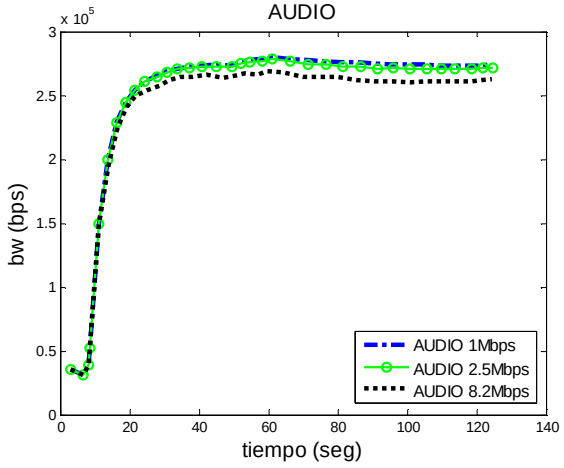


Fig. 1. Consumo de ancho de banda de audio.

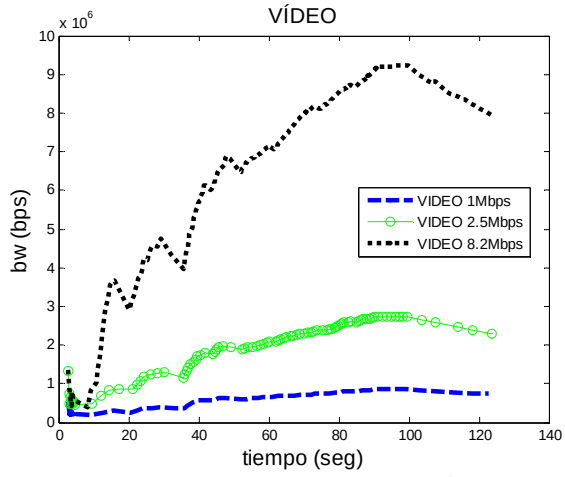


Fig. 2. Consumo de ancho de banda de vídeo.

Calidad y fases	Audio		Vídeo	
1Mbps:	**Media**	**Desv. Típ.**	**Media**	**Desv. Tip.**
Fase 1				
Tam. paq.	1392 bytes	45.5 byte	462.4 bytes	642.5 byte
Tpo. entre paq	0.375 seg	0.064 seg	0.030 seg	0.039 seg
Fase 2				
Tam. paq.	903 bytes	69.1 byte	1179.3 bytes	467.6 byte
Tpo. entre paq	0.021 seg	0.029 seg	0.013 seg	0.027 seg
Fase 3				
Tam. paq.	1091 bytes	299.1 byt		
Tpo. entre paq	0.033 seg	0.034 seg		
2.5Mbps:				
Fase 1				
Tam. paq.	1392 bytes	45.5 byte	794.1 bytes	699.1 byte
Tpo. entre paq	0.375 seg	0.064 seg	0.020 seg	0.035 seg
Fase 2				
Tam. paq.	903 bytes	69.4 byte	1359.9 bytes	292.1 byte
Tpo. entre paq	0.021 seg	0.030 seg	0.005 seg	0.017 seg
Fase 3				
Tam. paq.	1090 bytes	299.2 byt		
Tpo. entre paq	0.033 seg	0.035 seg		
8.2Mbps:				
Fase 1				
Tam. paq.	1392 bytes	45.5 byte	546.2 bytes	627.1 byte
Tpo. entre paq	0.375 seg	0.064 seg	0.014 seg	0.031 seg
Fase 2				
Tam. paq.	902 bytes	69.9 byte	1377.1 bytes	297 bytes
Tpo. entre paq	0.022 seg	0.030 seg	0.001 seg	0.009 seg
Fase 3				
Tam. paq.	1089 bytes	298.9 byt		
Tpo. entre paq	0.034 seg	0.037 seg		

Tabla 2. Análisis por calidades y fases de audio y vídeo.

En la Tabla 2 se muestra un resumen de los tamaños de paquetes y tiempos entre paquetes enviados para cada flujo durante cada fase. Los tamaños no incluyen las cabeceras Ethernet, IP y UDP (42 bytes), sólo el tamaño del paquete RTP.

F.1. Caracterización de los paquetes de audio

Habiendo diferenciado RTP de audio y RTP de vídeo, mediante las diferentes sesiones RTP y mediante el campo PT de sus cabeceras, se procede a la caracterización de cada tráfico por separado. En ambos casos es necesario caracterizar tanto el tamaño de los paquetes como el tiempo entre éstos, ya que ambos parámetros son variables. Se han utilizado estimadores MLE para obtener las distribuciones estadísticas que mejor se ajusten a los parámetros reales.

En cuanto al audio, se han analizado las tres fases presentadas en el apartado anterior por separado. La primera fase es muy corta y sólo contiene 16 paquetes a analizar. Dada la poca cantidad de datos y que, tanto el tamaño como el tiempo entre paquetes son parecidos para todos los paquetes, esta fase queda caracterizada mediante las medias presentadas en la Tabla 2.

Para las dos fases siguientes ya se dispone de muchos más datos para estimar las distribuciones correspondientes. En la Fig. 3 se puede observar por ejemplo la CDF (Cumulative Distribution Function) para los tamaños medidos durante la segunda fase de la calidad más baja (1Mbps). La distribución estimada en este caso sería una

Weibull con parámetros MLE forma = 14.621 y escala = 934.1841. El test K-S valida esta estimación con un valor estadístico de 0.0710 y un p-valor de 0.12. Las distribuciones estimadas para los tamaños en esta misma segunda fase para las otras dos calidades son también Weibull con parámetros parecidos. En la tercera y última fase los valores de los tamaños de las tres calidades también se estiman con las mismas distribuciones y parámetros parecidos. Pero, en este caso, como se puede ver en la Fig. 4, se observan dos distribuciones: la primera de ellas hasta un máximo de 1100 bytes y la segunda hasta 1450 bytes. Estas dos distribuciones estimadas y sus parámetros son:

- Lognormal, μ=6.6616, σ=0.0578, 49%, K-S=0.0582, p-valor=0.0101
- Weibull, forma=32.6818, escala=1397.0818, 51%, K-S=0.0338, p-valor=0.2859

La caracterización de los tiempos entre paquetes en las fases 2 y 3 se hace más compleja porque se obtienen resultados diferentes para cada calidad y se necesitan al menos dos distribuciones distintas para caracterizar cada caso. En la Tabla 3 se resumen todas estas distribuciones estimadas, así como sus parámetros MLE y el porcentaje porc. de valores caracterizados con la primera distribución estimada.

F.2. Caracterización de los paquetes de video

En cuanto al vídeo, se hace un análisis parecido, pero esta vez dividido en dos fases (Fig. 2).

El análisis de los tiempos entre paquetes lleva a resultados parecidos a los de audio, con dos o tres distribuciones en cada fase para cada calidad.

A la hora de caracterizar los tamaños de los paquetes de vídeo se observó que había una mayoría de paquetes de tamaño 1450 bytes. De esta manera, se identificó que si el tamaño del frame era muy grande, se dividía en sucesivos paquetes, todos con el mimo timestamp, ya que representaban el mismo instante de la reproducción. Los primeros paquetes del frame eran de 1450 bytes y el último de un valor menor, para completar el tamaño total del frame. La división en 1450 se considera lógica, ya que sumándole los 42 bytes de cabeceras, dan un total de 1492 bytes, justo en el límite de los 1500 bytes máximos de la MTU (Maximum Transfer Unit) de Ethernet. Debido a este razonamiento se decidió caracterizar los tamaños de los frames, en lugar de los paquetes. Además, en la codificación del vídeo según H.264 se distinguen dos tipos de frames, I y P. Esta identificación se hizo gracias a un analizador de H.264 (H264Visa). Por tanto, es necesario identificar la secuencia de frames I y P y caracterizar el tamaño de los frames de cada tipo.

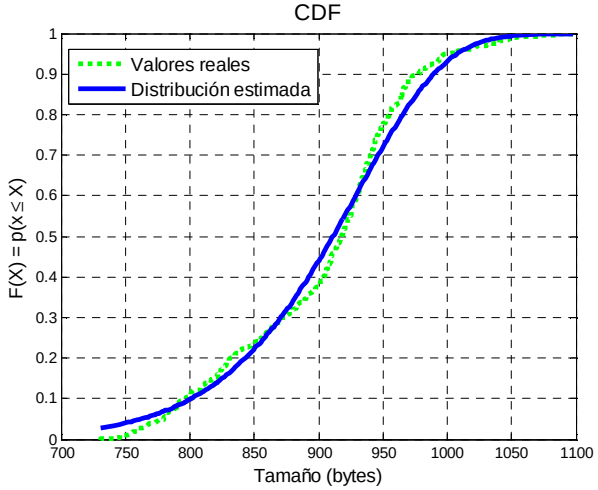


Fig. 3. Tamaños paquetes de audio, calidad 1Mbps, Fase 2.

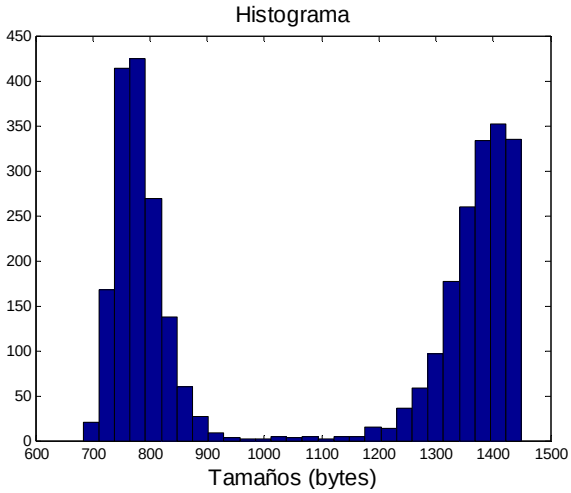


Fig. 4. Tamaños paquetes de audio, calidad 1Mbps, Fase 3.

Fase 2	**Fase 3**
1Mbps	**1Mbps**
Distribución: Lognorm. + Weibull.	Distribución: Lognorm. + Lognorm.
Parámetros: μ_1 = -10.1255	Parámetros: μ_1 = -9.6648
σ_1 = 0.54899	σ_1 = 0.78875
$form_2$ = 12.7144	μ_2 = -2.7098
esc_2 = 0.064331	σ_2 = 0.15371
porc. = 65.57%	porc. = 51.55
K-S_1 = 0.1278, p-v_1= 0.005	K-S_1 = 0.0996, p-v_1= 1.1e^{-7}
K-S_2 = 0.1587, p-v_2= 0.015	K-S_2 = 0.1143, p-v_2= 2.2e^{-9}
2.5Mbps	**2.5Mbps**
Distribución: Exp. + Weibull	Distribución: Weibull + Lognorm.
Parámetros: μ_1 = 0.000074	Parámetros: $form_1$ = 0.87292
	esc_1 = 0.00018078
$form_2$ = 12.1519	μ_2 = -2.7
esc_2 = 0.064496	σ_2 = 0.16475
porc. = 65.7%	porc. = 51.7
K-S_1 = 0.2017, p-v_1= 6.1e^{-7}	K-S_1 = 0.1282, p-v_1= 2.5e^{-12}
K-S_2 = 0.1746, p-v_2= 0.0054	K-S_2 = 0.1046, p-v_2= 7.5e^{-8}
8.2Mbps	**8.2Mbps**
Distribución: Lognorm. + Weibull.	Distribución: Weibull + Lognorm.
Parámetros: μ_1 = -9.4171	Parámetros: $form_1$ = 0.65184
σ_1 = 1.3379	esc_1 = 0.0006093
$form_2$ = 14.5144	μ_2 = -2.6727
esc_2 = 0.064678	σ_2 = 0.17921
porc. = 65.43	porc. = 52.25
K-S_1 = 0.1582, p-v_1= 0.0002	K-S_1 = 0.1027, p-v_1= 6.8e^{-8}
K-S_2 = 0.1230, p-v_2= 0.1093	K-S_2 = 0.1104, p-v_2= 2.6e^{-8}

Tabla 3. Tiempos entre paquetes de audio, Fase 2 y Fase 3: distribuciones y parámetros MLE.

En cuanto a la secuencia de frames I y P, para las calidades de 1Mbps y 2.5Mbps se identifica la siguiente secuencia periódica: I PPPPPPPPPPP I PPPPPPPPPPP I. Por otro lado, en la calidad de 8.2Mbps aparece otra secuencia periódica con 23 frames tipo P seguidos entre cada par de frames tipo I. Sin embargo, esta periodicidad no se cumple siempre, ya que pueden aparecer desde 0 hasta 23 frames tipo P entre cada par de frames tipo I. La caracterización de esta última secuencia se hizo mediante los porcentajes de aparición de cada cantidad de frames tipo P seguidos. Así, se determinan desde un 0.59% para 0, 6, 20, 21 ó 22 frames tipo P, hasta un 45.88% para las 23 frames tipo P, que es la secuencia mayoritaria, con porcentajes variados para muchos otros valores intermedios entre 0 y 23.

Tipo I	Tipo P
1Mbps	**1Mbps**
Distribución: Exponencial	Distribución: Gamma
Parámetros: μ = 12833.5042	Parámetros: form = 0.64789
	esc = 4516.8381
K-S = 0.1102, p-v = 0.1064	K-S = 0.0596, p-v = 0.0002
2.5Mbps	**2.5Mbps**
Distribución: Weibull	Distribución: Gamma
Parámetros: form = 1.0839	Parámetros: form = 0.56293
esc = 17608.4698	esc = 20518.7583
K-S = 0.1234, p-v = 0.0512	K-S = 0.0544, p-v = 0.0009
8.2Mbps	**8.2Mbps**
Distribución: Normal	Distribución: Gamma
Parámetros: μ = 45378.5741	Parámetros: form = 0.62243
σ = 43658.4656	esc = 66782.4584
K-S = 0.1420, p-v = 0.0693	K-S = 0.0961, p-v = $5.2e^{-11}$

Tabla 4. Tamaños de *frames* de vídeo, Fase 2: distribuciones y parámetros MLE.

Respecto a los tamaños de *frames*, se hace la caracterización de cada tipo en cada fase. En la fase 1, los tamaños de cada tipo son bastante uniformes, por lo que se establece su caracterización mediante su media, resultando los siguientes valores para cada calidad:

- 1Mbps – I: 7759 bytes
- 1Mbps – P: 21 bytes
- 2.5Mbps – I: 20159 bytes
- 2.5Mbps – P: 22 bytes
- 8.2Mbps – I: 289 bytes
- 8.2Mbps – P: 258 bytes

Sin embargo, en la fase 2 de nuevo se hace uso de los estimadores MLE para obtener distribuciones estadísticas que se ajusten a los tamaños de cada tipo de *frame*. Los resultados obtenidos para estas distribuciones, según la calidad, se resumen en la Tabla 4.

V. MODELO DEL CLIENTE/SERVIDOR

Una vez analizados todos los elementos del servicio de vídeo bajo demanda, se procede a la implementación de un modelo que represente el funcionamiento del sistema real. Se ha diseñado por un lado, un modelo del cliente en base al comportamiento del usuario analizado, teniendo en cuenta las dependencias entre las interacciones y las duraciones de los vídeos y, por otro lado, un modelo del servidor considerando los datos de la carga de tráfico analizada para ofrecer vídeos de alta calidad. Todos los modelos han sido implementados utilizando el lenguaje de simulación OPNET Modeler [12].

A. Modelo del cliente

El modelo del cliente debe seguir la funcionalidad indicada en apartados anteriores en cuanto a su comportamiento durante cada sesión y cada reproducción de la sesión. Los estados y diagramas de transiciones del modelo diseñado siguen la misma línea que el modelo del cliente presentado en [5]. Las grandes diferencias introducidas en el nuevo modelo que se presenta aquí residen en las dependencias introducidas entre interacciones del usuario y duración de los vídeos y el establecimiento de las sesiones RTP/RTCP para el intercambio de datos con el servidor.

En el inicio de cada reproducción se tienen dos primeros estados que controlan, mediante el intercambio de los mensajes correspondientes, el establecimiento de las conexiones RTSP y RTP/RTCP con el servidor. En el primero de estos estados es donde se tienen en cuenta también los parámetros de las distribuciones marginales univariantes estimadas para cada interacción y para la duración de los vídeos, así como el coeficiente de correlación entre ambos. A partir de todos estos datos, se generan las distribuciones bivariantes utilizando el procedimiento descrito en [13], mediante las cópulas gaussianas [14].

Mediante este procedimiento se generan parejas de valores dependientes, uno de duración del vídeo y otro de la interacción correspondiente, siguiendo ambos su distribución univariante estimada. El problema está en que, para cada vídeo reproducido por el cliente se debería tener una única duración de vídeo y varios valores para las diferentes interacciones. No es posible utilizar entonces todas las parejas de valores dependientes obtenidas según el procedimiento, porque significaría tener varias duraciones del vídeo diferentes para un mismo vídeo. Para solucionar este problema, se hizo lo siguiente:

- Al inicio de cada reproducción se generarán tablas de valores dependientes, según las distribuciones adecuadas, siguiendo el procedimiento de las cópulas gaussianas [13]. Así, tendremos tantas tablas como interacciones del cliente, cada una con dos columnas de valores, una de duraciones de vídeo y otra de las interacciones correspondientes.
- A continuación, se utiliza la duración de vídeo indicada por el servidor para buscar en las tablas el valor que más se le acerque. A partir de éste, se obtiene como valor de la interacción correspondiente la pareja de esa duración de vídeo en la tabla.

De esta manera, se tiene una duración única del vídeo a reproducir, la indicada por el servidor, y varios valores para las diferentes interacciones, cada una dependiente de la duración de vídeo según su determinado coeficiente de correlación.

Una vez establecidas las conexiones, el cliente pasa al estado de reproducción, en el que empieza a recibir los datos de audio/vídeo del servidor, así como a intercambiar paquetes de control (RTSP) y de monitorización de los datos (RTCP). Cuando se termina el envío del vídeo o el cliente solicita su interrupción, se pasa al estado final en el que se cierran todas las conexiones establecidas y se implementa la posibilidad de lanzar una nueva reproducción o terminar la sesión.

B. Modelo del servidor

El modelo del servidor de vídeo bajo demanda debe seguir la funcionalidad indicada en apartados anteriores en cuanto a la carga de tráfico caracterizada para vídeos de alta calidad. Los estados y diagramas de transiciones del modelo diseñado siguen la misma línea que el modelo del servidor presentado en [5]. Las grandes diferencias introducidas en el modelo que se presenta aquí residen en la nueva caracterización de los vídeos de alta calidad, en cuanto a tamaños y tiempos entre paquetes de datos (Tablas 3 y 4), haciendo distinción entre *frames* tipo I y tipo P en el caso del vídeo, y en el intercambio de datos y control mediante los protocolos RTP/RTCP.

De esta manera, el servidor se mantiene a la espera de peticiones de clientes para establecer nuevas conexiones RTSP y RTP/RTCP. Cuando esto ocurre se genera un nuevo proceso esclavo que controlará la reproducción de ese cliente, mientras que el servidor vuelve al estado de esperar nuevas peticiones de clientes. Cada proceso esclavo debe controlar tanto el envío de audio y vídeo al cliente mediante

RTP, como el intercambio de paquetes RTCP para la monitorización de ese envío de datos, según la caracterización presentada en el apartado IV. Cuando el envío del vídeo finaliza o el cliente solicita su interrupción, el proceso esclavo cierra todas las conexiones y es destruido para optimizar la ejecución del modelo.

El principal problema que se encontró a la hora de implementar el envío de los datos mediante RTP fue la sincronización de los dos flujos de información, ya que ambos van en sesiones RTP independientes. Para facilitar esta sincronización, en la cabecera de RTP los paquetes de datos llevan su *timestamp*, el cual indica el instante de presentación de los datos. Sin embargo, no se puede usar directamente este dato para sincronizar los flujos porque realmente no se incrementa según el tiempo real, sino según la tasa de muestreo de cada flujo. Para solucionar este problema y poder relacionar el número de muestras indicado en cada *timestamp* RTP con el instante de reproducción real, los paquetes SR (*Sender Report*) enviados por el servidor llevan tanto un *timestamp* RTP como un *timestamp* NTP (*Network Time Protocol*), representando ambos el instante de generación de ese SR. Los NTP dan información absoluta del tiempo según el RFC1305 [15]. Así, haciendo uso de estos *timestamps* y aplicando el método detallado en [16] se puede obtener el instante de reproducción real T de un paquete RTP, según la fórmula siguiente:

$$T = T_{SR}(i+1) + \frac{T_{SR}(i+1) - T_{SR}(i)}{M_{SR}(i+1) - M_{SR}(i)}(M - M_{SR}(i+1)) \quad (1)$$

En (1) T_{SR} indica el *timestamp* NTP de los SR i e i+1 (SR enviado anterior y posteriormente al paquete analizado, respectivamente). Por otro lado, M_{SR} indica los *timestamps* RTP correspondientes a esos SR y M el correspondiente al paquete analizado.

VI. RESULTADOS

Con el objetivo de validar el modelo de vídeo bajo demanda implementado, se ha simulado un escenario con 20 clientes y un servidor. En la Fig. 5 y la Tabla 5 se muestran algunos resultados que validan el comportamiento del cliente. La Fig. 5 representa los valores obtenidos en el modelo para la duración de los avances en vídeos cortos y su distribución estimada, cuyos parámetros MLE se pueden validar con los de [7] para esta interacción. Se han hecho validaciones similares para el resto de interacciones, pero no se incluyen aquí por el volumen de información que supondría añadir todas ellas. En la Tabla 5 se muestran los coeficientes de correlación entre cada interacción del cliente y la duración del vídeo obtenidos en la generación de tablas iniciales, los cuales se pueden validar con los valores reales obtenidos en [7].

La validación del tráfico enviado por el servidor se puede hacer gracias a las Fig. 6, 7, y 8. La Fig. 6 muestra los tamaños de los paquetes de audio obtenidos en el modelo para vídeos de calidad 1Mbps durante la fase 3, cuyos resultados pueden ser validados con las medidas reales mostradas en la Fig. 4. Por otro lado, las Fig. 7 y 8 muestran el consumo de ancho de banda de audio y vídeo, según la calidad en cada cliente del modelo, superpuesto al real mostrado en las Fig. 1 y 2, pudiendo así validar éste.

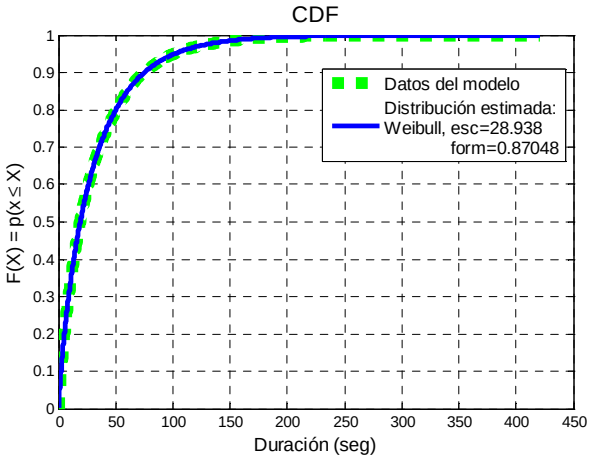


Fig. 5. Duración de avances para vídeos cortos en el modelo.

Interacción	Videos Cortos	Vídeos Largos
Número pausas		
Coef. Real	0.0980	0.4619
Coef. Simulado	0.0721	0.4191
Duración pausas		
Coef. Real	0.1304	0.2372
Coef. Simulado	0.1369	0.2322
Número avances		
Coef. Real	0.0088	0.2850
Coef. Simulado	0.0068	0.2618
Duración avances		
Coef. Real	0.2689	0.3067
Coef. Simulado	0.2629	0.3118
Número retrocesos		
Coef. Real	0.0142	0.3322
Coef. Simulado	0.0181	0.3152
Duración retrocesos		
Coef. Real	0.1486	0.2894
Coef. Simulado	0.1489	0.2889

Tabla 5. Coef. correlación entre interacciones y duraciones de vídeo de las tablas generadas en el modelo

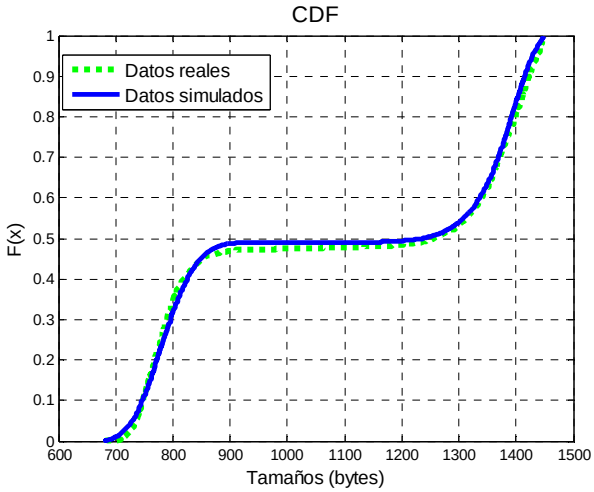


Fig. 6. Tam. paq. de audio, calidad 1Mbps, Fase 3 con datos simulados.

VII. CONCLUSIONES Y TRABAJOS FUTUROS

El objetivo de este trabajo es construir un modelo lo más realista posible de un sistema de vídeo bajo demanda. Para ello, se analizaron ficheros log del servidor de un sistema real (http://tv.lne.es), con el fin de caracterizar el comportamiento de los clientes. En este comportamiento se demostró que existían dependencias entre las diferentes interacciones del usuario y la duración del vídeo reproducido. Estas dependen-

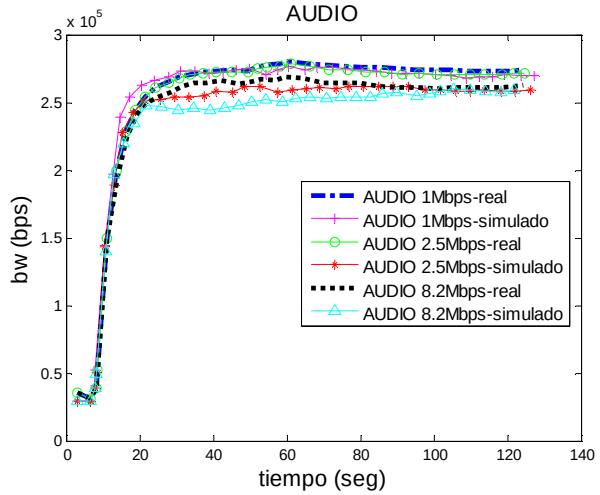


Fig. 7. Consumo de ancho de banda de audio por cliente en el modelo.

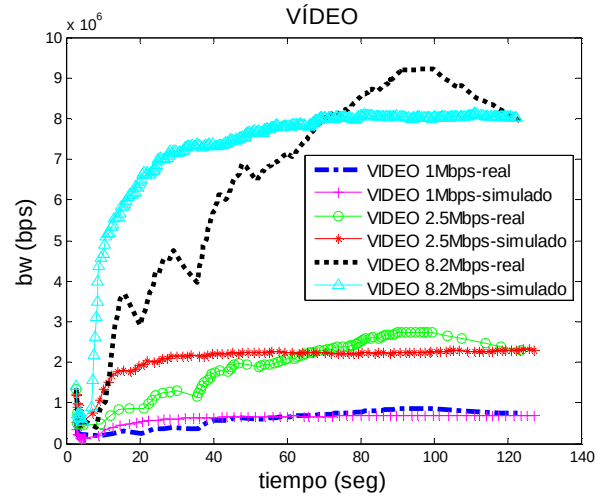


Fig. 8. Consumo de ancho de banda de vídeo por cliente en el modelo.

cias fueron introducidas en el modelo gracias al método de las cópulas gaussianas, creando así simulaciones más representativas que en trabajos anteriores, en los que se suponían todas las variables independientes. Por otro lado, para modelar la carga de tráfico generada por el servidor, se realizaron experimentos de laboratorio transmitiendo vídeos de alta calidad (superior a 1Mbps) desde un servidor streaming DSS a un cliente y se capturó el tráfico recibido por éste para realizar su posterior análisis. El servidor DSS utiliza los protocolos estándares RTSP y RTP/RTCP para el envío y control de los datos. Simular esta carga de tráfico permite adelantarse a la situación del futuro, ya que actualmente no se están ofreciendo estas calidades en servicios bajo demanda reales.

Una vez estudiados los resultados de la simulación del modelo, se puede concluir que éste responde al comportamiento del usuario y carga de tráfico analizadas, por lo que servirá para realizar futuras pruebas. Estas pruebas pueden ser introducir dependencias muy fuertes de las interacciones del usuario respecto a la duración del vídeo, o aumentar el número de clientes considerablemente. Sería interesante ver qué pasaría en estas situaciones con el volumen de tráfico, el coeficiente de autosimilitud de éste o las posibles pérdidas de paquetes, ya que pueden ser detectadas en futuros estudios.

Otra vía de trabajo que se puede considerar es introducir en el modelo del cliente posibles dependencias multivariantes entre todas las variables del sistema.

Por último, se han empezado a estudiar nuevos vídeos y se ha comprobado que el consumo de ancho de banda y sus fases no siguen el mismo patrón que el caracterizado, por lo que será necesario caracterizare e incluir nuevos vídeos en el modelo del servidor.

AGRADECIMIENTOS

Este trabajo ha sido realizado gracias a la colaboración del operador de red *Telecable de Asturias SAU* y al periódico español *La Nueva España*, en el marco del proyecto *MediaXXI* (Ref: FUO-EM-174-07) y el proyecto TSI2007-60474 dentro del Plan Nacional de Investigación.

REFERENCIAS

[1] J. Almeida, J. Krueger, D. Eager, and M. Vernon, “Analysis of educational media server workloads”, in *Proceedings of NOSSDAV*, Port Jefferson, New York, USA, June 2001.

[2] A. Brampton, A. MacQuire, M. Fry, I. A. Rai, N. J. P. Race, and L. Mathy, “Characterising and exploiting workloads of highly interactive video-on-demand”, *Multimedia Systems*, vol. 15, pp. 3-17, 2009.

[3] D. Loguinov, and H. Radha, “Measurement study of low-bit rate internet video streaming”, in *ACM SIGCOMM Internet Measurement Workshop (IMW)*, 2001.

[4] T. Kuang, and C. Williamson, “A measurement study of RealMedia audio/video streaming traffic”, in *Proceedings of SPIE ITCOM*, Boston, MA, July 2002, pp. 68-79.

[5] R. García, X.G. Pañeda, V. García, D. Melendi, and M. Vilas, “Statistical characterization of a real video-on-demand service: user behaviour and streaming-media workload analysis”, *Simulation Modelling Practice and Theory*, vol. 15, pp. 672-689, 2007.

[6] W. Tang, Y. Fu, L. Cherkasova, and A. Vahdat, “Modeling and generating realistic streaming media server workloads”, *Computer Networks*, vol. 51, pp. 336-356, 2007.

[7] R. García, X.G. Pañeda, D. Melendi, and V. García, “Probabilistic analysis and interdependence discovery in the user interactions of a video on demand service”, *Computer Network*, vol. 53, pp. 2038-2049, 2009.

[8] G. Cheng, P. Li, and P. Shi, “A new algorithm based on copulas for VaR valuation with empirical calculations”, *Theoretical computer Science, Elsevier*, vol. 378, pp. 190-197, 2007.

[9] J.-T. Shiau, H.-Y. Wang, and C.-T. Tsai, “Bivariate frequency analysis of floods using copulas”, *Journal of the American Water Resources Association*, vol 42, pp. 1549-1564, 2007.

[10] A.M. Law, W.D. Kelton, *Simulation Modelling and Analysis*, McGraw-Hill International Series, 2000.

[11] Darwin Streaming Server, http://developer.apple.com/opensource/server/streaming/index.html.

[12] OPNET TECHNOLOGIES. OPNET Modeler: Making Networks and Applications Perform. www.opnet.com.

[13] D. Melendi, R. García, X.G. Pañeda, and V. García, “Multivariate distributions for workload generation in video on demand systems”, *Comm. Letters*, vol. 13, pp. 348-350, 2009.

[14] R. Nelsen, *An Introducton to Copulas*. New York: Springer, 1999.

[15] D. Mills, “Network time protocol specification, implementation and analysis,” *RFC 1305*, IETF, Mar. 1992.

[16] C. Kim, K-d. Seo, W. Sung, and S-h. Jung, “Efficient audio/video synchronization method for video telephony system in consumer cellular phones”, *Consumer Electronics, ICCE ’06*, pp. 137-138, 2006.

Análisis del goodput para sistemas IEEE 802.11n basados en AMC de lazo abierto y cerrado

Gabriel Martorell, Felip Riera-Palou y Guillem Femenias
Grupo de Comunicaciones Móviles,
Universitat de les Illes Balears
Ctra. Valldemosa Km 7.5
07122 Palma de Mallorca
{gabriel.martorell, felip.riera, guillem.femenias}@uib.es

***Resumen*—Este artículo presenta un modelo *cross-layer* MAC-PHY semi-analítico que permite evaluar el rendimiento en *goodput* de esquemas adaptativos de lazo abierto y cerrado, en entornos de redes locales inalámbricas basadas en IEEE 802.11n. Sin pérdida de generalidad, se considera el conocido algoritmo de lazo abierto ARF (*Automatic Rate Fallback*) y un algoritmo de lazo cerrado, como es el FLA (*Fast Link Adaptation*) basado en la SNR efectiva exponencial. A diferencia de otros trabajos anteriores, se consideran condiciones de canal no ideales y que los usuarios pueden utilizar diferentes modos de transmisión. Los resultados obtenidos demuestran la precisión del modelo propuesto. Además, se observa una clara superioridad de las técnicas de lazo cerrado respecto a las de lazo abierto para cualquier longitud de paquete, especialmente cuando el número de estaciones en contención en el medio es moderadamente alto.**

***Palabras Clave*—MAC, DCF, acceso básico, AMC, *Fast Link Adaptation*, ARF, IEEE 802.11n, *Cross-layer*.**

I. Introducción

El comité de estándares del IEEE ha publicado recientemente la versión final de la enmienda IEEE 802.11n [1] para redes locales inalámbricas (WLAN). Esta nueva norma, basándose en el uso de múltiples antenas en transmisión y recepción (MIMO-*Multiple-Input Multiple-Output*) en la capa física (PHY), la incorporación de un canal de realimentación entre transmisor y receptor que posibilita el uso de mecanismos adaptativos en lazo cerrado y la utilización de mecanismos de agregación de tramas en la subcapa de control de acceso al medio (MAC- *Medium Access Control*), permite la utilización de tasas de transmisión superiores a las que ofrecen los estándares IEEE 802.11a/g y la satisfacción de requisitos de calidad de servicio (QoS- *Quality of Service*) más exigentes.

En estos sistemas, la adaptación juega un rol importante para contrarrestar la variabilidad temporal del canal inalámbrico. Los mecanismos adaptativos permiten la reconfiguración de los parámetros de sistema para explotar la capacidad disponible mientras se satisfacen determinados requisitos de calidad de servicio. Una de las técnicas de reconfiguración más ampliamente utilizadas es la modulación y codificación adaptativa (AMC- *Adaptive Modulation and Coding*), que selecciona un esquema de codificación y modulación (MCS- *Modulation and Coding Scheme*) adecuado en respuesta a los cambios experimentados en el entorno o en el comportamiento del sistema en términos de probabilidad de error por paquete o retardo de transmisión. En función de la existencia o no de un canal de retorno de control (o de realimentación) entre el receptor (Rx) y el transmisor (Tx), los algoritmos AMC pueden clasificarse en algoritmos de lazo abierto o algoritmos de lazo cerrado. Para las configuraciones de lazo abierto, el transmisor debe decidir el MCS a utilizar sin disponer de información sobre el estado del canal procedente del receptor. Estas técnicas operan, habitualmente, de forma heurística y su tasa de adaptación tiende a ser lenta con respecto a los cambios del canal, por tanto, dificultan el cumplimiento de los requisitos de QoS. En cambio, los mecanismos de lazo cerrado utilizan el canal de retorno para adoptar las decisiones tomadas en el receptor, donde se dispone de información fidedigna sobre el comportamiento del canal y, por tanto, proporcionan una respuesta más precisa a las variaciones rápidas del entorno.

La mayoría de sistemas IEEE 802.11 utilizan la DCF (*Distributed Coordination Function*) en la subcapa MAC y adoptan políticas AMC de lazo abierto tales como ARF (*Automatic Rate Fallback*) [2] y sus variantes (p.e. CARA [3], SARA [4]). Debido a su simplicidad, ARF es el algoritmo en uso más popular, pero su rendimiento disminuye considerablemente en los entornos multiusuario a medida que aumenta el número colisiones (véase por ejemplo, [3], [5], [6], [7]). El esquema DCF no distingue entre errores de transmisión causados por condiciones de canal desfavorables o colisiones y, en consecuencia, cuando el sistema sufre una probabilidad de colisión alta, ARF tiende a utilizar el MCS con la tasa de transmisión más baja aunque las condiciones de canal sean favorables para utilizar modos de transmisión con tasas mucho más elevadas. Para solucionar este problema se han propuesto otras estrategias que requieren de modificaciones en el formato de trama, de otros esquemas de transmisión (p.e. RTS/CTS) o del uso de indicadores de calidad del canal (p.e. indicador de potencia del señal SSIR). En cualquier caso, ninguno de ellos ha sido adoptado ampliamente en los sistemas WLAN actuales.

Estudios recientes han demostrado que, en el contexto de IEEE 802.11n, el uso de algoritmos de lazo cerrado como el de adaptación rápida del enlace (FLA- *Fast Link Adaptation*) ofrecen una importante mejora del *throughput* de capa física [8], [9]. Basándonos en el trabajo de Bianchi [10] y utilizando los modelos de capa física presentados por nuestro grupo en [9], en este artículo presentamos un modelo *cross-layer* MAC-PHY semi-analítico que permite estimar el *goodput* de las redes IEEE 802.11n que utilizan esquemas de adaptación del lazo cerrado o abierto. A diferencia del trabajo de Bianchi, nuestro modelo toma en consideración condiciones de canal no ideales y la posibilidad de utilizar modos de transmisión

diferentes. La contrastación con los resultados de simulación ilustra la alta precisión del modelo propuesto.

II. Visión general del Sistema

A. Descripción de la capa física

Este estudio se centra en la enmienda IEEE 802.11n que utiliza una capa física basada en MIMO-OFDM. La técnica OFDM transforma un canal de banda ancha selectivo en frecuencia en múltiples canales paralelos de banda estrecha frecuencialmente planos, simplificando de esta forma la arquitectura del receptor. Dependiendo de la técnica MIMO utilizada (p.e., codificación de bloque espacio-tiempo (STBC- *Space Time Block Coding*), multiplexación por división espacial (SDM- *Spatial Division Multiplexing*), diversidad de retardo cíclico (CDD- *Cyclic Delay Diversity*) y/o combinaciones de estos), la componente MIMO explota las múltiples antenas en transmisión y recepción para incrementar la capacidad del sistema o su fiabilidad [11].

En el transmisor, los bits de información se codifican utilizando un codificador convolucional de tasa $R = \frac{1}{2}$ con polinomios generadores $[133, 177]$ y posteriormente se perforan a una de las tasas de codificación disponibles $R_m \in \{1/2, 2/3, 3/4, 5/6\}$. De acuerdo con la configuración MIMO seleccionada, los bits obtenidos son demultiplexados en N_s flujos espaciales. Para simplificar la explicación, este artículo se centrará en el estudio de sistemas MIMO 2×2 ($NT = 2$ y $NR = 2$), implicando que los MCSs con $N_s = 1$ y $N_s = 2$ flujos espaciales utilizan STBC [12] y SDM [13], respectivamente. Para cada flujo, los bits codificados se entrelazan y se asignan a símbolos de una de las constelaciones permitidas (BPSK, QPSK, 16-QAM o 64-QAM). Los símbolos obtenidos se introducen a un modulador OFDM convencional, formado por una transformada rápida inversa de Fourier (IFFT- *Inverse Fast Fourier Transform*) y un mecanismo para añadir un intervalo de guarda.

En el receptor, se aplica la decodificación de Alamouti o un detector MMSE (*Minimum Mean Square Error*), en función de si el transmisor utiliza STBC o SDM, respectivamente. En ambos casos, el detector extrae la información *soft* en forma de coeficientes de verosimilitud (LLRs) que, después de los procesos de desentrelazado, pueden ser explotados utilizando un decodificador de Viterbi *soft* [9].

B. Descripción de la capa MAC

La capa MAC del IEEE 802.11 especifica tres mecanismos de control de acceso al medio (MAC) para WLANs: DCF (*Distributed Coordination Function*), PCF (*Point Coordination Function*) y HCF (*Hybrid Coordination Function*). DCF es el mecanismo MAC obligatorio del estándar IEEE 802.11 [1]. Se trata de CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) un esquema de acceso aleatorio, que además incorpora un algoritmo de *backoff* exponencial binario (BEBA-*Binary Exponential Backoff Algorithm*) para controlar cuando se deben realizar las retransmisiones de los paquetes que han sufrido colisión o errores de recepción. En DCF, cada estación (STA) monitoriza el canal antes de la transmisión de sus paquetes. La STA transmite el paquete sólo si se detecta que el medio está disponible *(idle)*, esto es, libre de transmisiones durante un DIFS (*Distributed Interval Frame Space*) determinado. Por otro lado, si la STA detecta alguna transmisión durante el DIFS, seguirá esperando hasta que el medio esté disponible durante DIFS. Seguidamente, la STA divide el tiempo en ranuras (o *slots*) de duración σ y ejecuta un algoritmo BEBA que determina el número de ranuras a esperar previas a la transmisión. Para evitar la captura del canal[1] por parte de una estación, el algoritmo de *backoff* es aplicado entre dos transmisiones consecutivas de paquetes nuevos originados desde la misma STA, aunque se detecte que el medio está disponible durante todo el tiempo DIFS.

Después de aplicar el algoritmo BEBA, la STA utiliza un contador de ranuras para determinar su ranura de transmisión. Durante el periodo de *backoff*, las otras STAs en contención pueden acceder al medio y transmitir sus paquetes. Si alguna de las otras estaciones empieza a transmitir, el resto de STAs en contención detectarán el medio ocupado y pausarán sus procesos de espera, memorizando los contadores de las ranuras del proceso de *backoff*. Gracias a esto, consiguen evitar la colisión con la transmisión en curso y su proceso de espera se puede restablecer en el mismo punto en que fue interrumpido. De hecho, una vez la transmisión actual ha finalizado y el medio es *idle*, las estaciones en contención cargarán sus contadores de backoff en el punto anterior, previo a la interrupción. El algoritmo BEBA determina el número de ranuras a esperar seleccionando un número aleatorio entre 0 y $w-1$ de forma uniforme, donde w es la ventana de contención (CW). El valor inicial de w es la ventana de contención mínima (CW_{min}) y se duplica después de cada transmisión fallida. El valor máximo de w es $CW_{max} = 2^{m_{max}} CW_{min}$, donde m_{max} es el número máximo de retransmisiones por paquete. Después de cada transmisión de paquete exitosa, CW se resetea a CW_{min}.

En 802.11 una transmisión exitosa es replicada siempre con una trama de reconocimiento (ACK- *Acknowledgement*) desde el receptor. Esta respuesta se transmite tras esperar un tiempo SIFS (*Short Interval Frame Space*) después del último bit del paquete recibido. El SIFS (más el tiempo de propagación) es más corto que el DIFS, evitando así que otras estaciones listas para la transmisión perciban el medio *idle* y empiecen sus transmisiones. Este es el único mecanismo disponible en el transmisor para reconocer una transmisión exitosa. Si no se recibe la trama ACK después de un intervalo DIFS, posiblemente debido a un error de transmisión o a una colisión, el transmisor decide que la transmisión ha fallado y empieza el proceso de *backoff* para retransmitir el paquete. Se debe advertir que la trama ACK introduce *overhead*, reduciendo así el *goodput* en la capa MAC ya que cada transmisión tiene que esperar por un periodo de SIFS y luego comprobar la secuencia de verificación de trama (FCS-*Frame Check Sequence*) incluida en el ACK.

El intercambio de tramas descrito anteriormente se conoce como la técnica de acceso básico y es el esquema de acceso más usado en DCF [3] y el que vamos a analizar en este estudio. Por completitud, se debe mencionar que hay otra técnica de acceso, llamada RTS/CTS, que es de uso obligatorio cuando la longitud de paquete supera el umbral *dot11RTSThreshold* configurable por cada sistema.

[1] Una estación ocupa el medio continuamente sin permitir la transmisión por parte de otras estaciones

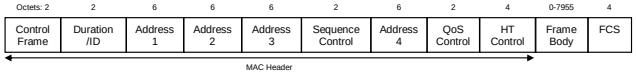


Fig. 1. Formato de trama MAC.

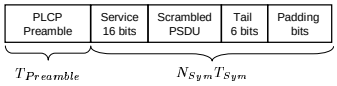


Fig. 2. PPDU frame format

Para paquetes de longitud corta o que utilizen una tasa de transmisión elevada que reduzca considerablemente la duración de la transmisión del paquete, el *overhead* introducido por esta técnica afecta considerablemente el rendimiento del sistema. En RTS/CTS, previamente a la transmisión de un paquete, el transmisor envía una solicitud de envío (RTS-*Request to Send*) en forma de trama MAC para reservar el medio de canal, si esta trama es recibida correctamente, la estación receptora responde con una trama MAC de CTS (*Clear to Send*), indicando la disponibilidad del medio para que el transmisor realice la transmisión del paquete una vez haya recibido el CTS. Nótese que las colisiones sólo pueden ocurrir durante el intercambio de las tramas RTS y CTS, reduciendo drásticamente el tiempo de colisión para paquetes muy largos en comparación con la técnica de acceso básico. El intercambio de tramas RTS/CTS también permite evitar el problema del terminal oculto[2].

C. Formatos de trama y tiempos

En la subcapa MAC, las MSDUs (*MAC Service Data Units*) son los datos de información procedentes de la capa superior y se convierten a MPDUs (*MAC Protocol Data Units*). Si el tamaño de las MSDUs supera el umbral de fragmentación, las MSDUs son fragmentadas y convertidas a MPDUs. En la capa física, las MPDUs son las PSDUs (*Physical Service Data Unit*) y se procesan por el procedimiento de PLCP (*Physical Layer Convergence Procedure*) para formar las PPDUs (*PLCP Protocol Data Unit*) previos a la transmisión.

1) Formato de la MPDU: La trama MAC del IEEE 802.11n [14], llamada MPDU y presentada en la Fig. 1, tiene una estructura similar a su equivalente en el IEEE 802.11 genérico [1]. La cabecera MAC incorpora dos subcampos adicionales, el *Address 4* y el *HT control* que contienen la información de control de realimentación intercambiada entre los extremos de la comunicación, implementando así el canal de retorno utilizado por los algoritmos adaptativos de lazo cerrado. Los otros campos MPDU definidos (*variable length information*, *frame body* y *frame check sequence*) son idénticos a sus homónimos en las especificaciones del IEEE 802.11 [1].

Para poder añadir el subcampo *HT control* en las tramas de control del IEEE 802.11 (p.e., ACK, RTS o CTS), el 802.11n crea una nueva trama de control, llamada *control wrapper frame*. Esta trama contiene el subcampo *HT control* y además encapsula la trama de control de los estándares WLAN anteriores, habilitando así la adaptación rápida del enlace. Mencionar que esta trama de control sólo puede ser usada si ambos elementos de la transmisión cumplen con la norma IEEE 802.11n.

[2]Un par de estaciones en el rango del punto de acceso están ocultas una de la otra porque la transmisión desde una a las otras no puede ser oída por la otra

Nombre	Valor	Descripción
σ	9μs	Tiempo de ranura
T_{SIFS}	16μs	*Short Interval Frame Space*
T_{DIFS}	34μs	$t_{SIFS} + 2 \times t_{Slot}$
T_{Prop}	$<< 1\mu s$	Tiempo de propagación
$T_{Preamble}$	$40\mu s$	Duración del preámbulo PLCP
T_{Sym}	$4\mu s$	Periodo de símbolo OFDM
CW_{min}	15	Mínimo tamaño de la ventana de contención
CW_{max}	1023	Máximo tamaño de la ventana de contención

Tabla I
VALORES DE TIEMPO ESPECIFICADOS EN EL IEEE 802.11N [14].

2) Formato de la PPDU: El IEEE 802.11n define tres formatos de PPDU: *Non-HT format* y *HT-mixed format* (obligatorios), y *HT-greenfield format* (opcional). Sin pérdida de generalidad hemos utilizado el formato *HT-mixed format* que es compatible con receptores IEEE 802.11 de OFDM y ERP (*Extended Rate PHY*). La PPDU, presentada en Fig. 2, consiste en el preámbulo PLCP, el campo de servicio, la PSDU ya entrelazada y codificada (transmitida desde la subcapa MAC), los bits de cola, y los bits de relleno (si son necesarios). El preámbulo PLCP, con duración $T_{Preamble}$, es complementado con nuevos subcampos para mejorar la fiabilidad de la estimación de canal cuando se utilizan técnicas de *beamforming*. También contiene la información de señalización requerida para procesar la PSDU entrelazada y codificada.

Los tiempos previamente definidos y otros parámetros significativos del sistema se encuentran especificados en el documento del estándar IEEE 802.11n y se presentan en la Tabla I.

3) Tiempo de transmisión: La duración de una transmisión exitosa para una MPDU de *L*-bits utilizando el MCS m es

$$\begin{aligned} T_s(m,L) =& T_{Tr}(m,L) + T_{Prop} + T_{SIFS} \\ &+ T_{Prop} + T_{ACK+HTC}(m) + T_{DIFS}, \end{aligned} \quad (1)$$

donde $T_{Tr}(m,L)$ es el tiempo dedicado a la transmisión de la MPDU, y puede expresarse como:

$$T_{Tr}(m,L) = T_{Preamble} + N_{sym}(L)T_{sym}, \quad (2)$$

con

$$N_{sym}(x) = m_{STBC}\left\lceil \frac{x+22}{m_{STBC}N_{DBPS}(m)} \right\rceil, \quad (3)$$

donde $m_{STBC} = 2$ para STBC y $m_{STBC} = 1$ para los otros casos, $N_{DBPS}(m)$ es la cantidad de bits que forman cada símbolo OFDM en función del MCS m, $\lceil x \rceil$ denota el entero menor o igual que x, y N_{sym} es el número de símbolos OFDM involucrados en la transmisión de un paquete completo. De igual forma, el tiempo requerido para la transmisión de una trama ACK+HTC[3] utilizando el MCS m puede calcularse como

$$T_{ACK+HTC}(m) = T_{Preamble} + N_{sym}(20 \cdot 8)T_{sym}. \quad (4)$$

[3]*wrapper control frame* que encapsula una trama de control ACK.

Una colisión se produce cuando dos o más estaciones transmiten sobre la misma ranura y termina cuando finaliza la transmisión más duradera de las estaciones en colisión. Por tanto, su duración depende de la combinación del MCS m^* y longitud de MPDU L^* que supongan una transmisión más duradera. De esta manera, la duración de la colisión se puede expresar como

$$T_c(m^*, L^*) = T_{Tr}(m^*, L^*) + T_{Prop} + T_{DIFS}. \quad (5)$$

El tiempo de transmisión para una MPDU errónea $T_e(m, L)$ es el tiempo transcurrido en una transmisión que experimenta error pero no colisión y puede calcularse como

$$T_e(m, L) = T_{Tr}(m, L) + T_{Prop} + T_{DIFS}. \quad (6)$$

En este modelo no hemos considerado la posibilidad de que se produzca error de transmisión durante la transmisión del ACK, dado que la probabilidad de este evento es extremadamente baja.

III. Modulación y codificación adaptativa

A. ARF

Como se ha mencionado en la introducción, el algoritmo ARF es un algoritmo de lazo abierto muy simple que ha sido ampliamente utilizado en la mayoría de los sistemas WLAN predecesores del estándar IEEE 802.11n. Este algoritmo adapta la tasa de transmisión conforme al número de errores y éxitos de transmisión consecutivos, ambos conocidos gracias al mecanismo de reconocimiento ACK. El algoritmo ARF disminuye la tasa de transmisión después de dos errores de transmisión consecutivos y la incrementa tras diez transmisiones exitosas sucesivas o después de un determinado *timeout*. Este *timeout* es reinicializado tras un cambio de tasa de transmisión y se utiliza para seguir los ACKs válidos y perdidos, mejorando así la adaptación del sistema durante largos intervalos de inactividad [2]. Un valor de *timeout* aceptable está comprendido en el rango de 50-200 ms [15]. Además, es importante mencionar que después de un incremento de tasa, la transmisión siguiente se utiliza como una transmisión de prueba para el nuevo modo seleccionado. Si no se recibe un ACK para este paquete de prueba, el sistema adopta la tasa de transmisión previa al incremento.

Para implementar ARF en IEEE 802.11n se necesita determinar las tasas disponibles en el conjunto de MCSs, denotado por $\boldsymbol{\mathcal{M}}$. En contraposición con los estándares previos al IEEE 802.11, en 802.11n la misma tasa de transmisión puede ser proporcionada por diferentes MCSs $\in \boldsymbol{\mathcal{M}}$, pero sólo uno de ellos va a ser utilizado por el algoritmo ARF. Por esta razón, los MCSs del conjunto $\boldsymbol{\mathcal{M}}$ deben reorganizarse en función de su tasa de transmisión. En aquellas tasas obtenidas tanto con SDM o STBC, sólo se utilizarán los MCS basados en STBC dado que son más robustos frente a las variaciones de canal [12]. El conjunto ordenado y reducido de MCSs es $\overline{\boldsymbol{\mathcal{M}}}$.

B. FLA

La adaptación rápida del enlace (FLA) es una técnica de lazo cerrado que utiliza el canal de retorno de control existente desde el receptor al transmisor. La idea principal detrás del FLA es que el receptor, gracias a un conocimiento preciso de la respuesta del canal, puede predecir la tasa de error para cada MCS disponible, elegir el MCS que maximiza el *throughput* instantáneo mientras se satisfacen los requisitos de calidad en forma de una probabilidad de *outage* de error por paquete [9] y comunicar el MCS seleccionado al transmisor vía canal de retorno. En este trabajo asumimos la utilización de la metodología presentada en [9], donde la predicción del estado del enlace para cada MCS está basada en el cálculo de la SNR efectiva exponencial (EESM) [16]. Utilizando esta aproximación, la SNR efectiva para un determinado MCS puede asociarse fácilmente a un valor de PER utilizando tablas de referencia previamente calculadas durante una fase de calibración *off-line*.

Nótese que el MCS utilizado se determina utilizando sólo la información instantánea sobre el estado del canal disponible en el receptor y, a diferencia de ARF, el transmisor no confía en la información correspondiente a los resultados de las transmisiones anteriores. Por lo tanto, y como se va a demostrar en la Sección V, FLA ofrece un rendimiento superior en relación a ARF a costa de incrementar la complejidad computacional y el uso de un canal de retorno de control.

IV. Análisis del goodput

Utilizando una metodología basada en [10], el análisis del *goodput* se centra en la región de saturación, definida como el punto operacional donde el sistema es expuesto a la carga máxima ofrecida. En esta región, se asume que cada estación dispone siempre de nuevos paquetes para la transmisión. A diferencia de otros puntos operacionales, en la región de saturación la respuesta del sistema es estable y más fácil de prever y caracterizar.

El *goodput* S de saturación del sistema se define como la cantidad media de información útil transmitida por unidad de tiempo, es decir,

$$S = \frac{E[\text{Información útil en una ranura}]}{E[\text{Duración de una ranura}]}. \quad (7)$$

Se debe advertir que la duración de una ranura se refiere al valor (constante) σ o al intervalo de tiempo (variable) entre dos decrementos consecutivos del contador de tiempo de *backoff*.

En [10] Bianchi presenta un estudio del rendimiento de DCF sobre IEEE 802.11 asumiendo condiciones de transmisión ideales. Este estudio fue extendido en [17] para tener en cuenta errores de transmisión. Nuestro análisis amplía el trabajo de [17] al considerar los efectos de los mecanismos de modulación y codificación en el contexto de un sistema MIMO-OFDM como IEEE 802.11n.

En una determinada ranura se pueden producir cuatro eventos: la transmisión exitosa del paquete, la transmisión errónea del paquete, una colisión o la no ocupación de la ranura (ranura libre). Desde el punto de vista del algoritmo BEBA, las transmisiones con errores y colisiones son indistinguibles, por lo tanto la probabilidad condicional de la unión de estos eventos se puede calcular como

$$p = 1 - (1 - \zeta_u)(1 - \tau)^{n-1}, \quad (8)$$

donde n es el número de estaciones activas en el escenario, ζ_u es la probabilidad de transmisión errónea para el algoritmo AMC considerado, promediado en función del número de usuarios, y τ es la probabilidad de que una estación concreta

transmita en una ranura determinada, que puede obtenerse como

$$\tau = \frac{2(1-2p)}{(1-2p)(CW_{min}+1)+pCW_{min}(1-(2p)^{m_{max}})}. \quad (9)$$

Cabe apreciar que p y τ se pueden calcular resolviendo el sistema no lineal formado por las ecuaciones (8) y (9).

Utilizando τ, la probabilidad de que sólo transmita una estación sobre una ranura concreta viene dada por

$$P_s = n\tau(1-\tau)^{n-1}. \quad (10)$$

La probabilidad de que una ranura concreta esté libre (i.e. no utilizada por ningún usuario) puede calcularse como

$$P_i = (1-\tau)^n. \quad (11)$$

Observando todos los eventos posibles, sólo la transmisión exitosa de paquetes incrementa la información de *payload*, cualquier otro evento conduce a una degradación del *goodput*. Consecuentemente, adaptando la expresión del *goodput* de [17, eq. (50)] a nuestro modelo, se obtiene

$$S = \frac{(1-\zeta_s)P_sE[L_p]}{P_i\sigma + (1-\zeta_s)P_s\overline{T_s^{(n,L)}} + \zeta_sP_s\overline{T_e^{(n,L)}} + (1-P_s-P_i)\overline{T_c^{(n,L)}}} \quad (12)$$

donde L_p es la longitud del paquete en bits, ζ_s denota la probabilidad de error media por paquete para una ranura dada y, $\overline{T_s^{(n,L)}}$, $\overline{T_c^{(n,L)}}$ y $\overline{T_e^{(n,L)}}$ representan, respectivamente, el tiempo medio en que se producen transmisiones exitosas, colisiones y errores de transmisión. L_p se calcula como $L_p = L - L_h$, donde L_h es la longitud de la cabecera MAC expresada en bits.

El tiempo medio transcurrido en una transmisión exitosa depende del número de estaciones en contención n y de la longitud de la MPDU L y se puede calcular como

$$\overline{T_s^{(n,L)}} = \sum_{m=0}^{|\mathcal{M}|} P_s^{MCS}(m,n)T_s(m,L), \quad (13)$$

donde $|\mathcal{M}|$ denota el cardinal del conjunto $\mathcal{M}$ y $P_s^{MCS}(m,n)$ es la probabilidad de utilizar el MCS m cuando el sistema se encuentra en un evento de transmisión exitosa.

De forma similar, $T_c^{(n,L)}$ y $T_e^{(n,L)}$ se calculan como

$$\overline{T_c^{(n,L)}} = \sum_{m=0}^{|\mathcal{M}|} P_c^{MCS}(m,n)T_c(m,L) \quad (14)$$

y

$$\overline{T_e^{(n,L)}} = \sum_{m=0}^{|\mathcal{M}|} P_e^{MCS}(m,n)T_e(m,L), \quad (15)$$

donde $P_c^{MCS}(m,n)$ y $P_e^{MCS}(m,n)$ denotan las probabilidades de utilizar el MCS m cuando hay colisiones y transmisiones erróneas, respectivamente.

Los parámetros $P_s^{MCS}(m,n)$, $P_c^{MCS}(m,n)$ y $P_e^{MCS}(m,n)$ se pueden determinar bien analíticamente, caracterizando el comportamiento estadístico de la SNR efectiva y luego determinando los umbrales de conmutación entre modos de transmisión, o bien a través de simulación. Este trabajo, para simplificar el análisis, se basa en la última aproximación, de ahí que el modelo resultante sea considerado semi-analítico.

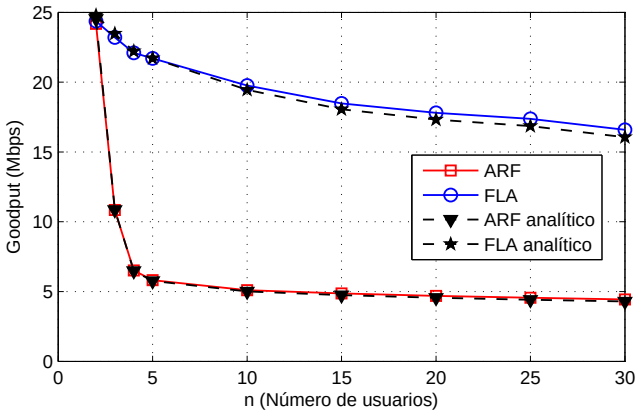


Fig. 3. Comparación del *goodput* de sistema simulado y analítico.

V. Resultados numéricos

Para validar el modelo propuesto, se ha implementado un simulador MATLAB del IEEE 802.11n a nivel de sistema, utilizando los parámetros de enlace derivados de [9]. Se debe destacar que este modelo es considerablemente más realista que el presentado por Bianchi en [10] ya que admite un comportamiento no ideal del canal y considera los mecanismos AMC. En este artículo nos concentramos en el análisis del rendimiento del sistema en un escenario que incluye el enlace ascendente y considera, también, las respuestas con tramas de control MAC en el enlace descendente. Dado un número de usuarios n, se han generado diferentes escenarios distribuyéndolos de forma uniforme sobre un área circular de radio R_{max} centrada alrededor de un punto de acceso (AP- *Access Point*) y además, se ha determinado la respuesta frecuencial para cada uno de estos usuarios hacia el AP durante un periodo de tiempo. Para modelar la respuesta del canal se ha utilizado la herramienta de simulación de Kermoal et al. [18] que permite generar canales MIMO a partir de la distancia de cada usuario respecto al AP. El radio máximo R_{max} ha sido fijado a un valor que asegura al mismo tiempo la eliminación del problema del terminal oculto e impide la utilización del modo no transmisión (disponible en FLA). El rendimiento del sistema para un número dado de usuarios se obtiene promediando los resultados de rendimiento sobre N_{sim} escenarios diferentes. Cada escenario se evalúa utilizando ARF y FLA, permitiendo de esta manera una comparación directa entre ambas técnicas.

Los parámetros principales del protocolo utilizados para obtener resultados analíticos y de simulación se han resumido en la Tabla I. La capa física sólo utiliza los primeros 16 modos del IEEE 802.11n (MCS0-MCS15), logrando tasas de transmisión de hasta 130 Mbps. Para ARF, el *timeout* es de $60ms$. Para obtener una estimación precisa del rendimiento medio del sistema se han generado $N_{sim} = 200$ simulaciones de duración $t_{sim} = 11$ segundos para cada valor de n.

Las figuras 3 y 4 presentan el rendimiento del sistema y las probabilidades condicionadas p y τ (ver las ecuaciones (8) y (9)) utilizando paquetes de longitud $L_p = 12000$ bits. En ambas figuras se compararan los resultados del sistema semi-analíticos y los de simulación para FLA y ARF, observándose buena concordancia entre resultados de análisis y de simu-

	ARF					FLA				
n	ζ_s	ζ_u	$\overline{T_s^{(n,L)}}$ (μs)	$\overline{T_e^{(n,L)}}$ (μs)	$\overline{T_c^{(n,L)}}$ (μs)	ζ_s	ζ_u	$\overline{T_s^{(n,L)}}$ (μs)	$\overline{T_e^{(n,L)}}$ (μs)	$\overline{T_c^{(n,L)}}$ (μs)
2	0.05245	0.05454	403.87	313.50	435.84	0.00007	0.00020	419.68	396.66	454.95
3	0.00835	0.00900	938.69	566.88	1191.85	0.00049	0.00070	430.46	300.25	472.49
4	0.00231	0.00440	1555.09	1112.48	1778.29	0.00122	0.00178	442.15	295.39	484.41
5	0.00157	0.00277	1711.08	1321.62	1870.29	0.00214	0.00245	439.84	278.28	488.16
10	0.00113	0.00217	1806.85	1324.23	1912.87	0.00640	0.00709	449.05	284.62	501.71
15	0.00117	0.00202	1804.63	1346.27	1912.87	0.01010	0.01157	456.56	289.67	515.70
20	0.00124	0.00205	1802.22	1309.61	1912.88	0.01319	0.01493	456.10	290.99	516.38
25	0.00146	0.00218	1796.45	1247.92	1911.08	0.01592	0.01829	452.45	288.03	514.55
30	0.00162	0.00251	1797.59	1227.69	1911.65	0.01886	0.02160	460.03	292.71	527.67

Tabla II
PARÁMETROS DE SISTEMA OBTENIDOS POR SIMULACIÓN.

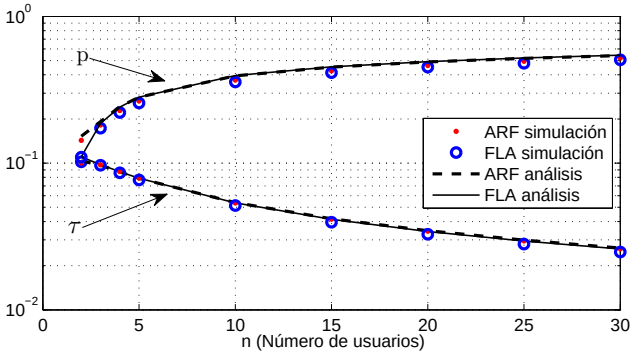


Fig. 4. Probabilidad de transmisión (τ) y probabilidad de error y/o colisión (p).

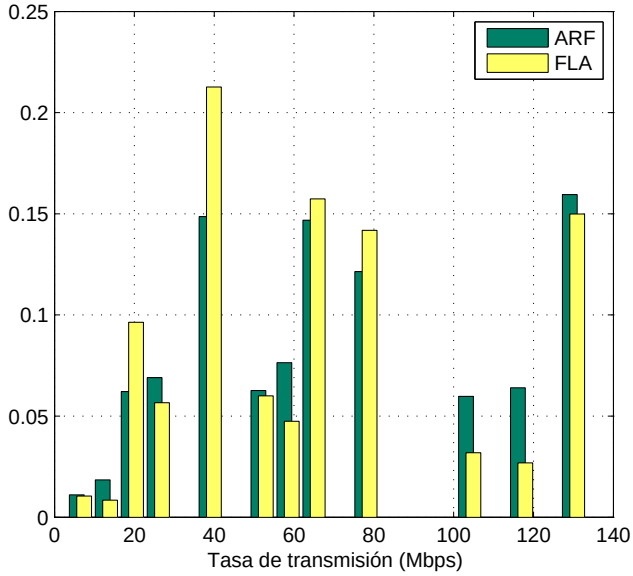


Fig. 5. Probabilidad de utilizar cada tasa de transmisión para una configuración con $n = 2$.

lación. Además, la Fig. 3 también ilustra los beneficios de *goodput* obtenidos por la adaptación basada en FLA respecto a la basada en ARF. A medida que el número de usuarios aumenta, la probabilidad de colisión crece y provoca un comportamiento muy diferente para los dos sistemas. ARF decrementa rápidamente el modo de transmisión con independencia de cuales sean las condiciones de propagación del canal. En cambio, FLA es capaz de determinar la tasa de transmisión de acuerdo con la información sobre el estado del canal adquirida a través del canal de realimentación, independientemente del número de usuarios en el sistema y, por tanto, cuando el canal presenta condiciones favorables puede utilizar tasas de transmisión más elevadas que ARF. En consecuencia y debido al incremento del número de colisiones en el sistema, ARF experimenta una reducción drástica en *throughput* cuando 3 o más usuarios están presentes en la red y FLA sólo exhibe una leve degradación por cada nuevo usuario incorporado al sistema. La figura 4 revela otro hecho destacable, en los escenarios con más de 2 usuarios la probabilidad de colisión y/o error por estación p y la probabilidad de transmisión para una ranura genérica τ son prácticamente idénticas para ambos métodos adaptativos. Sólo se observa una leve diferencia entre ARF y FLA para el caso de una configuración con 2 usuarios, donde ARF incrementa su tasa de error debido a la realización de la transmisión de prueba después de 10 transmisiones correctas cuando el sistema ya está utilizando el MCS que nos proporciona *throughput* máximo, causando en media un error de cada 11 transmisiones.

La Tabla II presenta los parámetros de sistema obtenidos mediante simulación para $L_p = 12000$ bits, incluyendo ζ_s, ζ_u, $\overline{T_s^{(n,L)}}$, $\overline{T_e^{(n,L)}}$ y $\overline{T_c^{(n,L)}}$, para ambos esquemas y suponiendo diferentes cargas de red. Nótese que en ARF el tiempo medio transcurrido crece con el número de usuarios, a causa del uso más frecuente de los modos de transmisión más bajos (véase Figs. 5, 6 y 7, explicadas en detalle más adelante), provocado por el incremento en el número de colisiones. Utilizando FLA, como era previsible, los valores de los tiempos medios transcurridos apenas guardan relación con el número de usuarios en el sistema. Sólo se observa un leve incremento para $T_s^{(n,L)}$ y $T_c^{(n,L)}$, atribuible al desajuste entre información de canal y el modo seleccionado debido a los retrasos en la realimentación en entornos con alta probabilidad de colisión.

En las Figs. 5, 6 y 7 se representa para cada AMC la probabilidad de utilización de cada una de las tasa de transmisión en los escenarios con 2, 3 y 15 usuarios, respectivamente. Para ARF, esta probabilidad cambia de forma considerable en función de n, utilizando tasas altas para 2 y 3 usuarios, y las más bajas en los escenarios con más usuarios en saturación. Este efecto se debe al incremento de la probabilidad de colisión experimentado en los entornos con más de 3 usuarios en saturación, donde ARF no es capaz de mantenerse adaptado a las condiciones reales del canal y

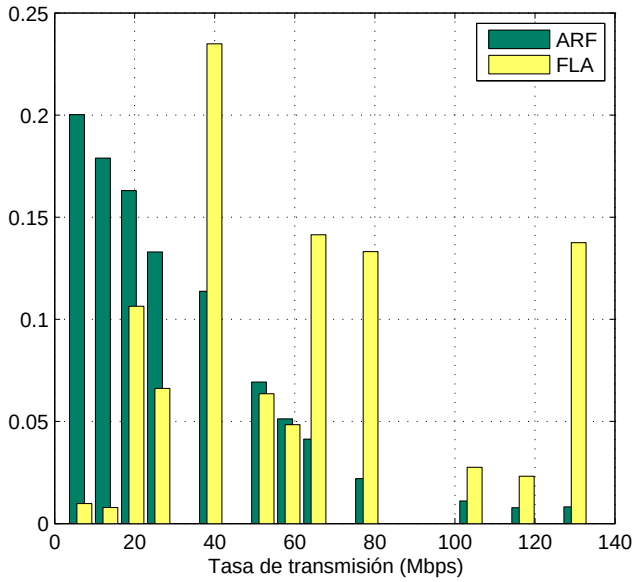


Fig. 6. Probabilidad de utilizar cada tasa de transmisión para una configuración con $n = 3$.

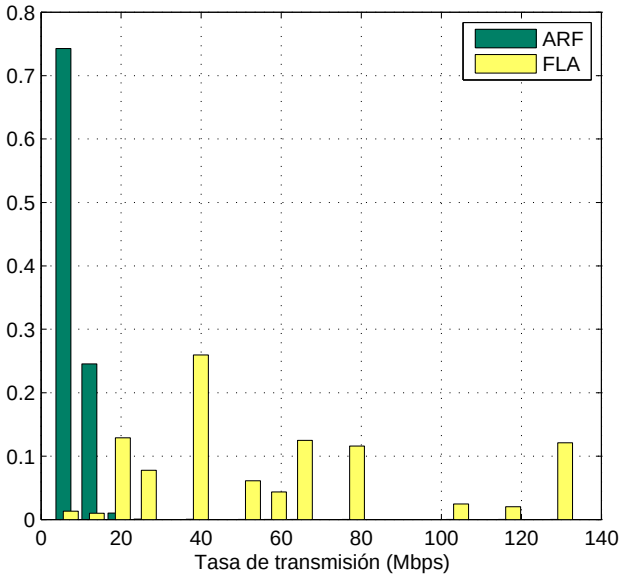


Fig. 7. Probabilidad de utilizar cada tasa de transmisión para una configuración con $n = 15$.

reduce la tasa de transmisión en respuesta a estas colisiones (identificadas como errores de transmisión). En cambio, para FLA se mantienen unas probabilidades de utilización de las diferentes tasas de transmisión en función de n (véase Figs 5, 6 y 7). En este caso la utilización de cada tasa depende de la SNR media y del estado del canal de cada usuario, que está directamente relacionado con la distribución de estos usuarios respecto al AP y su componente de *shadowing*. Queda claro, pues, que FLA selecciona la tasa de transmisión de acuerdo con las condiciones de canal e independientemente de la carga del escenario, mejorando claramente el comportamiento del algoritmo ARF.

En la Figura 8 se presentan los resultados de *goodput* para ambos esquemas AMC utilizando diferentes longitudes de paquete (L_p) y diferente número de usuarios. A medida que

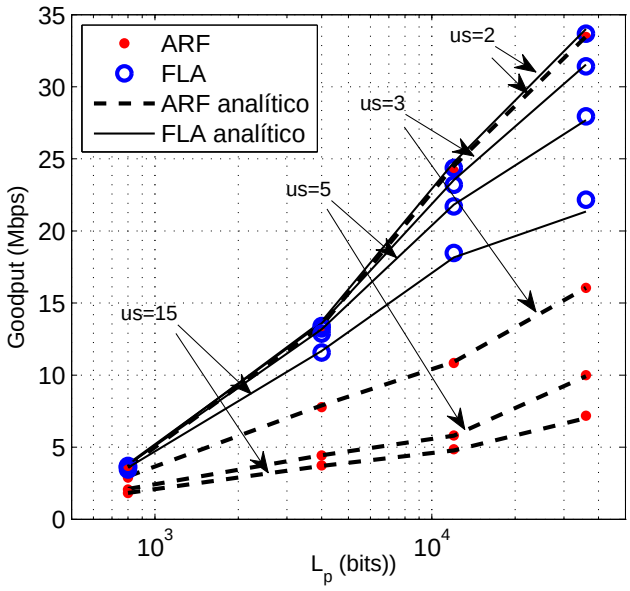


Fig. 8. *Goodput* para diferentes longitudes de paquete y número de usuarios.

se incrementa la longitud del paquete el *goodput* del sistema aumenta para ambos esquemas AMC. Por otro lado, y como ya se ha observado en la Fig. 3, si aumentamos el número de usuarios en saturación las prestaciones del sistema decrecen de forma abrupta en ARF y de forma más gradual en FLA. De todas formas, aunque para valores de L_p inferiores a 12.000 bits las diferencias del *goodput* ofrecido por ARF y FLA se acentúan, para valores superiores a 12000 bits y con entornos de más de 3 usuarios, las diferencias entre FLA y ARF disminuyen, ya que ARF mejora sus prestaciones debido al agotamiento del *timeout* del ARF y FLA entra en un estado de cierta saturación a causa del retardo en la realimentación. En la Fig. 9 se presenta el tiempo medio entre transmisiones para ambos AMC y se observa que para escenarios de ARF con más de 3 usuarios y $L_p > 12000$ bits, este tiempo se aproxima o supera el valor del *timeout* utilizado en ARF. Este fenómeno provoca una mayor utilización del incremento de tasa debida a la expiración del *timeout* del ARF. En cambio, en el esquema FLA en presencia de un número elevado de usuarios, el esquema tiende a un punto de saturación elevado del *goodput* para longitudes de paquete próximas a $L_p = 30000$ bits. Esta saturación se debe a que FLA utiliza el MCS utilizado en la última trama HTC+ACK recibida que, en presencia de colisiones y debido al retardo, introduce un desajuste considerable entre el MCS recomendado y el estado actual del canal. En la Fig. 10 se representa el tiempo medio entre transmisiones con éxito y se observa que este tiempo para 5 y 15 usuarios con las longitudes de paquete más elevadas alcanza valores cercanos al tiempo de coherencia del canal (170ms), provocando que el modo seleccionado por FLA no se corresponda con las características actuales del canal. En estos casos, para evitar la utilización de MCS no adecuados se tendría que añadir un mecanismo de control para determinar el tiempo transcurrido entre el MCS recibido y la siguiente transmisión, y solicitar un nuevo MCS cuando el retardo fuera mayor o igual que el tiempo de coherencia del canal.

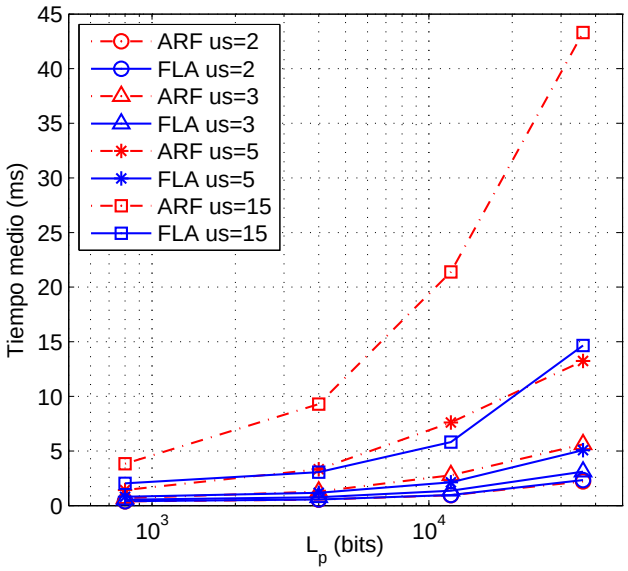


Fig. 9. Tiempo medio entre transmisiones de una estación.

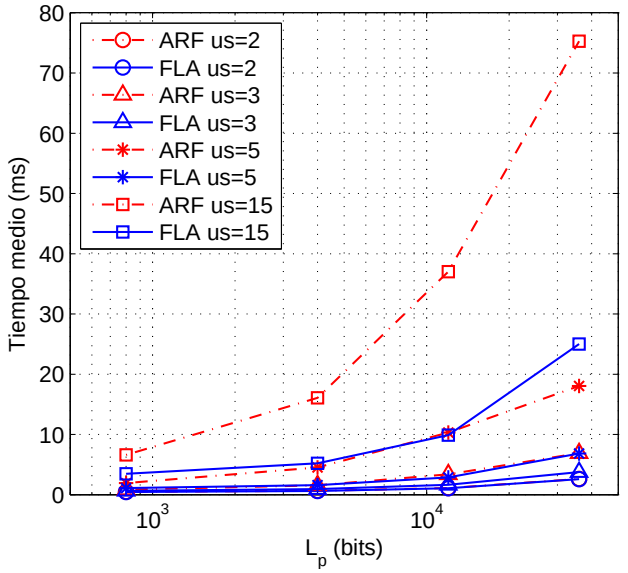


Fig. 10. Tiempo medio entre transmisiones correctas de una estación.

VI. Conclusiones

Este artículo ha presentado un modelo *cross-layer* MAC-PHY semi-analítico que permite evaluar el rendimiento en *goodput* de esquemas adaptativos de lazo abierto y cerrado, en entornos de redes locales inalámbricas basadas en IEEE 802.11n. Sin pérdida de generalidad, se ha considerado el conocido algoritmo de lazo abierto ARF (*Automatic Rate Fallback*) y un algoritmo de lazo cerrado, como es el FLA (*Fast Link Adaptation*) basado en la SNR efectiva exponencial. A diferencia de otros trabajos anteriores, se han considerado condiciones de canal no ideales y que los usuarios podían utilizar diferentes modos de transmisión. El modelo analítico ha sido validado contrastando sus resultados con los obtenidos a través de simulación y, además, ha permitido obtener varias conclusiones reseñables. Por una parte, a medida que el número de usuarios crece en el sistema, la adaptación basada en FLA es más robusta en presencia de colisiones que la adaptación basada en ARF. Concretamente, ARF experimenta una reducción drástica en *throughput* cuando 3 o más usuarios están presentes en la red y FLA sólo exhibe una leve degradación por cada nuevo usuario incorporado al sistema. Por otra parte, se ha observado que ambos esquemas AMC mejoran su rendimiento a medida que se incrementa la longitud de paquete especialmente el sistema FLA. De todos formas, el esquema FLA presenta un punto de saturación a partir de longitudes de paquete superiores a unos 30.000 bits y este problema podría solucionarse utilizando estrategias de adaptación que tomaran en consideración el tiempo de coherencia del canal.

Agradecimientos

Esta investigación ha sido parcialmente financiada por el MEC y FEDER en el marco del proyecto COSMOS (TEC2008-02422), Conselleria d'Economia, Hisenda i Innovació del Govern de les Illes Balears en el marco de los proyectos PCTIB-2005GC1-09 y beca predoctoral.

Referencias

[1] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, Dec. 2007.

[2] A. Kamerman and L. Monteban, "WaveLAN®-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs technical journal*, vol. 2, no. 3.

[3] J. Kim, S. Kim, S. Choi, and D. Qiao, "CARA: Collision-Aware Rate Adaptation for IEEE 802.11 WLANs," in *IEEE INFOCOM*, Barcelona, Spain, April 2006, pp. 1 –11.

[4] T. Joshi, D. Ahuja, D. Singh, and D. Agrawal, "Sara: stochastic automata rate adaptation for IEEE 802.11 networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 11, pp. 1579–1590, 2008.

[5] J. He, D. Kaleshi, A. Munro, and J. McGeehan, "Modeling Link Adaptation Algorithm for IEEE 802.11 Wireless LAN Networks," in *IEEE ISWCS*, Valencia, Spain, Sept. 2006, pp. 500 –504.

[6] J. Zhang, K. Tan, J. Zhao, H. Wu, and Y. Zhang, "A Practical SNR-Guided Rate Adaptation," in *IEEE INFOCOM*, Phoenix, AZ, April 2008, pp. 2083 –2091.

[7] H. Jung, T. Kwon, Y. Choi, and Y. Seok, "A scalable rate adaptation mechanism for IEEE 802.11e wireless," in *IEEE FGCN*, vol. 1, Jeju-Island, Korea, Dec. 2007, pp. 505–509.

[8] G. Martorell, F. Riera-Palou, G. Femenias, "Cross-layer link adaptation for IEEE 802.11n," in *IEEE IWCLD*, Palma de Mallorca, Spain, June 2009, pp. 1 –5.

[9] G. Martorell, F. Riera-Palou, and G. Femenias, "Cross-layer fast link adaptation for MIMO-OFDM based WLANs," *Springer Wireless Personal Communications*, 2010, online available.

[10] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535 –547, March 2000.

[11] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[12] Y.-S. Choi and S. Alamouti, "A pragmatic PHY abstraction technique for link adaptation and MIMO switching," *IEEE Journal of Selected Areas in Communications*, vol. 26, no. 6, pp. 960–971, 2008.

[13] G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 41–59, 1996.

[14] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," *IEEE Std 802.11n-2009*, 2009.

[15] G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive MAC protocol for multi-hop wireless networks," in *ACM MobiCom*, Rome, Italy, 2001, pp. 236–251.

[16] S. Simoens, S. Rouquette-Léveil, P. Sartori, Y. Blankenship, and B. Classon, "Error prediction for adaptive modulation and coding in multiple-antenna OFDM systems," *Elsevier Signal Process.*, vol. 86, no. 8, pp. 1911–1919, 2006.

[17] B. Bing, *Emerging Technologies in Wireless LANs: Theory, Design, and Deployment*. Cambridge Univ Press, 2007.

[18] J. Kermoal, L. Schumacher, K. Pedersen, P. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE Journal of Selected Areas in Communications*, vol. 20, no. 6, pp. 1211–1226, 2002.

Throughput optimization in QoS constrained adaptive wireless networks using Chase Combining HARQ

Jaume Ramis, Guillem Femenias, Felip Riera and Loren Carrasco
Grupo de Comunicaciones Móviles – Universiat de les Illes Balears
Email: {jaume.ramis,guillem.femenias,felip.riera,loren.carrasco}@uib.es

***Abstract*—A point to point wireless system using an AMC scheme at the physical layer and a truncated HARQ-CC error control protocol at the data link layer is considered. By using Markov chain-based models for the wireless fading channel and the queueing process, analytical expressions for performance metrics such as throughput, average packet delay and packet loss rate, are derived. These expressions allow the formulation of a constrained optimization problem to maximize the system throughput under the prescribed QoS constraints. Numerical results confirm the validity of the proposed model and reveal that HARQ-CC consistently outperforms the classical Type-I Hybrid FEC/ARQ schemes.**

I. Introduction

Recently, there has been great interest in protocols for wireless networks that actively exploit the dependence between protocol layers to obtain performance gains. These designs are generically referred to as cross-layer designs, and have become increasingly popular [1]–[3]. Many recent proposals coincide in combining *adaptive modulation and coding* (AMC) with an *automatic repeat request* (ARQ) protocol (see, e.g., [4]–[12]) with the aim of jointly exploiting the adaptability of AMC to the wireless channel conditions and the error-correcting capability of ARQ. One of the main drawbacks of existing works is that they relay on first-order *amplitude-based finite-state Markov chains* (AFSMC) to model the wireless fading channel. As it was shown by Tan and Beaulieu in [13], first-order AFSMCs having an exponentially decaying *auto-correlation function* (ACF) can not fit the hypergeometric ACF of the statistical Rayleigh fading process used to model wireless flat-fading channels [14], thus compromising the design of higher layer protocols. In [15]–[17], based on the use of a first-order two-dimensional FSMC model, which is able to improve the ACF fitting of the first-order AFSMC, we proposed a novel cross-layer analytical framework for AMC-based wireless systems using either infinitely persistent or truncated Type-I hybrid *forward error correction* (FEC)/ARQ.

In Type-I Hybrid FEC/ARQ schemes, both error detection and FEC bits are added to each packet prior to transmission. When a received codeword is detected in error, if the number of errors is within the designed error-correcting capabilities of the code, the errors are corrected; otherwise, the received data is discarded and a retransmission is requested by the receiver. A more sophisticated form of hybrid FEC/ARQ schemes is known as *hybrid ARQ* (HARQ) [18]. In Type-I HARQ, if the receiver fails to decode a packet, any previously received signal is stored in a buffer and a retransmission request is fed back to the transmitter, that will send the same coded packet again. At the receiver side, the optimal solution is to combine these multiple signals according to the *maximal ratio combining* (MRC) principle [19], [20]. The type-I HARQ with MRC is often referred to as the *Chase combining* (CC) scheme.

The main contribution of this paper is the generalization of the analytical tools proposed in [11], [12], [16], [17] to AMC/HARQ-CC wireless systems. Using this approach, analytical expressions for performance metrics are derived, which allow the formulation of a cross-layer design, conceived as a constrained optimization problem, that can be used to exploit the joint impact on *Quality-of-Service* (QoS) performance measures of both AMC at the physical layer and truncated HARQ-CC based error control at the *data link control* (DLC) layer.

The rest of this paper is organized as follows. In Section II the system model and assumptions are introduced. In Section III our proposed Markov chain based model is presented and analytical expressions for the performance parameters are derived. A cross-layer optimization strategy to support QoS-guaranteed traffic is proposed in Section IV. Numerical results to assess the validity of our model and to illustrate the system performance are presented in section V. Finally, VI provides some concluding remarks.

II. System model and assumptions

As in [4]–[6], a point-to-point wireless packet communication system is considered. The processing unit at the data link layer is a packet of fixed size equal to N_b bits, and the processing unit at the physical layer is a frame composed by a variable number of packets that depends on the *transmission mode* (TM) selected by the AMC scheme. The link is assumed to support QoS-guaranteed traffic characterized by a maximum average packet delay $D_{l\max}$ and a target link layer packet loss rate $P_{l\max}$.

At the transmitter side, the HARQ controller manages a buffer (queue) that operates in a *first-in-first-out* (FIFO) mode and can store up to $\overline{Q}$ packets. We set the maximum number of ARQ retransmissions to N_r. Packets will be removed from the buffer either after being successfully received by

TABLE I
TM WITH CONVOLUTIONALLY CODED MODULATION.

	Mode 1	Mode 2	Mode 3	Mode 4	Mode 5	Mode 6	Mode 7
Modulation	BPSK	QPSK	QPSK	16QAM	16QAM	64QAM	64QAM
Code rate $R_c^{(n)}$	1/2	2/3	5/6	2/3	5/6	3/4	5/6
R_n (bits/symbol)	1/2	4/3	5/3	8/3	10/3	9/2	5
$a_{n,0}$	4447.4	2068.5	514.7	850.9	142.9	101.2	079.5
$g_{n,0}$	11.104	3.315	1.759	0.816	0.339	0.123	0.085
$\gamma_{p_{n,0}}$ (dB)	-1.212	3.623	5.502	9.172	11.660	15.750	17.118

the mobile host or after $N_r + 1$ failed attempts. The AMC scheme is assumed to have a set $\boldsymbol{\mathcal{M}} = \{0, \ldots, M-1\}$ of M transmission modes, each of which corresponding to a particular combination of modulation and coding strategies, including the case in which the transmitter does not transmit.

Without loss of generality, convolutionally coded M-QAM schemes adopted from IEEE 802.16 standard [21] will be used in the AMC pool. All possible TMs (except the non-transmission mode) are listed in Table I. In this case, when using transmission mode $n \in \boldsymbol{\mathcal{M}}$, a rate-1/2 convolutional encoder generates a sequence $\tilde{\boldsymbol{b}} = \{\tilde{b}_l\}_{l=1}^{2N_b}$ of encoded bits and, after puncturing, the system transmits $N_c^{(n)} = N_b/R_c^{(n)}$ coded bits per packet, where $R_c^{(n)}$ denotes the code rate obtained after puncturing when using TM n. In HARQ schemes based on the CC strategy the same puncturing pattern is applied for each (re)transmission. For a generic packet, the sequence of punctured coded bits corresponding to (re)transmission $i \in \{0, \ldots, N_r\}$ can be denoted as $\boldsymbol{b}^{(i)} = \{b_l^{(i)}\}_{l=1}^{N_c^{(n)}}$. These punctured coded bits are mapped onto a sequence of symbols $\boldsymbol{s}^{(i)} = \{s_k^{(i)}\}_{k=1}^{N_c^{(n)}/\log_2 \mathrm{M}}$ which are selected from the M-QAM constellation corresponding to TM n. Moreover, the number of transmitted packets per frame depends on the TM n and it is given by $p_n = bR_n$, where R_n denotes the number of information bits per symbol used by TM n and b is a parameter which is up to the designer's choice. For convenience, we will consider that $p_0 < \cdots < p_{M-1}$, with $p_0 = 0$ (i.e., transmission mode 0 corresponds to the absence of transmission) and $p_{M-1} \triangleq \mathcal{C}$.

A Rayleigh block-fading channel model has been adopted [22], in which the channel gain h_ν corresponding to the νth frame transmission is characterized as a zero-mean circularly symmetric complex Gaussian random variable with unit power. That is, it is assumed that the frame duration T_f is much smaller than the coherence time of the channel. Furthermore, although the channel is assumed to remain invariant over at least one time frame interval while it is allowed to vary across successive frame intervals, it is also highly probable that it will remain practically invariant over a large number of successive frame intervals.

The received signal corresponding to transmitted symbol $s_k^{(i)}$, $k = 1, \ldots, N_c^{(n)}/\log_2 \mathrm{M}$, can be expressed as

$$r_k^{(i)} = s_k^{(i)} h_i + n_{i,k},$$

where, by convenient abuse of notation, h_i denotes the channel gain of the frame period corresponding to the ith (re)transmission and $n_{i,k}$ is a zero-mean circularly symmetric complex Gaussian noise with variance $N_0/2$ per dimension. The instantaneous received *signal-to-noise ratio* (SNR) during the νth frame transmission is defined as $\gamma_\nu = E_s|h_\nu|^2/N_0$, which is distributed according to the probability density function

$$p_{\gamma_\nu}(\gamma) = \frac{1}{\overline{\gamma}}\, e^{-\gamma/\overline{\gamma}}, \quad \gamma \geq 0,$$

where $\overline{\gamma} = E\{\gamma_\nu\} = E_s/N_0$ is the average received SNR and E_s is the average power of the received signal. According to [4], when implementing the AMC strategy, the entire SNR range is partitioned into a set of nonoverlapping intervals defined by the partition

$$\boldsymbol{\Gamma}^m = \{[\gamma_0^m, \gamma_1^m), [\gamma_1^m, \gamma_2^m), \ldots, [\gamma_{M-1}^m, \gamma_M^m)\}$$

and mode n is selected when $\gamma_\nu \in \left[\gamma_n^m, \gamma_{n+1}^m\right)$.

Assuming perfect *channel state information* (CSI) to be available at the receiver side, the HARQ-CC scheme combines multiple received signals according to the MRC principle. Thus, assuming without loss of generality that the 0th puncturing pattern has been used in all (re)transmissions, the combined signal after i (re)transmissions can be expressed as

$$\hat{r}_k^{(i)} = \sum_{j=0}^{i} r_k^{(j)} h_j^* = s_k^{(0)} \rho_i + \upsilon_k^{(i)},$$

where $\rho_i = \sum_{j=0}^{i} |h_j|^2$ and $\upsilon_k^{(i)}$ is a zero-mean circularly symmetric complex Gaussian noise with variance $\sigma_{\upsilon,i}^2 = \rho_i N_0$. The *logarithmic likelihood ratio* (LLR) corresponding to bit $b_l^{(0)}$ mapped onto symbol $s_k^{(0)}$ on the ith (re)transmission can be expressed as

$$\begin{aligned}\lambda_l^{(i)} &= \log \frac{Pr\{b_l^{(0)} = 1 | \hat{r}_k^{(i)}, \rho_i\}}{Pr\{b_l^{(0)} = 0 | \hat{r}_k^{(i)}, \rho_i\}} \\ &= \log \frac{\sum_{\hat{s}_k \in S_{l,i}^{(1)}} \exp\left(-|\hat{r}_k^{(i)} - \hat{s}_k \rho_i|^2/\sigma_{\upsilon,i}^2\right)}{\sum_{\hat{s}_k \in S_{l,i}^{(0)}} \exp\left(-|\hat{r}_k^{(i)} - \hat{s}_k \rho_i|^2/\sigma_{\upsilon,i}^2\right)},\end{aligned}$$

where $S_{l,i}^{(0)}$ and $S_{l,i}^{(1)}$ are, respectively, the sets of symbols $\hat{s}_k$ with the bit indexed by l, corresponding to the ith retransmission, equal to zero or one. These LLRs are subsequently depunctured to obtain the sequence $\tilde{\boldsymbol{\lambda}}^{(i)} = \{\tilde{\lambda}_l^{(i)}\}_{l=1}^{2N_b}$ that is then passed to the soft Viterbi decoder.

When using TM n on the ith (re)transmission, and with the assumption of a slow block-fading channel model, the instantaneous *packet error rate* (PER) at the output of the

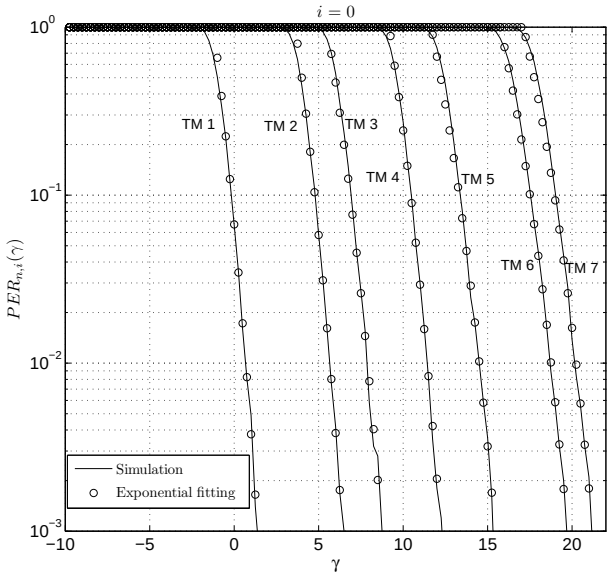


Fig. 1. Instantaneous PER fitting curves.

soft Viterbi decoder can be approximated as

$$\text{PER}_{n,i}(\gamma) \approx \begin{cases} 1 & ,0 \leq \gamma < \frac{\gamma_{p_{n,0}}}{i+1} \\ a_{n,0} e^{-g_{n,0}(i+1)\gamma} & ,\gamma \geq \frac{\gamma_{p_{n,0}}}{i+1} \end{cases}$$

for the HARQ-CC strategy. The variables $a_{n,0}$, $g_{n,0}$ and $\gamma_{p_{n,0}}$, listed in Table I, are the fitting parameters for TM n and transmission number 0 with a packet length of $N_b = 1080$ bits. These parameters have been obtained by least-squares fitting the above approximate expression of the PER to the curves obtained through simulation. Numerical results have been obtained as the ratio between the erroneously transmitted packets after transmission number 0 using TM n and the overall number of transmitted packets. It is clear from Fig. 1, that both curves are close to each other, which justifies the utilization of the exponential expression as an approximation of the instantaneous PER.

After soft Viterbi decoding, an error detection process (using, for instance, a CRC code) is performed and the corresponding ACK/NACK message is fed back to the ARQ controller. Given the short length of the ACK/NACK messages and the use of a high degree of FEC protection, an error-free and instantaneous ARQ feedback channel will be assumed in this paper.

III. Discrete time Markov chain model and analysis

A. Arrival process

As in [16], it is assumed in this paper that the packet generation model adheres to a special case of the discrete *batch Markovian arrival process* (D-BMAP) [23], which is characterized by a transition probability matrix

$$\boldsymbol{U} = \sum_{a=0}^{\infty} \boldsymbol{U}_a = \begin{bmatrix} u(0,0) & \cdots & u(\mathcal{A}-1,0) \\ \vdots & & \vdots \\ u(0,\mathcal{A}-1) & \cdots & u(\mathcal{A}-1,\mathcal{A}-1) \end{bmatrix},$$

where $u(a_\mu, a_{\mu'})$ denotes the probability of a transition from phase a_μ to phase $a_{\mu'}$ with a batch arrival of size a_μ new packets. The sub-stochastic matrices $\boldsymbol{U}_a$, for all $a \in \{0, \ldots, \mathcal{A}-1\}$ are constructed by keeping only the $(a+1)$th row of $\boldsymbol{U}$ and setting all other rows to zero, and by definition of the D-BMAP, $\boldsymbol{U}_a = \boldsymbol{0}$ for all $a \geq \mathcal{A}$.

Owing to the Markovian property of the arrival process we have that $\boldsymbol{\omega} = \boldsymbol{\omega}\boldsymbol{U}$ and $\boldsymbol{\omega}\boldsymbol{1}_{\mathcal{A}} = 1$, where $\boldsymbol{\omega}$ denotes the D-BMAP steady-phase probability vector and $\boldsymbol{1}_{\mathcal{A}}$ is an all-ones column vector of length $\mathcal{A}$. Then the average arrival rate λ can be calculated as

$$\lambda = \boldsymbol{\omega} \sum_{a=0}^{\mathcal{A}-1} a\, \boldsymbol{U}_a \boldsymbol{1}_{\mathcal{A}}.$$

B. Two-dimensional Markov channel modeling

Let us consider the Rayleigh block-fading channel quantities γ_ν and $\delta_\nu = \gamma_{\nu-1} - \gamma_\nu$. Let us also partition the ranges of γ_ν and δ_ν into sets of nonoverlapping two-dimensional cells defined by the partitions

$$\boldsymbol{\Gamma}^c = \left\{ [\gamma_0^c, \gamma_1^c), [\gamma_1^c, \gamma_2^c), \ldots, [\gamma_{K-1}^c, \gamma_K^c) \right\}$$

with $\gamma_0^c = 0$ and $\gamma_K^c = \infty$, and $\boldsymbol{\Delta} = \{(-\infty, 0), [0, \infty)\}$, respectively. The partition $\boldsymbol{\Gamma}^c$ is designed using the methodology introduced in our companion paper [16]. Thus, a first-order two-dimensional Markov channel model can be defined where each state of the channel corresponds to one of such cells. That is, the Markov chain state of the channel at time instant $t = \nu T_f$ can be denoted as $\boldsymbol{\zeta}_\nu = (\chi_\nu, \Delta_\nu)$, $\nu = 0, 1, \ldots, \infty$, where $\chi_\nu = k$ if and only if $\gamma_k^c \leq \gamma_\nu < \gamma_{k+1}^c$ and $\Delta_\nu = 0$ (or $\Delta_\nu = 1$) if and only if $\delta_\nu < 0$ (or $\delta_\nu \geq 0$).

C. Physical layer two-dimensional Markov model

Keeping in mind both the TM selection process used by AMC scheme and the first-order two-dimensional Markov channel model, let us now partition the range of γ_ν into the set of non-overlapping intervals defined by the partition

$$\boldsymbol{\Gamma}^{m,c} = \left\{ [\gamma_0^{m,c}, \gamma_1^{m,c}), [\gamma_1^{m,c}, \gamma_2^{m,c}), \ldots, [\gamma_{N_{\text{PHY}}-1}^{m,c}, \gamma_{N_{\text{PHY}}}^{m,c}) \right\}$$

with $\gamma_0^{m,c} = 0$ and $\gamma_{N_{\text{PHY}}}^{m,c} = \infty$, where each partition interval $[\gamma_k^{m,c}, \gamma_{k+1}^{m,c})$ is characterized by a particular combination of TM and channel state. As in Subsection III-B, let us also consider the partition of δ_ν into the set of nonoverlapping intervals $\boldsymbol{\Delta} = \{(-\infty, 0), [0, \infty)\}$. Using this two-dimensional partitioning, a first-order two-dimensional Markov model for the physical layer can be defined where each state corresponds to one of such two-dimensional rectangular-shaped cells. Furthermore, the physical layer Markov chain state at time instant $t = \nu T_f$ can be denoted as $\boldsymbol{\varsigma}_\nu = (\varphi_\nu, \Delta_\nu)$, $\nu = 0, 1, \ldots, \infty$, where $\varphi_\nu \in \{0, \ldots, N_{\text{PHY}} - 1\}$ denotes the combination of TM and channel state in this frame interval and $\Delta_\nu \in \{0, 1\}$ is used to denote the *up* or *down* characteristic of the instantaneous SNR in time frame interval $t = (\nu - 1)T_f$ (if $\gamma_\nu < \gamma_{\nu-1}$ then the instantaneous SNR is descending and it can be tagged as *down*; on the contrary, if $\gamma_\nu \geq \gamma_{\nu-1}$ then

the instantaneous SNR is ascending and it can be tagged as *up*).

At any time instant $t = \nu T_f$ the physical-layer state can be univocally characterized by an integer number $n_\nu = 2\varphi_\nu + \Delta_\nu$ and obviously, $n_\nu \in \{0, \ldots, 2N_{\text{PHY}} - 1\}$. The physical layer will be in a state $n \in \{0, \ldots, 2N_{\text{PHY}} - 1\}$ with a steady-state probability $P^{\text{PHY}}(n)$, that can be calculated using [16, eqs. (8)-(9)], and each of these states will be characterized by a conditional average packet error rate for the ith (re)transmission given by

$$\overline{PER}_{n,i}^{\text{PHY}} = \begin{cases} \dfrac{\int_{\gamma_{n/2}^{m,c}}^{\gamma_{n/2+1}^{m,c}} \int_0^x PER_{\beta_n,i|i-1}(x) p_{\gamma_\nu,\gamma_{\nu-1}}(x,y) dy dx}{P^{\text{PHY}}(n)}, & n \text{ even} \\ \dfrac{\int_{\gamma_{(n-1)/2}^{m,c}}^{\gamma_{(n+1)/2}^{m,c}} \int_x^{+\infty} PER_{\beta_n,i|i-1}(x) p_{\gamma_\nu,\gamma_{\nu-1}}(x,y) dy dx}{P^{\text{PHY}}(n)}, & n \text{ odd} \end{cases}$$

where β_n denotes the TM corresponding to the nth physical layer state, $p_{\gamma_\nu,\gamma_{\nu-1}}(x,y)$ is the joint pdf of the random variables γ_ν and $\gamma_{\nu-1}$, and $PER_{n,i|i-1}(\cdot)$ represents the probability that the ith transmission attempt fails conditioned on that the previous transmissions have been erroneous, that is,

$$PER_{n,i|i-1}(\gamma) = \frac{PER_{n,i}(\gamma)}{PER_{n,i-1}(\gamma)}.$$

Furthermore, the physical-layer FSMC will be characterized by a transition probability matrix

$$\boldsymbol{P}_s = \left[P_s(n_\mu, n_{\mu'})\right]_{n_\mu, n_{\mu'}=0}^{2N_{\text{PHY}}-1},$$

whose elements can be calculated using [16, eqs. (11)-(15)]. In this paper, the steady-state probabilities, the conditional average packet error rates and the state-transition probabilities have all been computed either numerically or by simulation. Clarke's statistical Rayleigh fading process, characterized by a maximum normalized Doppler frequency $f_d T_f$, has been used to model the wireless flat-fading channel [14].

D. Embedded Markov chain

The queueing process induced by both the truncated HARQ protocol and the AMC scheme can be formulated in discrete time with one time unit equal to one frame interval. The system states are observed at the beginning of each time unit. Let $\sigma_\nu = (\mathbf{q}_\nu, a_\nu, \varphi_\nu, \Delta_\nu)$ denote the system state at time instant $t = \nu T_f$, where $\mathbf{q}_\nu = (q_{\nu,0}, \ldots, q_{\nu,N_r})$ denotes the queue state at this time instant, with $q_{\nu,i}$ denoting the number of packets in the queue that have been already transmitted i times and $Q_\nu \triangleq \sum_{i=0}^{N_r} q_{\nu,i} \in \{0, \ldots, \overline{Q}\}$ denoting the total number of packets in the queue, $a_\nu \in \{0, \ldots, \mathcal{A} - 1\}$ represents the phase of the D-BMAP, $\varphi_\nu \in \{0, \ldots, N_{\text{PHY}} - 1\}$ represents the combination of TM and channel state in this frame interval and $\Delta_\nu \in \{0, 1\}$ is used to denote the *up* or *down* characteristic of the instantaneous SNR in time frame interval $t = (\nu - 1)T_f$. If we just look at the set of time instants $t = \nu T_f$, $\nu = 0, 1, \ldots, \infty$, the transitions between states are Markovian. Therefore, an embedded Markov chain can be used to describe the underlying queueing process. The state space of this embedded finite state Markov chain is $\boldsymbol{\mathcal{S}} = \{\mathcal{S}_n\}_{n=1}^{N_s}$ with size

$$N_s = 2N_{\text{PHY}}\mathcal{A}\sum_{k=0}^{\overline{Q}} \binom{k + N_r}{k}.$$

The transition probability from state $\mathcal{S}_\mu = (\mathbf{q}_\mu, a_\mu, n_\mu) \in \boldsymbol{\mathcal{S}}$ to state $\mathcal{S}_{\mu'} = (\mathbf{q}_{\mu'}, a_{\mu'}, n_{\mu'}) \in \boldsymbol{\mathcal{S}}$, where $n_\mu = 2\varphi_\mu + \Delta_\mu$ and $n_{\mu'} = 2\varphi_{\mu'} + \Delta_{\mu'}$ can be written as

$$P_{\mathcal{S}_\mu, \mathcal{S}_{\mu'}} = u(a_\mu, a_{\mu'}) P_s(n_\mu, n_{\mu'}) P_{\mathbf{q}_\mu, \mathbf{q}_{\mu'}|a_\mu, n_\mu},$$

where $P_{a_\mu, a_{\mu'}}$ denotes the transition probability between D-BMAP phases a_μ and $a_{\mu'}$, which can be obtained from matrix $\boldsymbol{U}$, $P_{n_\mu, n_{\mu'}}$ is the physical layer transition probability between states n_μ and $n_{\mu'}$, which can be derived from matrix $\boldsymbol{P}_s$, and

$$P_{\mathbf{q}_\mu, \mathbf{q}_{\mu'}|a_\mu, n_\mu} = \prod_{i=0}^{N_r} P_{q_{\mu,i}, q_{\mu',i}|a_\mu, n_\mu}$$

corresponds to the queue transition probability from state $\mathbf{q}_\mu$ to state $\mathbf{q}_{\mu'}$ when the D-BMAP is in phase a_μ and the physical layer state is n_μ.

Consider that the system state is $\mathcal{S}_\mu$ and that $Q_{\mu,i} = \sum_{l=i}^{N_r} q_{\mu,l}$ represents the number of packets in the queue that have already been transmitted i or more times (obviously, $Q_{\mu,0} = Q_\mu$). Let $\tau_\mu = \min\{Q_\mu, c_{n_\mu}\}$ denote the number of transmitted packets, $\tau_{\mu,i} = \min\{q_{\mu,i}, \tau_\mu - Q_{\mu,i+1}\}$ the number of transmitted packets among those in the queue that have been already transmitted i times and $\epsilon_{\mu,i}$ the number of packets erroneously transmitted among those in the queue that have been already transmitted i times. Using this notation, the feasible queue transitions can be expressed as

$$q_{\mu',N_r} = \begin{cases} q_{\mu,N_r} - \tau_\mu & , \tau_\mu \le q_{\mu,N_r} \\ \epsilon_{\mu,N_r-1} & , \tau_\mu > q_{\mu,N_r} \end{cases}$$

$$q_{\mu',i} = \begin{cases} q_{\mu,i} & , \tau_\mu \le Q_{\mu,i+1} \\ Q_{\mu,i} - \tau_\mu & , Q_{\mu,i+1} < \tau_\mu \le Q_{\mu,i} \\ \epsilon_{\mu,i-1} & , \tau_\mu > Q_{\mu,i} \end{cases}$$

for $i \in \{1, \ldots, N_r - 1\}$, and

$$q_{\mu',0} = \begin{cases} \min\left\{\overline{Q} - Q_{\mu',1}, q_{\mu,0} + a_\mu\right\} & , \tau_\mu \le Q_{\mu,1} \\ \min\left\{\overline{Q} - Q_{\mu',1}, Q_\mu + a_\mu - \tau_\mu\right\} & , Q_{\mu,1} < \tau_\mu \le Q_\mu. \end{cases}$$

Consequently, by defining $\mathcal{P}_y^x(z) \triangleq \binom{x}{y} z^y (1-z)^{x-y}$, and assuming a slow block-fading channel, the state transition probabilities can be safely approximated as

$$P_{q_{\mu,N_r}, q_{\mu',N_r}|a_\mu, n_\mu} = \begin{cases} 1 & , \begin{array}{l} q_{\mu',N_r} = q_{\mu,N_r} - \tau_\mu \\ \tau_\mu \le q_{\mu,N_r} \end{array} \\ \mathcal{P}_{q_{\mu',N_r}}^{\tau_{\mu,N_r-1}}\left(\overline{PER}_{n_\mu,N_r-1}^{\text{PHY}}\right) & , \begin{array}{l} \tau_\mu > q_{\mu,N_r} \\ \tau_{\mu,N_r-1} \ge q_{\mu',N_r} \end{array} \\ 0 & , \text{ otherwise} \end{cases}$$

$$P_{q_{\mu,i},q_{\mu',i}|a_\mu,n_\mu} = \begin{cases} 1 & , \ q_{\mu,i}=q_{\mu',i} \\ & \ \tau_\mu \le Q_{\mu,i+1} \\ 1 & , \ Q_{\mu,i+1}<\tau_\mu \le Q_{\mu,i} \\ & \ q_{\mu',i}=Q_{\mu,i}-\tau_\mu \\ \mathcal{P}_{q_{\mu',i}}^{\tau_{\mu,i-1}}\left(\overline{PER}_{n_\mu,i-1}^{\text{PHY}}\right) & , \ \tau_\mu > Q_{\mu,i} \\ & \ \tau_{\mu,i-1}\ge q_{\mu',i} \\ 0 & , \ \text{otherwise} \end{cases}$$

for $i \in \{1,\ldots,N_r-1\}$, and

$$P_{q_{\mu,0},q_{\mu',0}|a_\mu,n_\mu} = \begin{cases} 1 & , \ \tau_\mu \le Q_{\mu,1} \\ & \ q_{\mu',0}=\min\left\{\overline{Q}-Q_{\mu',1}, q_{\mu,0}+a_\mu\right\} \\ 1 & , \ Q_{\mu,1}<\tau_\mu \le Q_\mu \\ & \ q_{\mu',0}=\min\left\{\overline{Q}-Q_{\mu',1}, Q_\mu+a_\mu-\tau_\mu\right\} \\ 0 & , \ \text{otherwise.} \end{cases}$$

To derive the system performance measures, we need to obtain the steady-state probability vector, which can be calculated using the fact that the transition probability matrix $\boldsymbol{P}$ and steady-state probability vector $\boldsymbol{\pi} = \begin{bmatrix}\pi_{\mathcal{S}_1} & \cdots & \pi_{\mathcal{S}_{N_s}}\end{bmatrix}$ satisfy $\boldsymbol{\pi P} = \boldsymbol{\pi}$ along with the normalization condition $\boldsymbol{\pi}\mathbf{1}_{N_s} = 1$.

E. Packet loss rate and throughput

The number of lost packets due to buffer overflow when the system changes from state $\mathcal{S}_\mu$ to state $\mathcal{S}_{\mu'}$ is given by

$$N_{l_{BO}|\mathcal{S}_\mu,\mathcal{S}_{\mu'}} = \begin{cases} \max\{0, Q_{\mu',1}+q_{\mu,0}+a_\mu-\overline{Q}\} & , \tau_\mu \le Q_{\mu,1} \\ \max\{0, Q_{\mu',1}+Q_\mu-\tau_\mu+a_\mu-\overline{Q}\} & , \tau_\mu > Q_{\mu,1}. \end{cases}$$

Therefore, the average number of lost packets due to buffer overflow can be calculated as

$$\bar{N}_{l_{BO}} = \sum_{\mu=1}^{N_s}\sum_{\mu'=1}^{N_s} \pi_{\mathcal{S}_\mu} P_{\mathcal{S}_\mu,\mathcal{S}_{\mu'}} N_{l_{BO}|\mathcal{S}_\mu,\mathcal{S}_{\mu'}}$$

and the packet loss rate $P_{l_{BO}}$ (measured in packets per frame) can then be obtained as

$$P_{l_{BO}} = \frac{\bar{N}_{l_{BO}}}{\lambda}.$$

The number of lost packets due to exceeding the maximum number of allowed retransmissions when the system state is $\mathcal{S}_\mu$ can be calculated as

$$N_{l_{\text{ARQ}}|\mathcal{S}_\mu} = \sum_{l=0}^{\tau_{\mu,N_r}} l\ \mathcal{P}_l^{\tau_{\mu,N_r}}\left(\overline{PER}_{n_\mu,N_r}^{\text{PHY}}\right)$$

with $\tau_{\mu,N_r} = \min\{q_{\mu,N_r}, c_n\}$, and the corresponding average number of lost packets can be obtained as:

$$\bar{N}_{l_{\text{ARQ}}} = \sum_{\mu=1}^{N_s} \pi_{\mathcal{S}_\mu} N_{l_{\text{ARQ}}|\mathcal{S}_\mu}.$$

Accordingly, the probability of packet loss due to exceeding N_r retransmissions can be expressed as

$$P_{l_{\text{ARQ}}} = \frac{\bar{N}_{l_{\text{ARQ}}}}{\lambda}.$$

In our finite buffering truncated ARQ-based error control system, the packet loss rate P_l (measured in packets per frame) can be expressed as $P_l = P_{l_{\text{BO}}} + P_{l_{\text{ARQ}}}$, and given the packet loss rate P_l, the average throughput can be calculated as $\eta = \lambda(1-P_l)$.

F. Average queue length and average packet delay

Using the well-known Little's formula [24], the average delay for our embedded Markov chain can be calculated as

$$D_l = \frac{L_q}{\lambda(1-P_{l_{BO}})},$$

where L_q denotes the average number of packets in the queue that can be obtained as

$$L_q = \sum_{\mu=1}^{N_s} \pi_{\mathcal{S}_\mu} Q_\mu.$$

IV. Cross-layer optimization

As shown in previous sections, given a maximum afforded queue length $\overline{Q}$, an average SNR $\bar{\gamma}$ and a normalized maximum Doppler frequency $f_d T_f$, performance measures of the system like, for instance, throughput, average packet delay or packet loss rate, are a function of the AMC transmission mode switching levels $\boldsymbol{\Gamma}^m \in \mathbb{R}_+^{M+1}$, where $\mathbb{R}_+$ denotes the set of non-negative real numbers, and the measured or estimated arrival packet rate $\lambda \in \boldsymbol{\Theta}$, where $\boldsymbol{\Theta}$ is the range of feasible arrival rate values. Therefore, if the objective of the link adaptation scheme is to maximize the average throughput when supporting QoS-guaranteed traffic characterized by a maximum packet loss rate $P_{l\max}$ and a maximum average packet delay $D_{l\max}$, the system needs to jointly optimize the selected protocol parameters at the physical and data link control layers by solving the cross-layer optimization problem

$$\left(\boldsymbol{\Gamma}_{\text{opt}}^m, \lambda_{\text{opt}}\right) = \arg \max_{\boldsymbol{\Gamma}^m \in \mathbb{R}_+^{M+1}, \lambda \in \boldsymbol{\Theta}} \eta\left(\boldsymbol{\Gamma}^m, \lambda\right)$$

subject to the constraints

$$P_l\left(\boldsymbol{\Gamma}_{\text{opt}}^m, \lambda_{\text{opt}}\right) \le P_{l\max}, \quad D_l\left(\boldsymbol{\Gamma}_{\text{opt}}^m, \lambda_{\text{opt}}\right) \le D_{l\max}.$$

The analytical expressions for η, P_l and D_l do not leave much room for developing efficient algorithms in solving our constrained optimization problem. However, considering that $\boldsymbol{\Gamma}^m$ and λ lie in a bounded space $\mathbb{R}_+^{M+1} \times \boldsymbol{\Theta}$, we could resort to a multidimensional exhaustive search to numerically solve the proposed cross-layer optimization problem. In order to simplify this multidimensional optimization approach, let us define the AMC switching thresholds as the instantaneous SNR values for which the value of $PER_{n,N_r} = P_0$, that is,

$$\gamma_n^m = \frac{1}{(N_r+1)g_{n,0}} ln\left(\frac{a_{n,0}}{P_0}\right)$$

for $n = 1,\ldots,M-1$, with $\gamma_0^m = 0$, and $\gamma_M^m = \infty$. In this case, the simplified constrained optimization problem can be formulated as

$$\left(P_{0\text{opt}}, \lambda_{\text{opt}}\right) = \arg \max_{P_0 \in \mathbb{R}_+, \lambda \in \boldsymbol{\Theta}} \eta\left(P_0, \lambda\right)$$

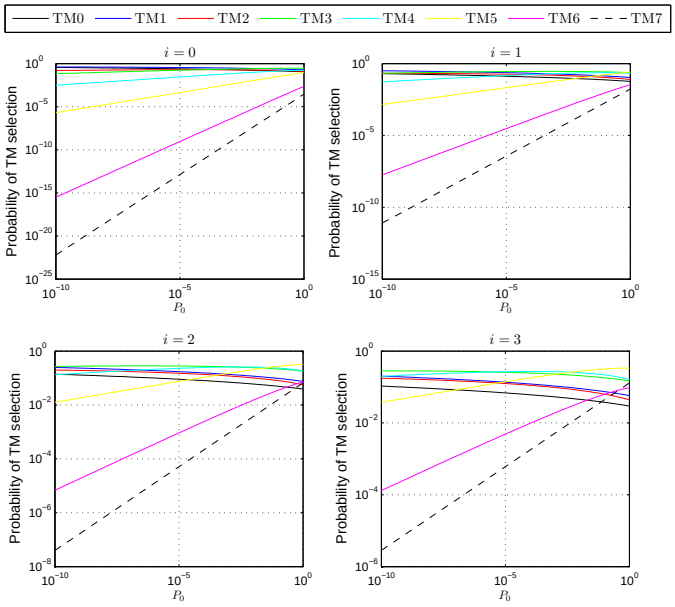


Fig. 2. TM selection probabilities vs. target PER with $\overline{\gamma} = 8$ dB.

subject to the constraints

$$P_l\left(P_{0\text{opt}}, \lambda_{\text{opt}}\right) \leq P_{l\max}, \quad D_l\left(P_{0\text{opt}}, \lambda_{\text{opt}}\right) \leq D_{l\max}.$$

Obviously, because P_0 and λ lie in a bounded space $\mathbb{R}_+ \times \boldsymbol{\Theta}$, we can resort to a 2-D exhaustive search to numerically solve the proposed cross-layer optimization problem.

V. Numerical results

In order to verify the validity of the proposed cross-layer framework, analytical results obtained with the 2D-FSMC model will be confronted with computer simulation results obtained using Clarke's statistical Rayleigh model. Unless otherwise specified, numerical results correspond to the following default parameters: a normalized maximum Doppler frequency $f_d T_f = 0.02$, an average received SNR $\overline{\gamma} = 8$ dB, a buffer size $\overline{Q} = 8$, a number of channel states $K = 5$, a parameter $b = 6$ and a DBMAP either characterized with the transition probability matrix

$$\boldsymbol{U} = \begin{bmatrix} 0.8 & 0.1 & 0.05 & 0.05 \\ 0.05 & 0.8 & 0.1 & 0.05 \\ 0.05 & 0.05 & 0.8 & 0.1 \\ 0.05 & 0.05 & 0.1 & 0.8 \end{bmatrix}$$

or parameterized to obtain a truncated Poisson process with variable arrival rate λ. Only the subset of transmission modes from TM0 to TM5 adopted from IEEE 802.16 standard has been considered, given the low probability of selection of higher TMs, as illustrated in Fig. 2.

The dependence of the average packet loss rate P_l, as well as of its two components $P_{l_{BO}}$ and $P_{l_{ARQ}}$, on the target average PER P_0, is depicted in Figs. 3, 4 and 5, respectively. The analysis of these graphs reveals that higher P_0 values entail an increase in the packet loss rate due to exceeding the maximum number of allowed retransmissions $P_{l_{ARQ}}$. On

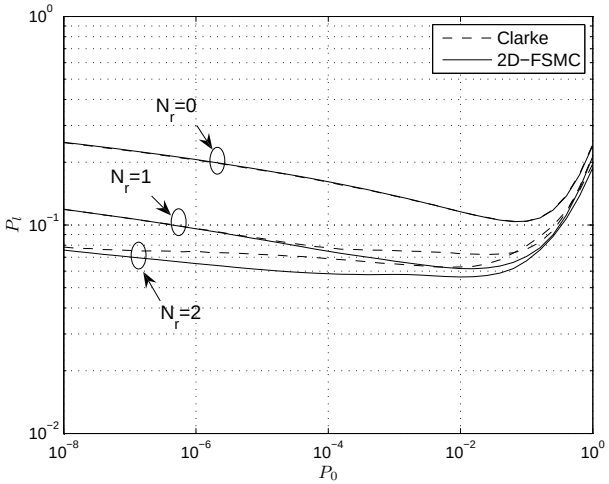


Fig. 3. Average packet loss rate vs. target PER.

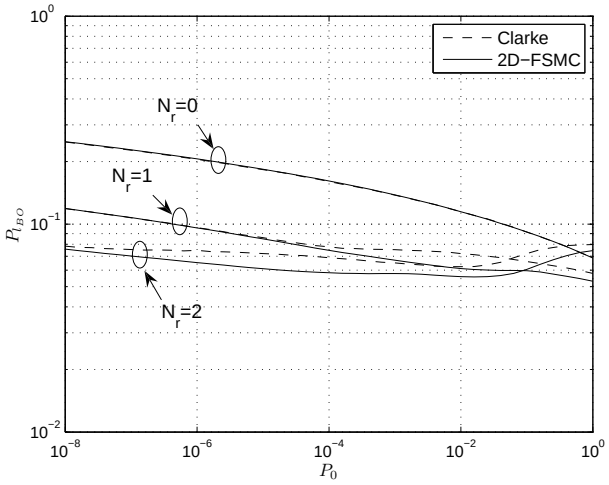


Fig. 4. Average packet loss rate due to buffer overflow vs. target PER.

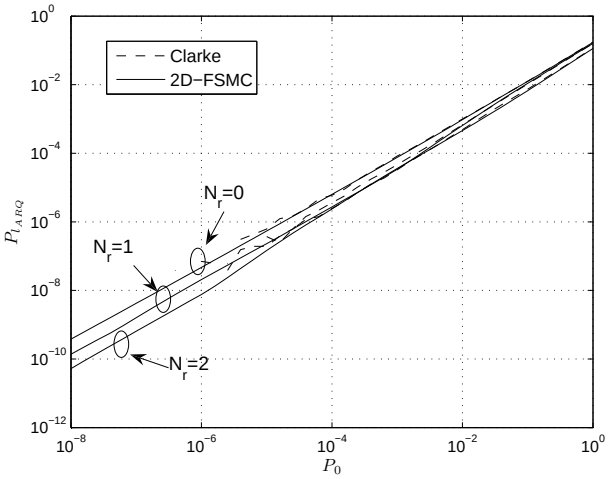


Fig. 5. Average packet loss rate due to exceeding N_r vs. target PER.

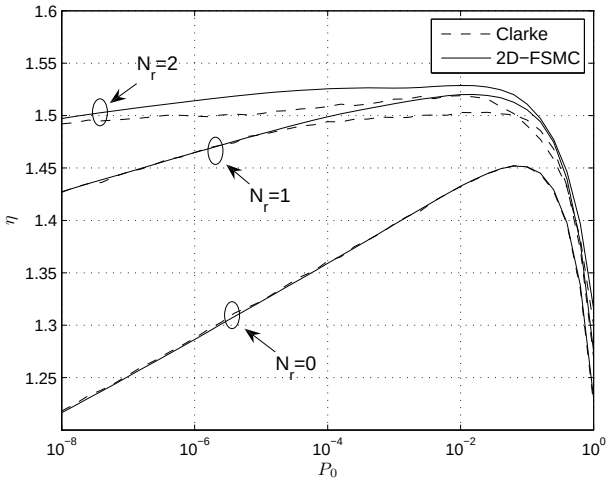


Fig. 6. Average throughput vs. target PER.

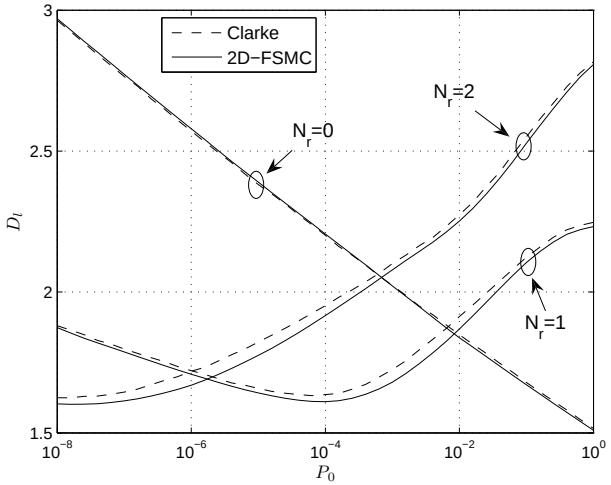


Fig. 7. Average packet delay vs. target PER.

the contrary, it also implies the utilization of higher order TMs, which lead to an increment of the queueing service rate and, consequently, to a decrease in the buffer overflow probability $P_{l_{BO}}$. Nevertheless, it can be perceived that when the number of allowed retransmissions N_r raises, the increase of the service rate cannot cope with the huge number of required retransmissions, implying that more packets remain in the queue and $P_{l_{BO}}$ increases accordingly. A decrease in $P_{l_{BO}}$ and $P_{l_{ARQ}}$ is obtained when higher N_r values are allowed.

Figures 6 and 7 show an increment in the maximum throughput η and a reduction in the minimum delay D_l as the number of allowed retransmissions is increased; however, the most significant gain is obtained in going from $N_r = 0$ to $N_r = 1$, and the advantage of using higher N_r values becomes marginal. These results are aligned with those obtained in [17]. As it can be observed, in all cases the behaviour of the simulation of a FIFO queuing system under a truncated HARQ-CC protocol and with a physical layer based on Clarke's model is faithfully reproduced by the presented analytical physical-link layer 2D-FSMC model. The shape and location of the

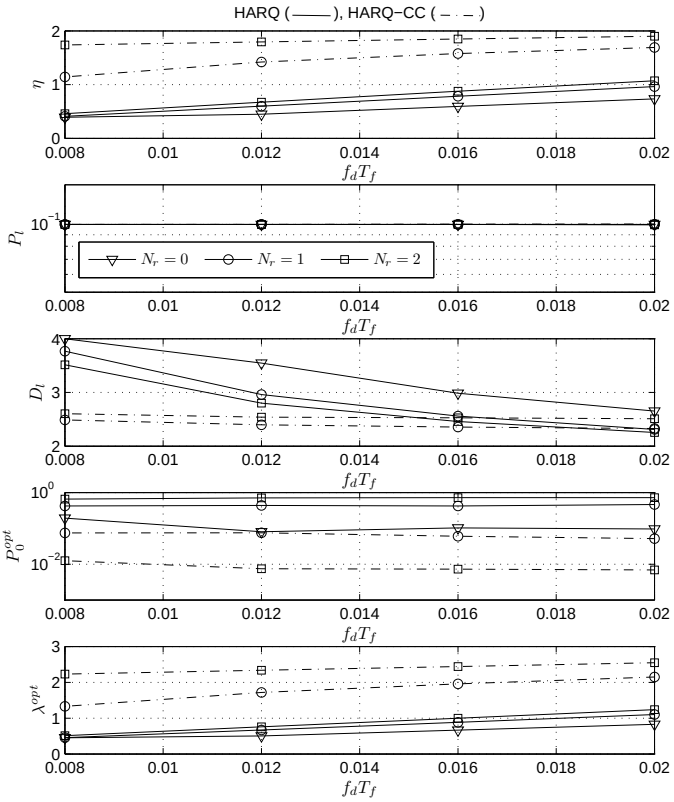


Fig. 8. Optimization vs. Maximum normalized Doppler frequency.

minimum of the curves obtained by simulation (Clarke's) coincide with those obtained using the proposed analytical model (2D-FSMC), which is particularly important to ensure an optimal cross-layer design.

QoS-guaranteed traffic characterized by a maximum average packet loss rate $P_{l_{\max}} = 0.1$ packets/frame and a maximum average packet delay $D_{l_{\max}} = 4$ frames has been considered with the objective of analyzing the dependence of the proposed cross-layer design on the maximum normalized Doppler frequency f_dT_f, with an average received SNR $\overline{\gamma} = 6$ dB. Traffic has been generated using a truncated-Poisson process with a truncation length equal to 3 packets and, thus $\mathbf{\Theta} = (0, 3]$. Figure 8 plots the dependence on the maximum normalized Doppler frequency of the obtained QoS parameters η, P_l and D_l, as well as the optimum values of the target PER P_0^{opt} and arrival rate λ^{opt}. It can be observed that for higher f_dT_f values, which correspond to better channel conditions, the optimum sustainable arrival rate λ^{opt} increases while ensuring the fulfillment of both QoS requirements.

The dependence of this cross-layer design on the average SNR with a normalized maximum Doppler frequency $f_dT_f = 0.022$ is depicted in Fig. 9, where the considered QoS parameters are $P_{l_{\max}} = 0.01$ packets/frame and $D_{l_{\max}} = 1.4$ frames. It can be inferred from the shape of the curves that for higher $\overline{\gamma}$ values, which lead to the use of higher order TMs and imply a decrease in P_l and D_l, a better throughput can be achieved. It can be clearly observed in both figures that when using the HARQ-CC scheme with $N_r = 1$, the optimum

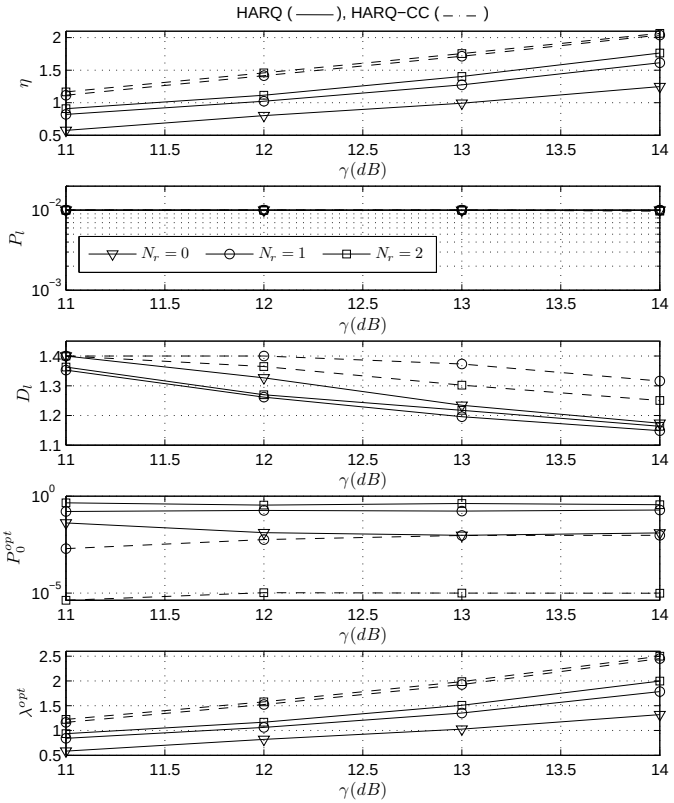


Fig. 9. Optimization vs. Average SNR.

arrival rate λ^{opt} is much greater than when the classical Type-I Hybrid FEC/ARQ scheme is utilized, even with $N_r = 2$. In short, both pictures reveal a significant improvement in the maximum achieved throughput when using the HARQ-CC error control protocol in comparison to the classical Type-I Hybrid FEC/ARQ scheme.

VI. Conclusion

We have proposed a novel link level queueing model that generalizes the analytical tools presented in our previous contribution [17] to AMC/HARQ-CC wireless systems. Using our proposed Markov chain-based models for the wireless fading channel and the queueing process, analytical expressions for performance metrics have been derived. The analytical link level queueing model has then been used to formulate a cross-layer design conceived as a constrained optimization problem to exploit the joint impact on QoS performance of both AMC and HARQ-CC-based error control. Numerical examples have shown that the derived performance metrics of our analytical model faithfully reproduce simulation results based on Clarke's statistical Rayleigh fading model. Furthermore, they have brought to light the improvement in the maximum achieved throughput when the HARQ-CC scheme is used. The ongoing work is now focused on extending the proposed queueing model to include cooperative ARQ schemes.

Acknowledgments

This work has been supported in part by the MEC and FEDER under project COSMOS (TEC2008-02422).

References

[1] S. Shakkottai, T. S. Rappaport, and P. C. Karlsson, "Cross-layer design for wireless networks," *IEEE Commun. Magazine*, vol. 41, pp. 74–80, Oct. 2003.

[2] V. Srivastana and M. Motani, "Cross-layer design: a survey and the road ahead," *IEEE Commun. Magazine*, vol. 43, pp. 112–119, Dec. 2005.

[3] V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Commun.*, pp. 3–11, Feb. 2005.

[4] Q. Liu, S. Zhou, and G. B. Giannakis, "Cross-layer combining of adaptive modulation and coding with truncated ARQ over wireless links," *IEEE Trans. Wireless Commun.*, vol. 3, no. 5, pp. 1746–1755, Sept. 2004.

[5] ——, "Queuing with adaptive modulation and coding over wireless links: cross-layer analysis and design," *IEEE Trans. Wireless Commun.*, vol. 4, no. 3, pp. 1142–1153, May 2005.

[6] ——, "Cross-layer scheduling with prescribed QoS guarantees in adaptive wireless networks," *IEEE JSAC*, vol. 23, no. 5, pp. 1056–1066, May 2005.

[7] L. B. Le, E. Hossain, and A. S. Alfa, "Service differentiation in multirate wireless networks with weighted round-robin scheduling and ARQ-based error control," *IEEE Trans. Commun.*, vol. 54, no. 2, pp. 208–215, Feb. 2006.

[8] ——, "Radio link level performance evaluation in wireless networks using multi-rate transmission with ARQ-based error control," *IEEE Trans. Wireless Commun.*, vol. 5, no. 10, pp. 2647–2653, Oct. 2006.

[9] F. Ishizaki and G. U. Hwang, "Cross-layer design and analysis of wireless networks using the effective bandwidth function," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3214–3219, Sept. 2007.

[10] M. Poggioni, L. Rugini, and P. Banelli, "Analyzing performance of multi-user scheduling jointly with AMC and ARQ," in *Proc. IEEE GLOBECOM*, Nov. 2007, pp. 3483–3488.

[11] X. Wang, Q. Liu, and G. B. Giannakis, "Analizing and optimizing adaptive modulation coding jointly with ARQ for QoS-guaranteed traffic," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 710–720, Mar. 2007.

[12] L. B. Le, E. Hossain, and T. Le-Ngoc, "Interaction between radio link level truncated ARQ, and TCP in multi-rate wireless networks: a cross-layer performance analysis," *IET Commun.*, vol. 1, no. 5, pp. 821–830, 2007.

[13] C. C. Tan and N. C. Beaulieu, "On first-order Markov modeling for the Rayleigh fading channel," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2032–2040, 2000.

[14] R. H. Clarke, "A statistical theory of mobile radio reception," *Bell System Tech. Journal*, vol. 47, no. 6, pp. 957–1000, Sept. 1968.

[15] J. Ramis, L. Carrasco, and G. Femenias, "A two-dimensional Markov model for cross-layer design in AMC/ARQ-based wireless networks," in *Proc. IEEE GLOBECOM*, Dec. 2008, pp. 4637–4642.

[16] G. Femenias, J. Ramis, and L. Carrasco, "Using two-dimensional Markov models and the Effective-Capacity approach for Cross-Layer design in AMC/ARQ-based wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4193–4203, Oct. 2009.

[17] J. Ramis, G. Femenias, and L. Carrasco, "Cross-layer Design of Multi-rate Wireless Networks based on link-layer Truncated ARQ," in *Proc. IWCLD*, Jun. 2009.

[18] J.-F. T. Cheng, "On the coding gain of incremental redundancy over chase combining," *IEEE Transactions on Communications*, vol. 54, no. 6, pp. 1017–1029, Jun. 2006.

[19] D. Chase, "A combined coding and modulation approach for communications over dispersive channels," *IEEE Transactions on Communications*, vol. 21, no. 3, pp. 159–174, Mar. 1973.

[20] ——, "Code combining: A maximum-likelihood decoding approach for combining an arbitrary number of noisy packets," *IEEE Transactions on Communications*, vol. 33, no. 5, pp. 385–393, May 1985.

[21] IEEE, *802.16: Standard for Local and metropolitan area networks*. New York: IEEE, 2004.

[22] E. Biglieri, G. Caire, and G. Taricco, "Limiting performance of block fading channels with multiple antennas," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1273–1289, May 2001.

[23] C. Blondia, "A discrete time batch markovian arrival process as b-isdn traffic model," *Belgian Journal of Operations Research, Statistics and Computer Science*, vol. 32, no. 3/4, pp. 3–23, 1993.

[24] L. Kleinrock, *Queuing Systems*. New York: Wiley, 1975, vol. I.

Combinación de Protocolos de Encaminamiento en Redes Inalámbricas Malladas

Alfonso Ariza, Alicia Triviño Cabrera, Eduardo Casilari
Departamento Tecnología Electrónica,
Universidad de Málaga
29071 Málaga
{aarizaq, atc, ecasilari}@uma.es

***Resumen*- Wireless mesh networks are supported by a network of static routers called (or backbone) usually intended to provide Internet access to mobile terminals. In order to discover and maintain the paths among these static routers, multiple routing strategies have been proposed for wireless mesh networks. The convenience of each strategy strongly depends on the mobility of the nodes that compose the paths. This paper presents a novel technique by which routers in the backbone are simultaneously equipped with two routing protocols. The use of each protocol depends on the destination of the path to discover. In particular, mesh routers implement a reactive scheme and a proactive protocol. The execution of the proactive routing protocol is restricted to the backbone so only stable routes are periodically updated. On the other hand, the reactive protocol is kept to maintain the compatibility with the mobile nodes (which can form a widely extended MANET) and to search routes to a mobile destination. Aiming at guaranteeing the IP compatibility, the combination of the two protocols is carried out in the MAC layer. Simulation results show the goodness of the proposal in terms of data packet losses, data delay and protocol overhead.**

***Palabras Clave*- redes mesh, protocolo de encaminamiento, comunicaciones inalámbricas.**

I. INTRODUCCIÓN

Las redes inalámbricas han experimentado un gran auge en las últimas décadas. Su popularidad se debe principalmente a que este tipo de comunicaciones reduce los costes de la infraestructura a desplegar. Además, estas redes aumentan la flexibilidad del sistema que puede incluir nuevos terminales y permitir su movilidad a través de una técnica de gestión sencilla. La expansión de los sistemas inalámbricos, en especial los basados en 802.11 [1], ha repercutido en la aparición de servicios específicos destinados a terminales inalámbricos. En este sentido, existen en la actualidad proveedores de Internet que proporcionan un acceso inalámbrico al servicio basado en 802.11 en Cambridge [2] o en Alemania [3]. Una posible implementación de este tipo de acceso la constituyen las redes inalámbricas malladas.

Una red inalámbrica mallada o red *mesh* se compone de *routers* inalámbricos conectados entre sí siguiendo un esquema multisalto [4]. Esta estructura estática se denomina *backbone*. Un terminal móvil se conecta a alguno de estos elementos del *backbone* de igual forma que lo hace a un *router* de acceso. En algunas ocasiones, se contempla que los terminales móviles accedan al router a través de una red MANET (*Mobile Ad Hoc Network*) formada por los terminales inalámbricos. Además, gracias a la comunicación multisalto dentro del *backbone*, el terminal móvil puede acceder a Internet si en la red mallada existe una pasarela o Gateway con conexión a Internet.

Generalmente, entre el *router* al que se conecta el terminal móvil y el *Gateway* es posible establecer múltiples caminos. El responsable de descubrir, seleccionar y mantener el camino que se elige para la comunicación es el protocolo de encaminamiento. Para redes inalámbricas malladas, se han propuesto una multitud de protocolos de encaminamiento. Muchos de ellos son adaptaciones de los propuestos para redes móviles ad hoc o MANET (*Mobile Ad hoc Networks*) como OLSR (*Optimized Link State Routing*) [5], DYMO [6]. Sin embargo, estos protocolos pueden optimizarse para aprovechar las posiciones fijas de los nodos así como la energía de la que disponen los *routers* en comparación con los terminales inalámbricos. En este sentido, han surgido protocolos de encaminamiento específicamente diseñados para las redes inalámbricas malladas. Entre ellos destaca el 802.11s [7] que constituye un estándar del IEEE para este tipo de redes. Según dichas especificaciones, las tareas de encaminamiento se transfieren a la Capa 2 para garantizar la compatibilidad con los puntos de acceso. Siguiendo el estándar, los nodos deben disponer obligatoriamente del protocolo HWMP (*Hybrid Wireless Mesh Protocol*) y, opcionalmente, pueden contar además con el protocolo RA-OLSR (*Radio Aware Optimized Link State Routing*). El protocolo HWMP ofrece dos modos de funcionamiento complementarios: un esquema proactivo y otro reactivo. El procedimiento proactivo se utiliza exclusivamente para mantener las rutas desde cualquier nodo (terminal móvil o *router* del *backbone*) al *Gateway* y viceversa. Por otro lado, el esquema reactivo se utiliza para establecer la ruta entre dos nodos cualesquiera. Por consecuencia, las rutas hacia el *Gateway* se calculan periódicamente en la red porque se asume que la mayoría del flujo de tráfico va desde o hacia dicho elemento.

Sin embargo, las rutas hacia el *Gateway* que se descubren según este esquema no son siempre estables. Esto se debe a que las rutas pueden contener un terminal móvil. Bajo estas circunstancias, la sobrecarga ocasionada para el descubrimiento de las rutas no resultaría siempre rentable. En este artículo, proponemos que las rutas que se descubran periódicamente sean aquellas formadas exclusivamente por

nodos del *backbone*. Como estas rutas son estables y son capaces de ofrecer una mayor capacidad, es recomendable tenerlas siempre disponibles para priorizar su uso. Para ello, los nodos del *backbone* disponen de un protocolo proactivo. Sin embargo, este tipo de protocolos no es beneficioso para los terminales móviles ya que ofrecen mejores prestaciones cuando ejecutan protocolos reactivos [8]. Para solventar este inconveniente, el esquema que se propone en este artículo combina dos protocolos: uno reactivo y otro proactivo. Los nodos móviles sólo ejecutan el reactivo mientras que los nodos del sistema troncal cuentan con las dos implementaciones. La inclusión de un protocolo reactivo en los *routers* del *backbone* garantiza la integración de los nodos móviles. Con el propósito de analizar las prestaciones que ofrece la solución propuesta, se ha evaluado el protocolo a través de simulaciones. Los resultados indican que el esquema propuesto es capaz de reducir las pérdidas de paquetes de datos, su retardo así como la sobrecarga que ocasiona el protocolo de encaminamiento.

El resto del artículo se estructura tal y como sigue. La Sección 2 presenta una descripción de otros trabajos que analizan la combinación de protocolos en redes inalámbricas malladas. La Sección 3 describe el esquema propuesto en este artículo. A través de las simulaciones que se muestran en la Sección 4, se evalúa el protocolo de encaminamiento. Por último, la Sección 5 muestra las principales conclusiones de nuestro trabajo.

II. Trabajo Relacionado

Existen en la actualidad propuestas que se basan en el uso simultáneo de dos protocolos de encaminamiento en redes inalámbricas malladas. En este sentido, AODV-ST (*Spanning Tree*) combina dos protocolos [9]. En concreto, las rutas hacia el *Gateway* se construyen periódicamente a través de un árbol de búsqueda (*spanning tree*). Por otro lado, AODV se emplea para establecer las rutas entre el resto de nodos. Una aproximación similar es la que sigue el estándar 802.11s [7] con su protocolo HWMP. Como diferencia, la implementación del HWMP se transfiere al nivel 2 para así poder permitir con facilidad el uso de puntos de acceso 802.11.

El trabajo en [10] es una de las primeras propuestas que considera diferente el comportamiento de un nodo móvil. Como en las soluciones anteriores, las rutas desde el *Gateway* hacia un nodo del backbone y viceversa se actualizan periódicamente. Para ello, el Gateway introduce un mensaje RREQ (*Route Request*) con el que se actualiza la ruta desde el nodo receptor al *Gateway*. La principal diferencia reside en que los nodos móviles ignoran este mensaje. Por lo tanto, las rutas que se actualizan periódicamente están formadas exclusivamente por nodos estáticos. Cuando lo necesiten, los nodos móviles ejecutan un protocolo reactivo para descubrir la ruta hacia el *Gateway*.

En [11] se presenta un esquema que combina dos tipos de protocolos para aplicaciones UAV (*Unmanned Aerial Vehicles*). En este tipo de escenarios, la movilidad de los nodos es heterogénea. El protocolo de encaminamiento para cada nodo se elige de acuerdo a sus condiciones de movilidad. En concreto, los nodos aéreos implementan un protocolo reactivo mientras que los terrestres optan por un esquema proactivo.

III. Protocolo Híbrido para Redes Malladas Inalámbricas

En el esquema propuesto, los *routers* del sistema troncal ejecutan simultáneamente dos protocolos de encaminamiento que intercambian información entre sí. En particular, estos dispositivos cuentan con una implementación de un protocolo proactivo y otro reactivo. Por otro lado, los nodos móviles no se modifican por lo que sólo disponen de un protocolo reactivo ad hoc. La elección de este tipo de protocolos para los nodos móviles se justifica en [8] donde se muestra que los protocolos reactivos ofrecen mejores prestaciones que los proactivos cuando los terminales son móviles. En concreto, hemos seleccionado DYMO como protocolo reactivo y OLSR como proactivo.

Cuando un nodo del *backbone* intenta enviar un paquete, los nodos primero buscan una entrada válida hacia el destino en la tabla de encaminamiento construida por el protocolo proactivo. Si existiese alguna ruta almacenada en dicha tabla, el camino encontrado sería muy estable ya que estaría compuesto exclusivamente por terminales fijos. Conviene, pues, que el tráfico sea encaminado por este tipo de rutas y, por ello, es la tabla de encaminamiento que se consulta en primer lugar.

Por otro lado, cuando un nodo móvil desea enviar un paquete busca una entrada hacia el destino en su tabla de encaminamiento creada por el protocolo reactivo. Si no dispone de ninguna o la que está almacenada es obsoleta, el nodo generará un RREQ (*Route Request*) tal y como se contempla en el comportamiento convencional de un protocolo reactivo. Los nodos móviles que reciben este mensaje lo retransmiten si no conocen ninguna ruta hacia el destino o responde con un RREP (*Route Reply*) con la información de la ruta demandada. Por otro lado, los nodos fijos, al disponer también del protocolo reactivo, también analizan la petición que les llega con el RREQ. En primer lugar, buscan una entrada en la tabla de encaminamiento generada por el protocolo proactivo. Si dispusiese de una entrada para el destino que se busca, el protocolo proactivo envía el RREQ que ha recibido junto con los datos de la ruta de interés al protocolo reactivo. Una vez que llega la petición al protocolo reactivo del nodo estático, éste analiza su propia tabla. Si los dos esquemas (proactivo y reactivo) han encontrado una ruta válida hacia el destino, se selecciona la ruta encontrada por la componente proactivo ya que al considerarse más estable tiene más prioridad. Por otro lado, cuando el protocolo proactivo no cuenta con ninguna ruta, la responsabilidad de encontrar la ruta completa se transfiere completamente al protocolo reactivo. La Fig. 1 muestra cómo se propagan los mensajes RREQ en la red. En este caso, el nodo móvil 1 intenta establecer una ruta con el nodo fijo A. Para ello, retransmite su mensaje de RREQ al nodo móvil 2 a través del que accede al nodo D. Como la ruta que se busca es hacia un nodo fijo, cuando la petición de ruta llega a un nodo fijo, éste es capaz de responder inmediatamente a la petición ya que las rutas entre nodos fijos se actualizan periódicamente. Por otro lado, cuando el nodo móvil 3 desea encontrar la ruta hacia el nodo móvil 4, el mensaje de RREQ se retransmite por la red a través de nodos móviles y fijos.

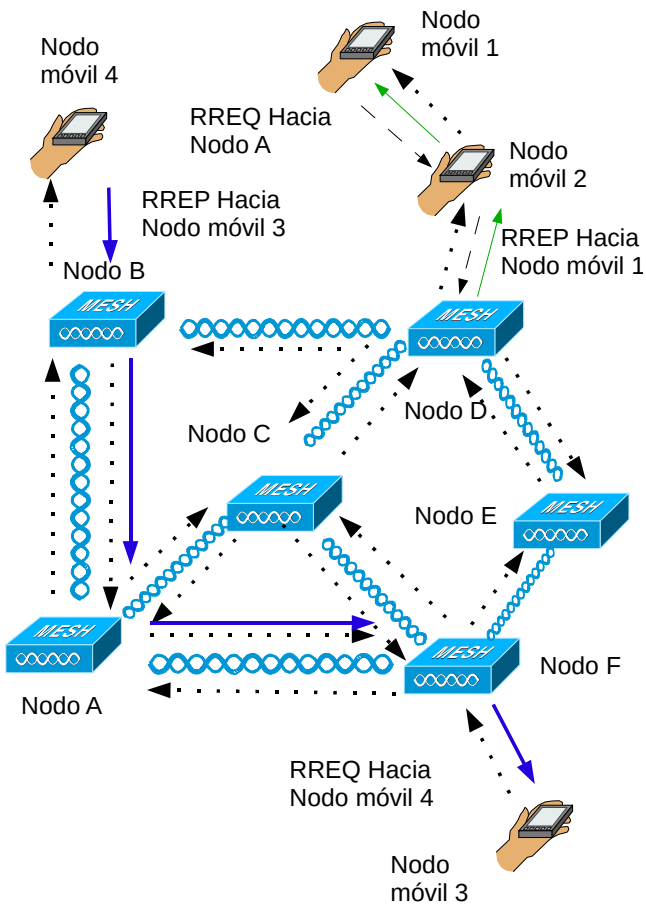


Fig. 1. Retransmisión de los mensajes RREQ en el esquema propuesto.

Con el propósito de ejecutar simultáneamente los dos protocolos de encaminamiento dentro de los *routers* del *backbone*, se ha optado por transferir estos procesos al nivel MAC. A diferencia del nivel IP, en la capa de enlace se permite el uso de varias tablas de transmisión. Siguiendo el funcionamiento de 802.11s [7], las tramas en este nivel cuentan con cuatro direcciones MAC asociadas a la fuente original del dato, al destino final, al siguiente salto y al nodo retransmisor actual. En el proceso de transmisión se actualizan los campos relacionados con el siguiente salto y el nodo retransmisor actual. En concreto, el protocolo de encaminamiento es el responsable de proporcionar la dirección MAC del nodo considerado como siguiente salto. Para averiguar dicha dirección, consulta la información que mantiene en su tabla de encaminamiento (implementado en la capa MAC).

Las tramas de datos cuentan también con estas cuatro direcciones. A diferencia del encaminamiento a nivel IP, esta técnica permite que las tablas de encaminamiento se actualicen con la llegada de datos.

IV. Pruebas y Resultados

Con el objetivo de evaluar las prestaciones que ofrece el protocolo de encaminamiento propuesto, realizamos un estudio comparativo. Para realizar este estudio bajo las mismas condiciones (movilidad, propagación, tráfico, tasa de envío a nivel de enlace, etc.), las simulaciones son necesarias. En particular, nuestro estudio incluye distintos patrones de tráfico con diversas condiciones de movilidad que se evalúan en OMNeT ++ [12].

El área usada para las pruebas comprende una superficie de 2000x2000 m^2. Para las pruebas, se ha dispuesto un *backbone* formado por 49 nodos fijos tal y como aparece en la Figura 2 donde la distancia máxima de transmisión inalámbrica se ha fijado a 250 metros con el modelo de propagación de espacio libre. Además, se añaden 50 nodos móviles que se desplazan según el modelo de movilidad RWP (*Random WayPoint*), un patrón de movilidad ampliamente utilizado para el estudio de redes MANET. De acuerdo a este modelo, una vez que el nodo alcanza el destino, el nodo busca otro punto en el área de simulación al que se dirige con una velocidad constante. El proceso se repite hasta que la simulación termina. Es importante destacar que para nuestras simulaciones hemos particularizado el modelo RWP. En concreto, todos los trayectos se realizan con una velocidad constante que es común para todos los nodos. Además, no se ha incluido ningún tiempo de pausa. Este modelo es poco realista pero puede proporcionarnos el comportamiento de la red bajo un fuerte estrés ya que los enlaces están continuamente rompiéndose y creándose.

Sobre el nivel MAC empleado, se ha optado por el 802.11g [13] con una tasa binaria de 54 Mbits/s. Esta capa se modifica para incluir la técnica de retransmisión propuesta en este artículo. Para ello, los nodos del *backbone* cuentan con el OLSR y DYMO mientras que los nodos móviles sólo ejecutan el protocolo reactivo (DYMO en este caso).

Para cada condición de movilidad, de tráfico y de protocolo realizamos cinco simulaciones con semillas distintas. Las figuras que representan los resultados obtenidos muestran el valor medio del parámetro analizado así como los intervalos de confianza del 95 %.

El resto de los parámetros de la simulación se resume en la Tabla 1.

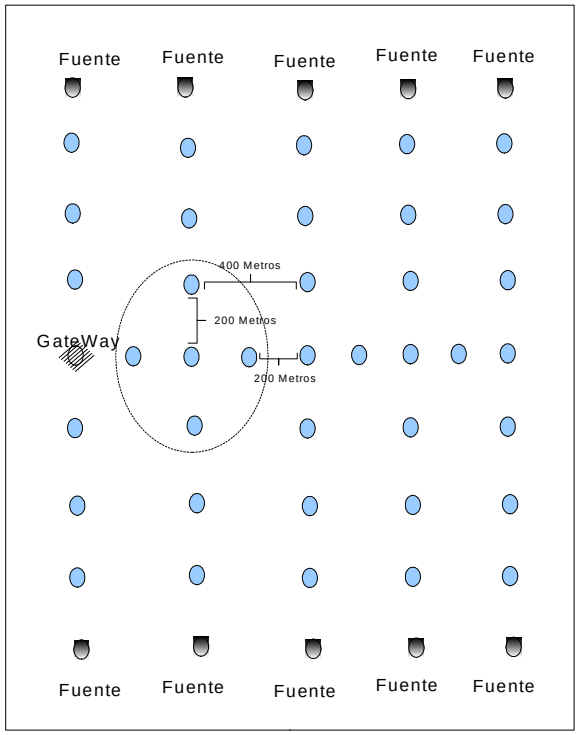


Fig. 2. Estructrura del *backbone* de la red *mesh* evaluada.

Área de simulación	2000x2000 m^2
Número de nodos estáticos	49
Número de nodos móviles	50
Velocidad de los nodos móviles	[1,10] m/s
Tiempo de pausa	0 s
Modelo de propagación	Espacio libre
Rango de transmisión	250 m
Modelo de Interferencias	Aditivo
Capa MAC	802.11g
Retry Limit (Capa MAC)	7
Velocidad de transmisión binaria	54 Mbits/s
Intervalo de actualización del vecindario en OLSR (*Hello interval*)	2 s
Intervalo de actualización entre coordinadores en OLSR (*TC interval*)	5 s
Mantenimiento de enlaces en DYMO	Realimentación por la capa de enlace
Tiempo de vida de las rutas no utilizadas en DYMO	10 s
Inclusión de nodos retransmisores en los paquetes RREQ y RREP	Sí
Tiempo de simulación	3000 s
Ejecuciones por punto	5

Tabla 1. Parámetros de las simulaciones realizadas.

Para cuantificar las prestaciones de la red, se han empleado las siguientes métricas que reflejan la calidad que perciben los usuarios:

- Retardo de los paquetes de datos. Representa el tiempo medio transcurrido desde que se genera un paquete de datos hasta que llega al destino final. En aquellos paquetes
- Porcentaje de pérdida de paquetes de datos.

Nuestro estudio compara las prestaciones de los siguientes esquemas de encaminamiento:

- Protocolo híbrido propuesto. Se trata de la combinación de dos tipos de protocolos (reactivo y proactivo) en los nodos del *backbone* mientras que los nodos móviles sólo ejecutan el protocolo proactivo. La implementación de los dos protocolos se lleva a cabo en la capa MAC.
- Protocolo reactivo implementado a nivel 2.
- Protocolo reactivo implementado a nivel 3.
- Protocolo proactivo implementado a nivel 2.
- Protocolo proactivo implementado a nivel 3.
- Protocolo basado en la construcción de un árbol. Se corresponde con la implementación del protocolo 802.11s cuando el tráfico va hacia o desde el *gateway*.

Respecto al tráfico, la estructura de la Figura 2 muestra qué nodos del *backbone* pueden actuar como fuentes. Al seleccionar un *router* estático como generador de tráfico, emulamos la concentración de tráfico que ocurre cuando varios nodos móviles se conectan a un Punto de acceso. Bajo estas circunstancias, los puntos de acceso publican la dirección MAC de los dispositivos que lo están empleando. Con esta información, otros nodos son capaces de iniciar la comunicación con los nodos que residen en el punto de acceso. Adicionalmente, algunos nodos móviles pueden ser a su vez generadores de tráfico. En concreto, analizamos dos patrones de tráfico distintos. En el patrón 1, el 80 % del tráfico lo generan los nodos móviles. Por otro lado, en el patrón 2, el 80% del tráfico lo inyectan los *routers* estáticos. Para los dos casos, las comunicaciones son bidireccionales aunque las tasas en los dos sentidos difieren. Las fuentes introducen 133.333 paquetes por segundo en la red a través de transferencias UDP. El tamaño de los paquetes de datos es de 512 Bytes.

Como primera parte de nuestro estudio, evaluamos las prestaciones de la red cuando el tráfico es desde o hacia Internet. La red estática dispone de un *gateway* al que hay que acceder para comunicarse con un host externo. Las Figuras 3, 4, 5 y 6 muestran la tasa de entrega de paquetes y el retardo de los paquetes de datos para este tipo de escenarios con los dos patrones de tráfico considerados. Tal y como se obtuvo en trabajos anteriores [8], los protocolos proactivos ofrecen mejores tasas de entrega de paquetes que los reactivos. Por el contrario, los proactivos están asociados a menores retardos ya que las rutas están disponibles. A pesar de esta ventaja, la reducción de la tasa de entrega de paquetes es tan elevada que se desaconseja emplear un protocolo proactivo para las aplicaciones móviles.

La implementación de las tareas de encaminamiento de un protocolo reactivo en el nivel MAC reduce el retardo. Esto se debe a que este tipo de implementación permite que los nodos aprendan rutas incluso cuando retransmiten las tramas de datos. De esta manera, el mantenimiento de las rutas es más frecuente que si se realiza a nivel 3. Como los protocolos proactivos construyen periódicamente las tablas de encaminamiento, esta mejora no puede apreciarse en este tipo de protocolos. Los resultados muestran además que el protocolo basado en árbol logra mejores tasas de entrega de paquetes. Bajo este protocolo, los nodos móviles participan en las rutas sólo como extremos. Por lo tanto, las rutas son más estables y, en consecuencia, las pérdidas ocasionadas por la ruptura de enlaces se reducen.

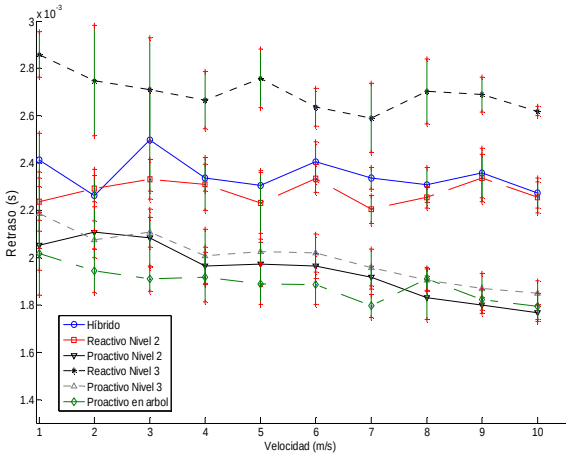


Fig. 3. Retardo extremo a extremo para patrón 1 (80% del tráfico generado por nodos móviles)

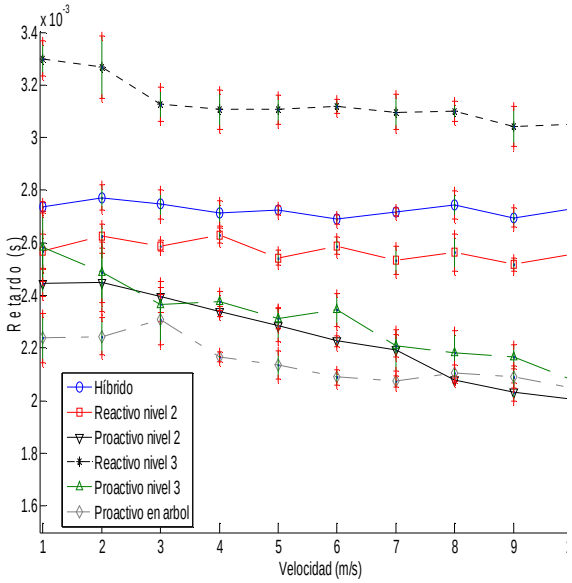


Fig. 4. Retardo extremo a extremo para patrón 2 (80% del tráfico generado por nodos fijos)

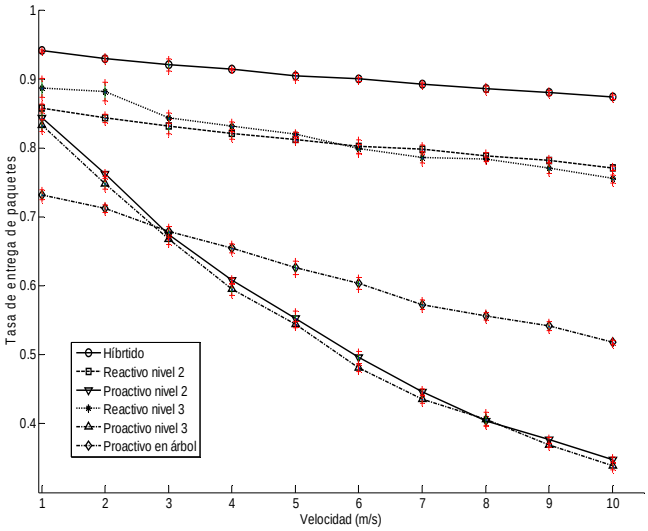


Fig. 6. Tasa de entrega de paquetes para patrón 2 (80% del tráfico generado por nodos fijos)

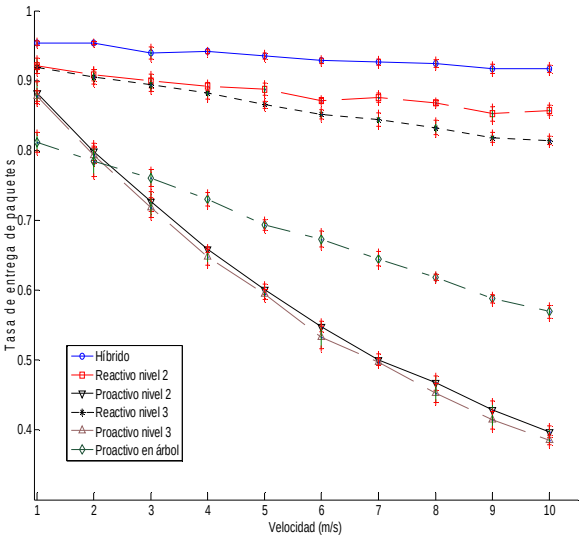


Fig. 5. Tasa de entrega de paquetes para patrón 1 (80% del tráfico generado por nodos móviles)

En estas figuras también se aprecia que el protocolo propuesto consigue un retardo intermedio (entre los obtenidos por los protocolos proactivos y los que se consiguen con los reactivos) pero con una mejora significativa en la tasa de entrega de paquetes. La combinación de protocolos propuesta en este artículo permite que las rutas se compongan de nodos móviles y de nodos estáticos. Las rutas entre los nodos estáticos se descubre a través del protocolo proactivo que ofrece mejores prestaciones que el protocolo reactivo. En cambio, las rutas entre nodos móviles se establecen con los algoritmos reactivos. Con este tipo de algoritmos, la red ofrece mejores prestaciones para los nodos móviles.

Como una segunda parte de nuestro estudio, analizamos las prestaciones de la red cuando el tráfico se intercambia exclusivamente entre los nodos de la red (no necesariamente el *Gateway*). Bajo este tipo de tráfico, 802.11s equivale al protocolo reactivo implementado en la capa MAC. Las Figuras 7 y 8 muestran los resultados obtenidos. Como puede observarse, el protocolo propuesto en este artículo logra mejores tasas de entrega de paquetes al mismo tiempo que consigue decrementar el retardo. Esto se produce porque el protocolo híbrido propuesto calcula periódicamente las rutas estables, esto es, entre los nodos estáticos. Según la implementación sugerida, estas rutas estables tienen prioridad frente a las que se puedan descubrir con el protocolo reactivo. Por lo tanto, las rutas están disponibles al mismo tiempo que presentan una alta fiabilidad (lo que reduce las pérdidas. Esta disponibilidad de rutas estables se traduce en menores retrasos y en menores pérdidas de datos.

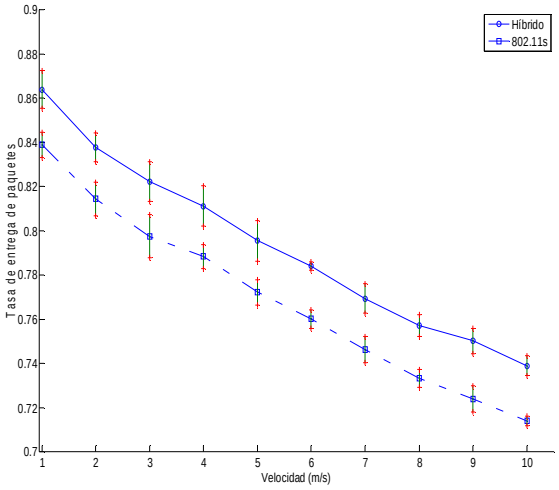


Fig. 7. Tasa de entrega de paquetes cuando el tráfico es entre los nodos del *backbone*.

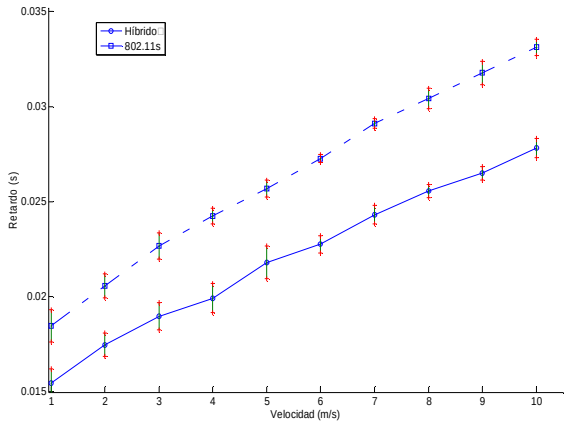


Fig. 8. Retardo extremo a extremo cuando el tráfico es entre los nodos del *backbone*.

V. CONCLUSIONES

Este artículo propone el uso de dos protocolos de encaminamiento (uno proactivo y uno reactivo) en los *routers* que constituyen el *backbone* en las redes inalámbricas malladas. Esta combinación permite que las rutas estables, esto es, las formadas por nodos estáticos, se actualicen periódicamente gracias al esquema proactivo. Por otro lado, las rutas hacia o desde los nodos móviles se construyen con un protocolo reactivo. La evaluación de las prestaciones llevada a cabo mediante simulación muestra que el esquema propuesto es capaz de reducir las pérdidas de datos, su retardo así como la sobrecarga en la red.

El código está públicamente disponible en la dirección http://github.com/inetmanet/inetmanet.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado con fondos del proyecto TEC2009-13763-C02-01.

REFERENCIAS

[1] B. O'Hara, A. Petrick, The 802.11 Handbook: a Designer's Companion, IEEE Press, 1999
[2] http://pdos.csail.mit.edu/roofnet/doku.php
[3] http://start.freifunk.net/
[4] I. F. Ai, X. Wang, W. Wang, "Wireless mesh networks: a survey", Computer Networks, vol. 47, Issue 4, Marzo 2005.
[5] T. Clausen, P. Jacquet, "Optimised Link State Routing", RFC 3626, Octubre 2003.
[6] I. D. Chakeres, C. E. Perkins "Dynamic MANET On-demand Routing Protocol", IETF Internet Draft, draft-ietf-manet-dymo-12.txt (trabajo en progreso), Febrero 2008.
[7] http://grouper.ieee.org/groups/802/11/Reports/tgs_update.htm
[8] A. Ariza, A. Triviño, E. Casilari, J. C. Cano, P. Manzoni, C. Calafate, "Assessing the impact of Link Layer Feedback mechanisms on MANET routing protocols", en 14th IEEE Symposium on Computers and Communications (ISCC 2009), Julio 2009.
[9] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, K. Almeroth, "On the Design and Implementation of Infrastructure Mesh Networks", en IEEE Workshop on Wireless Mesh Networks (WiMesh), Septiembre, 2005.
[10] A. Le, D. Kum, Y. Cho, "An Efficient Hybrid Routing Approach for Hybrid Wireless Mesh Networks", Lecture Notes in Computer Science, vol. 5576, 2009.
[11] N. Peppas, D. Turgut, "A Hybrid Routing Protocol in Wireless Mesh Networks" en Proceedings of Military Communications Conference (MILCOM), Octubre 2007.
[12] http://www.omnetpp.org/
[13] http://www.ieee802.org/11/

Evaluación de los mecanismos de handover implementados en redes comerciales de telefonía móvil

Almudena Díaz Zayas, Pedro Merino Gómez.
Departamento de Lenguajes y Ciencias de la Computación,
Universidad de Málaga
Campus Teatinos, Málaga, 29071 .
almudiaz@lcc.uma.es, pedro@lcc.uma.es.

***Resumen*—En este artículo se presenta un caso de estudio del rendimiento de los mecanismos de handover implementados en redes celulares comerciales. El estudio se lleva a cabo desde el punto de vista del impacto que tienen dichos mecanismos sobre el tráfico de datos. Concretamente, el análisis se centra en la evaluación del impacto de los handovers a nivel IP durante una conexión de datos: pérdidas de paquetes, variaciones del retardo y tiempos de interrupción del tráfico de datos. Adicionalmente se estudia el consumo de potencia durante la ejecución de los handovers, así como los niveles de potencia de señal recibidos en el transcurso de los mismos. Los resultados introducidos en este artículo son el resultado de extensivas pruebas de campo llevadas a cabo en redes comerciales españolas de telefonía móvil.**

***Palabras Clave*—Pruebas de campo, handover, rendimiento, redes de telefonía móvil comerciales**

I. Introducción

En el presente artículo se analiza el estado actual de los mecanismos de gestión de movilidad proporcionados en redes de telefonía móvil comerciales. Los aspectos evaluados se centran en el estudio del impacto sobre el tráfico de datos y en el consumo de potencia.

El impacto de los mecanismos de handover sobre las conexiones de datos en redes inalámbricas ha sido extensivamente estudiado en la literatura científica. Sin embargo, la mayoría de resultados proporcionados se basan en simulaciones [3] [4] [7] o en experimentos de laboratorio llevados a cabo en entornos controlados [5] [6]. Los resultados obtenidos en este tipo de escenario están, normalmente, basados en procesos de handover simplificados para delimitar la complejidad de la simulación o para conseguir una configuración controlable del entorno de pruebas. Por tanto, los resultados de estos trabajos resultan valiosos en una primera fase de evaluación de la tecnología bajo prueba. Pero se necesitan resultados más realistas para ajustar con mayor precisión el correcto funcionamiento de las implementaciones reales de los mecanismos de handover.

Como consecuencia, en una segunda fase del despliegue de una nueva tecnología, las pruebas de campo, las cuales constituyen el punto de partida de este artículo, son necesarias para contrastar los resultados de las simulaciones con datos reales. En [8] los autores se centran en el análisis del rendimiento de los mecanismos de handover para MIPv6 en redes WLAN. En este caso han implementado un banco de pruebas usando ordenadores con el sistema operativo Linux, sin embargo la ejecución de los handovers es forzada mediante ciertas utilidades inalámbricas presentes en Linux. La principal diferencia entre esta aproximación y las pruebas llevadas a cabo en nuestro estudio se encuentra en que en el presente trabajo se monitoriza los handovers de una forma pasiva, en ningún momento se trata de forzar la ejecución de los handovers. Por otro lado nuestro campo de actividad se centra en redes celulares. En [6] los autores se basan en simulaciones para analizar el impacto de las técnicas de soft y softer handover durante una sesión de streaming, mientras que en [9] se estudia el impacto del handover entre sistemas (ISHO) para redes comerciales GPRS y UMTS. La metodología seguida en nuestro artículo difiere del anterior en el protocolo de transporte utilizado. En este trabajo se ha utilizado como protocolo de transporte UDP, mientras que en trabajo citado utilizaban TCP. Mediante el uso de un protocolo como UDP los tiempos y comportamientos debidos a los handovers no se vieran alterados por los mecanismo de control de flujo propios de TCP. De igual forma en [10] se muestran resultados obtenidos de medidas llevadas a cabo en redes GPRS comerciales. Sin embargo se estudian las interrupciones debidas a los cambios de celda tomando como referencia los mensajes de señalización de bajo nivel mientras que este artículo se toma como referencia los instantes en los que se produce algún tipo de interrupción en los flujos de tráfico IP cursado por el usuario. De esta forma se consigue evaluar el impacto de los cambios de celda desde el punto de vista del servicio y de los usuarios finales. Además, a diferencia de lo que ocurre en los tres trabajos referenciados, en este artículo se citan las herramientas y la metodología utilizada, de forma que el estudio pueda ser replicado.

En relación con este último punto, en el presente trabajo se considera de especial relevancia proporcionar una técnica independiente de cualquier aproximación que se quiera testear, de esta forma se obtiene un técnica que permite analizar el comportamiento de cualquier procedimiento de handover en cualquier red inalámbrica. Las pruebas aquí introducidas no se centran en la evaluación de un caso particular de handover. Nuestro objetivo es determinar el rendimiento de los mecanismos de handover implementados en redes reales. La medidas realizadas se extienden también a redes HSDPA.

Para llevar a cabo las medidas se ha hecho uso de SymPA [1], una herramienta que se ejecuta en el propio teléfono móvil y que ha sido desarrollada por nuestro grupo de investigación. Dicha herramienta permite capturar el tráfico IP cursado por

el terminal móvil, detectar los cambios de celda, así como monitorizar los niveles de potencia de señal recibidos y el consumo de batería [2]. Toda la información recopilada durante las pruebas ha sido procesada con herramientas de análisis matemático para obtener las tablas y gráficos mostrados en este artículo. La principal conclusión que se extrae de los resultados obtenidos es que el rendimiento de los distintos mecanismos de handover en redes comerciales de telefonía móvil distan en gran medida de las soluciones de mejora propuestas por los distintos organismos de estandarización. Por tanto, se debe hacer un esfuerzo para trasladar estas mejoras a las implementaciones disponibles en redes reales.

La organización de este artículo es la siguiente: en primer lugar se proporciona una breve introducción sobre los principales mecanismos de gestión de la movilidad usados en redes celulares. A continuación se presenta un conjunto de resultados experimentales referentes al rendimiento de los mecanismos de handover en diferentes contextos y su impacto sobre las comunicaciones de datos en el dominio de la conmutación de paquetes.

II. Mecanismos de gestión de la movilidad en redes celulares

En esta sección se introducen las principales funciones de gestión de movilidad usadas para el manejo de los cambios de ubicación de los dispositivos móviles. Se pueden diferenciar dos tipos de funciones, dependiendo de si el terminal tiene una conexión activa o no.

El protocolo RRC es un protocolo de gestión de capa 3 entre cuyas funcionalidades se encuentran la ejecución de los handovers. Dicho protocolo se basa en una serie de estados de funcionamiento los cuales dependen de si el terminal tiene una conexión activa de datos o no, y del tipo de recursos asignados al usuario. Se dice que el terminal se encuentra en el estado inactivo (IDLE) cuando no existe ninguna conexión activa. En este estado, si el terminal detecta una celda más adecuada, de acuerdo a la configuración de red, se inicia un proceso de actualización de la localización para establecerse en la nueva celda. Durante el proceso de actualización de la ubicación se establece temporalmente una conexión RRC (Radio Resource Control) para el intercambio de la información de señalización. Cuando el terminal de usuario (UE) se encuentra en un estado conectado los mecanismos de gestión de movilidad son distintos. Si existe una conexión RRC activa y existen recursos dedicados asignados al UE los dos procedimiento principales que se aplican son el soft handover (*Active Set Update*) y el hard handover. Si en lugar de estar usando canales dedicados se están usando canales compartidos existen mecanismos específicos, tales como los procedimientos de actualización de celda llevados a cabo por el UE en el estado Cell_FACH (estado orientado al envío de pequeñas cantidades de datos, en el se que comparte canal tanto en el enlace ascendente como en el descendente) o los procedimientos de actualización del área de registro UMTS (UMTS Registration Area -URA-) para el estado Cell_PCH (estado en el cual el terminal no puede recibir datos pero puede ser localizado y avisado de que hay datos para él, en cuyo caso conmutará a un nuevo estado en el cual pueda recibir los datos).

Para la interacción entre diferentes tecnologías de acceso radio se usan dos procedimientos adicionales: handover entre sistemas (inter-system handover) y cambios de celda entre sistemas (inter-system cell reselection). A continuación se resumirá brevemente los mecanismos de señalización implicados en estos procedimientos.

II-A. Procedimientos de gestión de la movilidad

Para iniciar los procedimientos de gestión de la movilidad la red, normalmente, hace uso de la información proporcionada por los dispositivos móviles a través de los mensajes de reporte de medidas. La configuración de los mecanismos de reporte son llevados a cabo por la red mediante elementos específicos de información (IEs) que están contenidos en la información del sistema, que es transmitido por el canal de difusión (broadcast) en la celda, o usando mecanismos de señalización dedicados para el control de las medidas.

Durante la configuración de estas medidas se definen eventos específicos tales como la detección de la celda más adecuada y las condiciones de disparo para que el UE inicie el envió de los informes, que estará basado en la potencia de señal recibida y en la calidad de ésta. Los informes de medidas usualmente contienen los niveles de potencia de señal para todas las celdas monitorizadas. Adicionalmente a la configuración del evento que determina el inicio del envío de informes, también se pude configurar que los informes se envíen periódicamente. Aunque el envió periódico de dichos informes no se espera que se use en redes comerciales debido a que incrementa el consumo de potencia, su uso resulta útil en la ejecución de pruebas de conformidad, ya que permite verificar la precisión de los valores reportados en un entorno radio controlado.

II-B. Active Set Update

Ya que para UMTS se utiliza tecnología WCMDA, un dispositivo móvil puede, simultáneamente, recibir señal (a una misma frecuencia) desde más de una estación base ya que las señales son generadas con códigos de espectro ensanchado ortogonales. Esta interesante característica, proporcionada por el uso de técnicas de multiplexación por código, se usa para suavizar la transición entre celdas cuando existe una conexión dedicada activa, por ejemplo, es posible empezar a recibir datos desde una segunda celda sin tener que parar de recibir los datos de la celda original.

El procedimiento de *Active Set Update* es el encargado del intercambio de la información de señalización requerida para mantener los enlaces con las celdas implicadas en el proceso. En el transcurso de la ejecución de este procedimiento la red envía al UE un mensaje *Active Set Update*, a través de la portadora radio de señalización activa y el UE responde con un mensaje *Active Set Update Complete*, el cual implica la finalización del procedimiento.

II-C. Hard Handover

Los handovers son ejecutados por la red cuando el terminal de usuario envía un informe indicando que ha encontrado una celda más adecuada a la que conectarse. El procedimiento de hard handover se ejecuta cuando la celda destino opera en una banda, frecuencia o modo duplex distinto, o simplemente cuando no hay soporte para soft handover en la red.

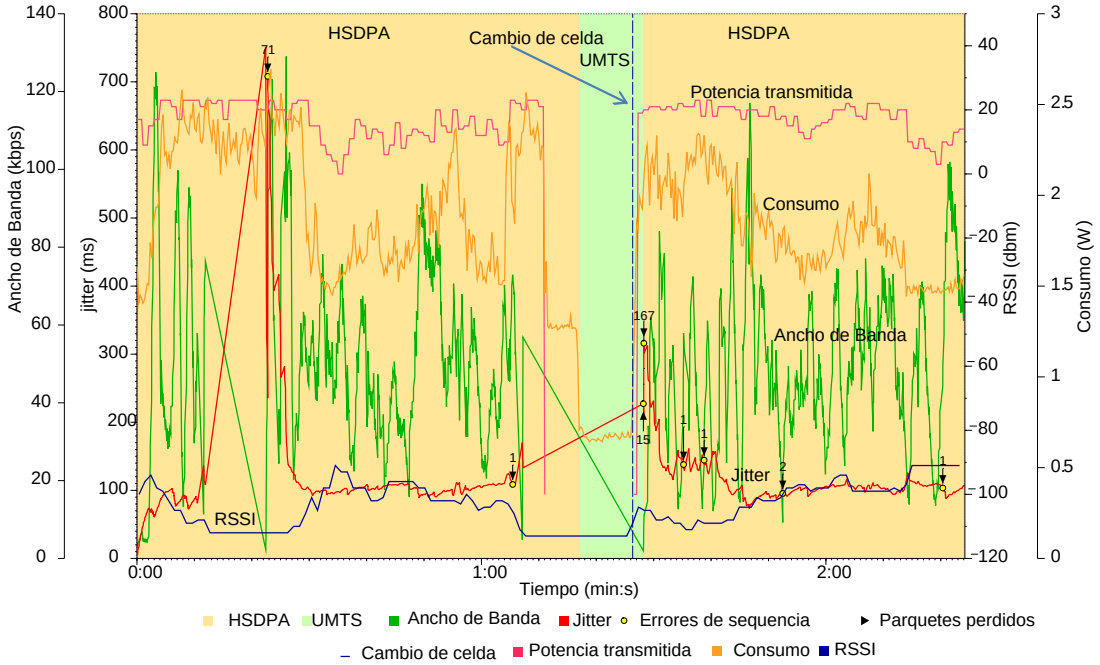


Figura 1. Impacto de las condiciones radio sobre una conexión de datos

Como en el caso del procedimiento *Active Set Update*, el procedimiento de hard handover se ejecuta sólo cuando existe una conexión activa dedicada. Al no haber mensajes de señalización específicos definidos para el hard handover se emplean, para su ejecución, algunos procedimientos RCC de señalización comunes.

II-D. Handover entre sistemas

Un handover entre sistemas tiene lugar cuando el dispositivo móvil cambia de tecnología de acceso mientras existe una conexión activa, por ejemplo de UMTS a GSM o viceversa. En el caso de un handover desde UMTS a GSM el procedimiento se inicia cuando el terminal de usuario reporta que ha encontrado una celda vecina GSM adecuada. Basándose en la información recibida la red decide si el handover debería ser ejecutado. Si es así se negociará con la red GSM la reserva de recursos en la celda destino y se le ordenará al UE que ejecute el handover empezando una nueva conexión con los recursos GSM reservados.

Cuando el UE está conectado pero no esta en el estado Cell_DCH porque no hay una conexión dedicada activa, por ejemplo se encuentra en algunos de los estados Cell_FACH, Cell_PCH, o URA_PCH (la diferencia entre el estado Cell_PCH y el estado URA_PCH es que mientras que en el primero se conoce la ubicación del terminal a nivel de celda en el segundo se conoce la ubicación a nivel de URA), hay procedimientos de gestión de la movilidad específicos para permitir moverse a una nueva celda. Los cambios de celda entre sistemas permiten a un terminal de usuario que se encuentre en cualquier de los estados citados anteriormente cambiar a una tecnología de acceso diferente. Las actualizaciones de celda pueden ser usadas por los UEs conectados a nivel de celda (Cell_FACH O Cell_PCH). Este procedimiento tiene diferentes usos, tales como actualizaciones periódicas de la localización del UE y los cambios de celda, para empezar a transmitir datos en el enlace ascendente o responder a un mensaje de ”paging.enviado por la red. Las actualizaciones del URA son ejecutadas cuando un UE en el estado URA_PCH entra en una nueva celda perteneciente a un URA diferente, por ejemplo, una celda que no contiene el mismo identificador URA asignado al UE en la celda precedente. Este procedimiento es requerido ya que el UE en el estado URA_PCH será únicamente alcanzable por la red si se encuentra emplazado en una celda en la se transmite el identificador URA esperado por el UE.

III. Impacto de los mecanismos de handover sobre las conexiones de datos

El principal efecto de una cambio de celda es la interrupción del servicio durante un intervalo de tiempo y la pérdida potencial de paquetes [10]. Estos parámetros y otros son analizados en la secciones siguientes.

Los resultados proporcionados en este artículo fueron recopilados durante pruebas de campo llevadas a cabo en un vehículo cuya velocidad media de desplazamiento era de 100 Km/h a lo largo de una autovía. Durante dichas pruebas el tráfico cursado por el terminal era tráfico UDP. Para recopilar la información necesaria para analizar el impacto de los mecanismos de handover sobre las conexiones de datos se hace uso de la herramienta SymPA que se ejecuta en el propio terminal móvil. Esta herramienta permite capturar el tráfico IP, medir los niveles de señal recibidos, detectar los cambios de celda y los cambios de tecnología de acceso radio.

En la Fig. 1 se introduce el tipo de correlación que se ha realizado con los datos monitorizados para analizar los handovers. Concretamente la figura 1 pertenece a una sesión de medidas en GPRS. En dicha sesión tiene lugar una primera interrupción de 10 segundos entre los segundos 12 y 22, intervalo en el cual la recepción de paquetes se interrumpe y una vez que se reanuda se detecta una pérdida de 71 paquetes.

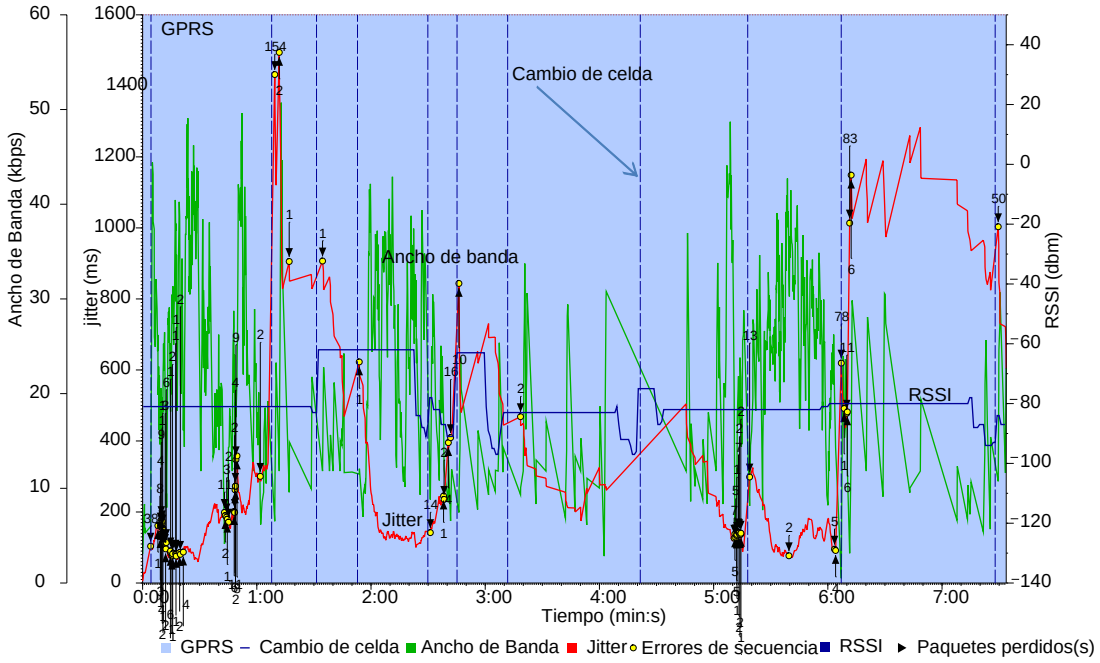


Figura 2. Cambios de celda durante una conexión de datos en un entorno vehicular (GPRS)

Esta interrupción en la recepción de los paquetes de datos está precedida de una variación en la potencia recibida, la cual decrece entre los segundos 2 y 12 desde los -94 dBm hasta un valor mínimo menor que -110 dBm. Al mismo tiempo, la potencia transmitida alcanza un valor máximo de 23 dBm, lo que parece ser el valor máximo, ya que la clase de potencia a la pertenece el dispositivo es la 3, y de acuerdo a las especificaciones de test del 3GPP [11] la máxima potencia medida estaría entre los +21 dBm y los +25 dBm. Un teléfono móvil transmitiendo a su máxima potencia indica que las condiciones del enlace radio ascendente son pobres, puesto que la red le ordena continuadamente que incremente su potencia en transmisión para tratar de mejorar la calidad de la señal que recibe. Pequeñas variaciones de la potencia entorno a su valor máximo en condiciones de niveles bajos de relación señal a ruido pueden aparecer, incluso si el enlace no se ve interrumpido, ya que, de acuerdo a [11], se permite hasta un 30 % de probabilidad de detección errónea de los comandos de control de potencia antes de deshabilitar la transmisión en el enlace ascendente.En esos momentos la potencia consumida alcanza 2.5 vatios, valor considerablemente mayor que los 1.5 vatios mostrados en la parte final de la gráfica, cuando las condiciones radio parecen ser mejores.

Otra interrupción de 21 segundos puede apreciarse entre los instantes de tiempo 1:07 y 1:28. Este tipo de interrupciones es bastante larga y debería ser considerada en el dimensionado de los buffers de aplicación. Durante el transcurso de la interrupción se puede apreciar un cambio temporal de tecnología de acceso radio representado por el cambio del color de fondo. Concretamente se detecta un cambio de HSDPA a UMTS en el instante 1:17 y un cambio de UMTS a HSDPA en el instante 1:26. Adicionalmente en los instantes finales de la interrupción tiene lugar un cambio de celda que viene representado por una línea vertical discontinua. Dicho cambio de celda indica que el dispositivo ha seleccionado una celda

Instante de inicio del cambio de celda	Tiempo transcurrido desde cambio de celda	Tiempo transcurrido desde último paquete IP
6:39:48.957	00:00:00.135	00:00:00.162
6:40:52.359	00:00:01.613	00:00:03.521
6:41:15.923	00:00:03.167	00:00:05.565
6:41:37.454	00:00:00.924	00:00:03.770
6:42:14.407	00:00:01.301	00:00:02.566
6:42:29.739	00:00:00.992	00:00:03.829
6:42:56.344	00:00:06.759	00:00:09.016
6:44:06.19	00:00:24.101	00:00:41.971
6:45:02.461	00:00:01.003	00:00:03.102
6:45:51.594	00:00:00.033	00:00:02.992
6:47:12.471	00:00:01.599	0:00:04.000

Cuadro I
DURACIÓN DE LOS CAMBIOS DE CELDA DURANTE LA CONEXIÓN DE DATOS GPRS REPRESENTADA EN AL FIG. 2

más adecuada en el instante 1:26. El comportamiento tanto de la potencia transmitida como de la recibida antes de la segunda interrupción es similar al observado con anterioridad en la primera interrupción. Sin embargo durante la última interrupción se puede ver que la transmisión ha sido desactivada. Este comportamiento, probablemente, es causado por la detección de un error en el enlace radio lo que provoca la interrupción de las conexiones salientes y motiva la ejecución del procedimiento de actualización de celda (cell update). Esto nos lleva a concluir que la observación de la potencia de señal transmitida y recibida, junto con otros parámetros adicionales, podría ser un instrumento útil para anticipar interrupciones en los servicios de datos. Por otro lado se proporciona, como parte de la metodología utilizada en este trabajo, mecanismos prácticos para llevar a cabo esta monitorización.

En relación con la duración de la interrupción detectada la especificación del 3GPP para el servicio de streaming sobre conmutación de paquetes (PSS) define un valor por defecto de 1 segundos para el buffer de precodificacion. En la práctica la

Instante de inicio del cambio de celda	Tiempo transcurrido desde cambio de celda	Tiempo transcurrido desde último paquete IP
22:41:01.828	00:00:03.497	00:00:24.024
22:41:21.343	00:00:05.584	00:00:13.583
22:41:49.921	00:00:09.024	00:00:30.305
22:41:57.46	00:00:01.926	00:00:00.027
22:42:22.906	00:00:02.572	00:00:18.959

Cuadro II
DURACIÓN DE LOS CAMBIOS DE CELDA DURANTE UNA CONEXIÓN DE DATOS UMTS (FIG. 4)

Instante de inicio del cambio de celda	Tiempo transcurrido desde cambio de celda	Tiempo transcurrido desde último paquete IP
12:45:32.989	00:00:10.739	00:00:16.580
12:45:37.94	00:00:06.669	00:00:00.035
12:45:41.162	00:00:02.611	00:00:00.010

Cuadro III
TIEMPOS DE INTERRUPCIÓN DURANTE LA SESIÓN DE DATOS EN UMTS REPRESENTADA EN LA FIG. 5

duración del buffer de precodificación en recepción se sitúa entorno a los 5-10 segundos [12]. Por tanto la interrupcion detectada en el caso de prueba analizado en esta sección causa el vaciado del buffer de reproducción y por tanto la detención momentánea de la reproducción del vídeo (rebuffering).

En las siguientes subsecciones se utilizará el mismo procedimiento introducido en esta sección para analizar los mecanismos de handover en GPRS, UMTS y HSDPA.

III-A. Handover en redes GPRS

En [10] las pérdidas del enlace radio medidas en una red GPRS real se encuentran en el rango de los 0,8 y los 3,86 segundos, usando como referencia temporal el tiempo transcurrido entre el momento en el que el canal BCCH (Broadcast Control Channel) de la nueva celda es detectado y el instante en el que el UE recibe datos de la nueva celda. En este artículo se han medido las interrupciones provocadas por los handovers a nivel IP obteniendo una duración media de 28,65 para dichas interrupciones, con una alta dispersión.

Un conjunto representativo de los resultados obtenidos durante los experimentos se muestra en la Fig. 2 y en la Tabla I. Concretamente los tiempos obtenidos en situaciones en las cuales tienen lugar varios cambios de celda de forma consecutiva presentan una alta variabilidad, como se muestra en la Tabla I. En [10] se menciona que los altos tiempos obtenidos están asociados a los procedimientos de actualización de área. Por tanto se recomienda una cuidadosa planificación de las áreas de localización.

III-B. Handovers en redes UMTS

La Fig. 3 muestra el comportamiento esperado para un handover en el cual hay muy pocos paquetes perdidos (sólo 3) y la interrupción del flujo de datos se encuentra entorno a los 8.5 segundos.

Sin embargo, generalmente, el rendimiento de los procedimientos de handover analizados en las redes reales no es tan bueno como el representado en la Fig. 3. En líneas generales los resultados obtenidos son muy variables respecto a la duración de las interrupciones y las pérdidas de paquetes. Como se muestra en la Fig. 4, los handovers tienen un gran impacto en la tasa de transmisión, produciendo una interrupción de decenas de segundos en el flujo de datos, como se muestra en la Tabla II. En este caso los niveles de señal recibidos son extremadamente bajos llegando a perderse la cobertura entorno al minuto 1:17. Esta interrupción tiene asociada una ráfaga de pérdidas de 483 paquetes.

El valor medio obtenido para la duración de los handovers en UMTS es de 10.54 segundos, aunque como ya se discutió previamente existe nuevamente un alto grado de dispersion en los resultados obtenidos.

La duración de los handovers es altamente variable especialmente en escenarios donde la potencia de señal recibida es muy baja, causando numerosos cambios de celda, como se muestra en la Fig. 5. Cuando varios cambios de celda tienen lugar consecutivamente, como se muestra en la Fig. 5, la longitud del primer cambio es mayor, mientras que el resto tiene una duración menor, como se aprecia en los valores presentados en la Tabla III, y como se apreció anteriormente también para GPRS.

Como resultado de las pruebas realizadas se puede concluir nuevamente que el comportamiento entorno a los handovers es bastante inesperado. Existe una considerable diferencia entre el rendimiento de las implementaciones reales de los mecanismos de handover y las nuevas propuestas estandarizadas en UMTS que buscan aliviar el impacto de los mecanismos de handover sobre las conexiones de datos.

III-C. Handovers en redes HSDPA

La técnica de soft handover no es soportada en HSDPA, sin embargo, se han especificado nuevos mecanismos para mejorar el rendimiento de los hard handover. Estos nuevos procedimientos son denominados como ”HS Serving Cell changes”. Su implementación es opcional y los cambios de celda pueden ser ejecutados realizando una transición previa a UMTS. Por tanto, en teoría, los procedimientos de handover para HSDPA pueden proporcionar cambios de celda sin pérdidas de paquetes, pero el rendimiento final depende de cómo esté configurada la red.

La Tabla IV proporciona los resultados de un conjunto de pruebas llevadas a cabo, nuevamente, en un entorno vehicular. La Fig. 6 muestra las interrupciones producidas en el tráfico de datos debido a los handovers, así como los pérdidas de paquetes asociadas con dichas interrupciones.

Cabe destacar también que durante las pruebas se observó que los mecanismos de handover implementados para HSDPA en las redes reales consisten en la transición a un canal dedicado UMTS (el cambio del color de fondo de la figura ilustra este fenómeno), en el cual se ejecuta el handover. Este comportamiento es el mostrado en la Fig. 6.

Sin embargo esta implementación es altamente ineficiente [13] en términos de los recursos de red consumidos, pudiéndose incluso producir un degradación significativa de la capacidad del sector si las transiciones a canales dedicados para la ejecución del handover son frecuentes. Durante las pruebas realizadas la duración media de las interrupciones se situaron entorno a los 10 segundos. Por tanto podemos concluir que el rendimiento de los handovers en HSDPA

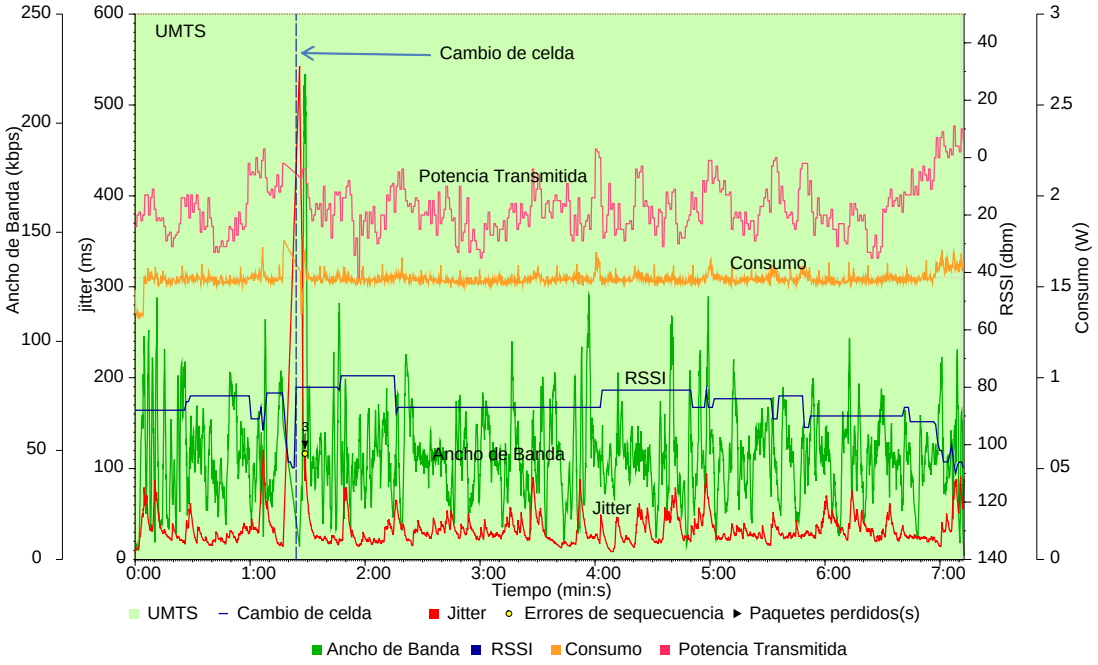


Figura 3. Comportamiento esperado durante un cambio celda en el transcurso de una conexión de datos en UMTS

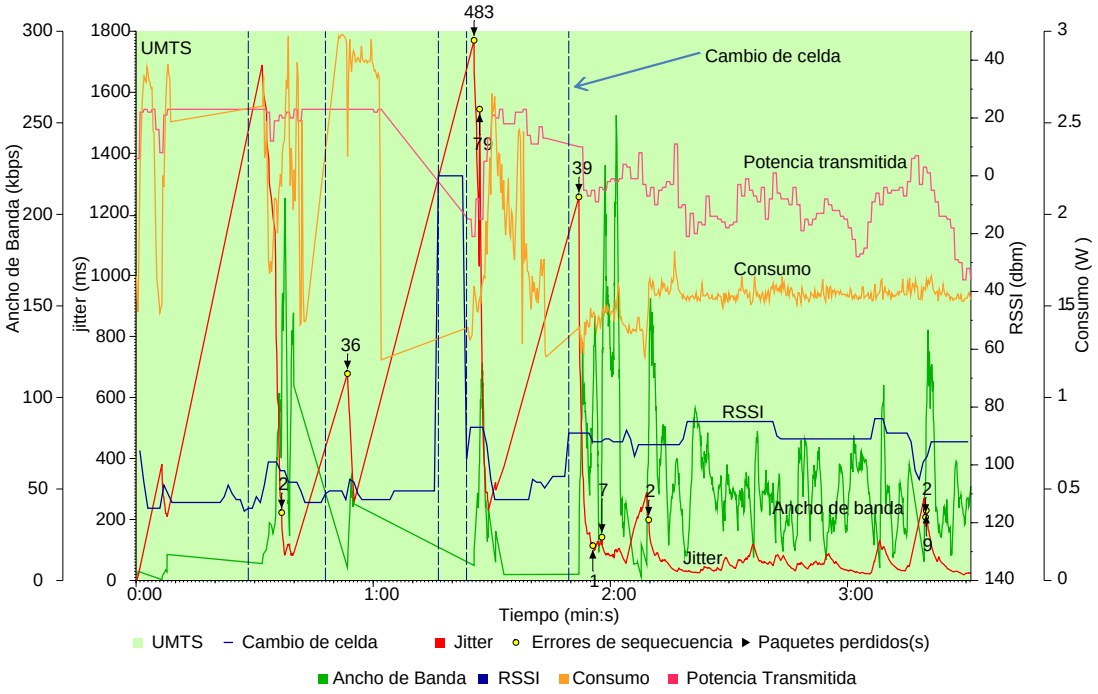


Figura 4. Cambios de celda durante una conexión de datos UMTS

debe ser mejorado con la implementación comercial de los mecanismos de cambios de celda estandarizados para HSDPA.

III-D. Handover entre sistemas

Para los handovers entre sistemas se obtiene un valor medio del tiempo de interrupción de 29 segundos y ráfagas de pérdidas de 200 paquetes. En la Fig. 7 se representa un handover entre sistemas. La Tabla V muestra los tiempos de interrupción asociados a los handovers representados en la figura anterior.

Instante de inicio del cambio de celda	Tiempo transcurrido desde cambio de celda	Tiempo transcurrido desde último paquete IP
9:01:35.656	00:00:29.087	00:00:53.210
9:01:51.907	00:00:13.232	00:00:00.396
9:02:42.35	00:00:03.150	00:00:06.363
9:03:01.505	00:00:54.616	00:00:56.933
9:03:39.632	00:00:16.539	00:00:00.050

Cuadro V
TIEMPO DE DURACIÓN DE LA INTERRUPCIONES PROVOCADA POR LOS HANDOVERS ENTRE SISTEMAS MOSTRADOS EN LA FIG. 7

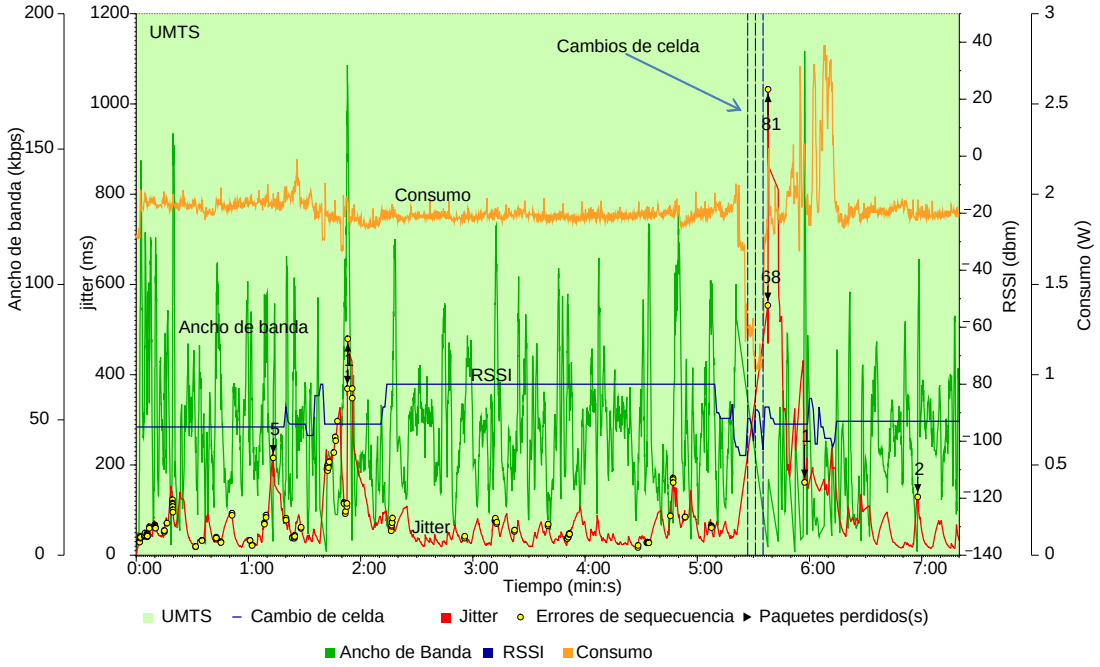


Figura 5. Cambios de celda consecutivos durante una sesión de datos UMTS

Interrupción tráfico IP (s)	19.04	34.85	7.982	9.371	10.44	13.97	10.45	8.285	17.84	9.343	11.72	17.72	15.74	17.82
Paquetes perdidos	200	230	59	55	129	77	78	99	54	128	119	59	3	8

Cuadro IV
HANDOVERS EN HSDPA

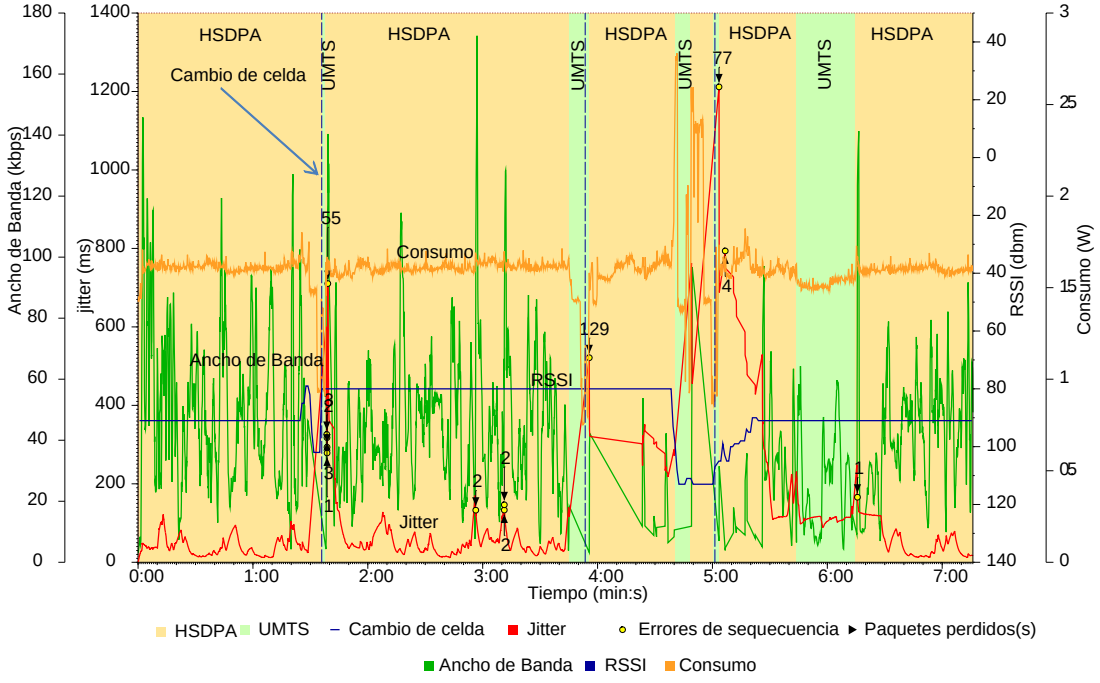


Figura 6. Cambios de celda durante una conexión de datos en un entorno vehicular (HSDPA)

Los handovers entre sistemas con claves en los escenarios vehiculares debido a las pérdidas de cobertura UMTS y los consiguiente cambios obligados a GPRS. Sin embargo como se ha visto en los resultados proporcionados, éstos tienen un gran impacto sobre las conexiones de datos. Para mejorar la calidad de servicio percibida por los usuarios en los escenarios vehiculares es esencial mejorar los mecanismos de handover entre sistemas.

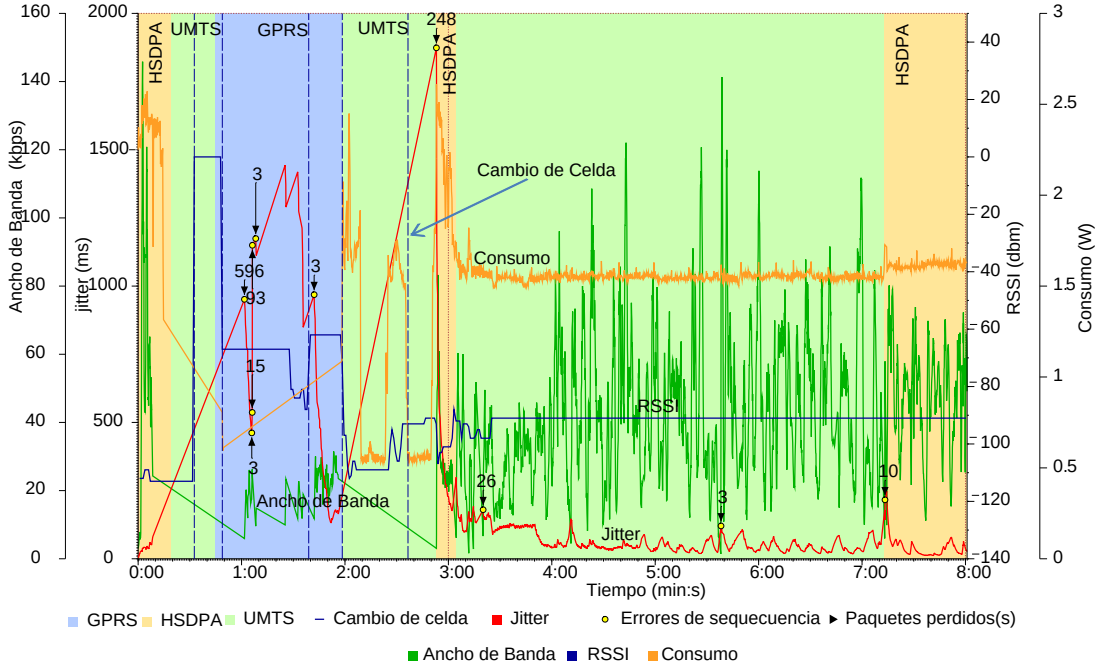


Figura 7. Handover entre sistemas: UMTS-GPRS

IV. Conclusiones

Los resultados de la aplicación de la metodología de medidas aplicada en este trabajo pueden ser utilizados para caracterizar el rendimiento de las distintas técnicas de handover en diferentes escenarios. Se han introducido los resultados más relevantes obtenidos después de aplicar la metodología en más de 100 sesiones de datos llevadas a cabo en un entorno vehicular. Los resultados presentados muestran un alta variabilidad en el rendimiento del handover, obteniendo en numerosas ocasiones un bajo rendimiento de los mecanismos de handover implementados en la redes de telefonía móvil comerciales. Es más, los resultados obtenidos para redes UMTS/HSDPA no son siempre mejores que los resultados obtenidos para redes GPRS debido a que las nuevas especificaciones técnicas desarrolladas por el 3GPP para mejorar los procedimientos de handover en redes UMTS y HSPDA son están disponibles en la redes comerciales.

Referencias

[1] A. Diaz, P. Merino, and F. Rivas, “Mobile application profiling for connected mobile devices,” *Pervasive Computing, IEEE*, vol. 9, no. 1, 2010.

[2] A. Diaz, P. Merino, ”A Testbed for Energy Profile Characterization of IP Services in Smartphones over Live Networks”, *Mobile Networks and Applications*, Springer, 2010 (to be published).

[3] I. Forkel, M. Schinnenburg, and B. Wouters, ”Performance evaluation of soft handover in a realistic UMTS network”, *57th IEEE Vehicular Technology Conference*, 2003.

[4] B. Singh, “Outage Probability Analysis in Soft Handover for 3G Wireless Networks”, *6th IEE International Conference on 3G and Beyond*, 2005.

[5] L. Bhebhe and A. Arjona, “Data outage across 3G and 2G wireless networks”, *International Symposium on a World of Wireless, Mobile and Multimedia Networks, WOWMOM 2008*.

[6] M. Lundan and I. D. D. Curcio, “Mobile streaming services in WCDMA networks,” , *10th IEEE Symposium on Computers and Communications*, 2005.

[7] Z. Becvar, P. Mach, and R. Bestak, “Impact of handover on voip speech quality in WiMAX networks”, *International Conference on Networking*, 2009.

[8] A. Cabellos-Aparicio, J. Núñez-Martínez, H. Julian-Bertomeu, L. Jakab, R. Serral-Gracià, and J. Domingo-Pascual, “Evaluation of the fast handover implementation for mobile IPv6 in a real testbed”, *IPOM*, ser. Lecture Notes in Computer Science, Springer, 2005.

[9] C. Gomez, M. Catalan, X. Figueras, J. Paradells, and A. Calveras, Impact of handover between umts and gprs on TCP/IP: An empirical approach. *64th IEEE Vehicular Technology Conference*, 2006.

[10] T. Halonen, J. Melero, and J. Garcia, GSM, GPRS and EDGE Performance: Evolution Toward 3G/UMTS, Wiley, 2002.

[11] “Technical Specification Group Radio Access Network; User Equipment (UE) conformance specification; Radio transmission and reception (FDD); Part 1: Conformance specification,” 3GPP, Techical Specification 34.121-1.

[12] D. Gou, B. Wei, and S. Wu, “An Optimized Transmission Scheme for UMTS Streaming Services”, *International Conference on Communications, Circuits and Systems ICCCAS*, 2004.

[13] P. Tapia, J. Liu, Y. Karimli, and M. Feuerstein, HSPA Performance and Evolution: A Practical Perspective, John Wiley, 2009.

Autenticación basada en IKEv2 y EAP para Escenarios de Redes Vehiculares

Pedro J. Fernández Ruiz {pedroj@um.es},
Cristian A. Nieto Guerra {cristian.nieto@um.es},
Antonio F. Gómez Skarmeta {skarmeta@um.es}

Departamento de Ingeniería de la Información y las Comunicaciones
Campus de Espinardo, Facultad de Informática, C.P. 30100, Murcia, SPAIN

***Resumen*—Este artículo pretende describir un escenario real de comunicaciones inalámbricas sobre una infraestructura WiMAX[1] [1], desplegada concretamente en el Campus de Espinardo de la Universidad de Murcia. Se aportan servicios tan necesarios en escenarios móviles como son la seguridad de las comunicaciones y la movilidad de los clientes. Estos servicios son provistos mediante los protocolos IKEv2[2] para la seguridad, y MIPv6[3] para la movilidad. El protocolo IKEv2 además nos permitirá el uso y estudio de diferentes métodos de autenticación basados en EAP[4], con lo que dispondremos con este escenario de un estupendo banco de pruebas real de donde extraer conclusiones sobre dichos métodos. Todo ello estará orientado a las redes vehiculares[5], donde la movilidad es uno de los aspectos fundamentales a tener en cuenta.**

***Palabras Clave*—WiMAX, IKEv2, IPsec, EAP, MIPv6, Autenticación, Mobilidad, Seguridad, OpenIKEv2, Redes Vehiculares.**

I. Introducción

El mundo de las telecomunicaciones está experimentando progresos notables en cuanto a movilidad, autonomía de los dispositivos, alcance y ancho de banda de las comunicaciones inalámbricas, entre otras mejoras. Además, el abaratamiento de los dispositivos móviles ha originado el acceso a dichas tecnologías por parte de millones de nuevos usuarios en todo el mundo. Esto ha supuesto que las tecnologías de comunicaciones inalámbricas tomen especial relevancia en estos momentos. Las tecnologías más destacadas son las comúnmente llamadas *Wi-Fi*[6] y *Bluetooth*[7], pensadas para interiores de edificios y vehículos, y las tecnologías *GPRS*[8] y *UMTS*[9], más orientadas a ofrecer conectividad en grandes áreas de cobertura.

Para las tecnologías Wi-Fi y Bluetooth no es necesario tener permisos especiales a la hora de desplegar su cobertura ya que dicha cobertura es reducida y se utilizan sólo frecuencias dentro de las bandas libres de licencias. Sin embargo, tecnologías donde la cobertura es mayor y se puede dar servicio a un mayor número de usuarios, como GPRS y UMTS, necesitan cumplir con unas licencias de explotación que las operadoras deben adquirir para poder desplegar dichas tecnologías.

La aparición del estándar IEEE 802.16, más conocido como *WiMAX*[1], ha supuesto una alternativa intermedia entre los dos grupos de tecnologías antes mencionadas como podemos ver en la figura 1. Inicialmente concebida para escenarios punto a punto para dotar de conectividad a poblaciones aisladas, a partir de la versión IEEE 802.16e publicada en 2006 se orientó a escenarios con infraestructuras inalámbricas que necesitaran cubrir un amplio rango de cobertura, y donde la movilidad de los clientes tomara suma importancia.

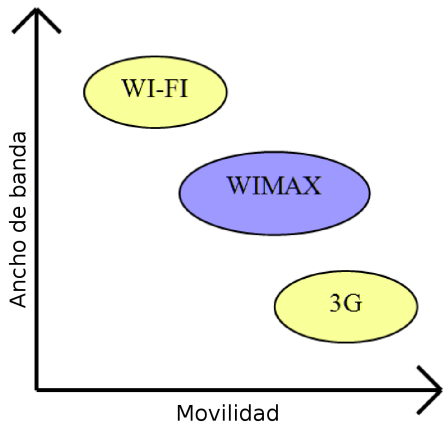


Fig. 1. Comparación entre tecnologías inalámbricas.

Este tipo de tecnología, conjuntamente con las tecnologías GPRS y UMTS, son perfectas para dar soporte a las denominadas *redes vehiculares*, principalmente debido a las largas distancias que pueden recorrer dichos vehículos en un corto periodo de tiempo. Sin embargo la tecnología WiMAX es la única que ofrece alternativas que permitan su uso sin la necesidad de adquirir licencias, siempre y cuando se utilicen frecuencias dentro de las bandas libres de licencias (de 4.9 a 5.8 GHz). A pesar de que dichas frecuencias son sensiblemente más direccionales que las comprendidas en algunas de las bandas licenciadas (de 2.3 a 3.6 GHz) y, por tanto, menor es la capacidad de salvar obstáculos, atravesar muros y accidentes geográficos, todavía pueden ser consideradas como frecuencias que nos permitan mantener comunicaciones *NLOS*[2], es decir,

[1]Worldwide Interoperability for Microwave Access

[2]Non-Line-Of-Sight

que no requieran que emisor y receptor tengan linea de visión directa. Por todo lo anterior, hemos propuesto y efectuado el despliegue de una infraestructura de red inalámbrica piloto basada en WiMAX en un entorno real, concretamente el Campus de Espinardo de la Universidad de Murcia.

En esta primera etapa de la implementación, se ha elegido desplegar la infraestructura de la red en base al protocolo WiMAX, a lo largo del anillo de circunvalación que rodea el Campus, dejando intencionadamente alguna zona donde no haya cobertura, y por supuesto zonas donde haya solapamientos de cobertura de diferentes estaciones base. Para asegurarnos de estas circunstancias es necesario efectuar un análisis de coberturas de la zona una vez desplegada la infraestructura.

Al tratarse de comunicaciones inalámbricas, uno de los aspectos más importantes a tener en cuenta es la seguridad. Este tipo de comunicaciones están expuestas a diferentes amenazas y posibles vulnerabilidades que permitan a un atacante desde impedir la comunicación mediante ataques de denegación de servicio (DoS), hasta interceptar y manipular la información transmitida. Se debe proveer de autenticidad y confidencialidad a las comunicaciones inalámbricas, y por eso hemos elegido IPsec[10] e IKEv2[2] como protocolos de seguridad. El uso de IKEv2 está justificado ya que es más seguro que su predecesor IKEv1[11] aportando además nuevas extensiones: asignación dinámica de direcciones IP y el transporte del protocolo de autenticación EAP[4], que nos permitirá utilizar y probar diferentes metodos de autenticación. Es importante mencionar aquí que la implementación elegida para IKEv2 es OpenIKEv2[14], implementación desarrollada también por la Universidad de Murcia.

En cuanto a la movilidad, aspecto fundamental en redes vehiculares[5], hemos utilizado la implementación de MIPv6[3] aportada por el proyecto *Nautilus 6*[15], soportado por el grupo de investigación WIDE[16].

II. Escenario de handover en redes vehiculares

La movilidad es uno de los principales tópicos de investigación en el estudio de las redes inalámbricas, debido a los beneficios que ofrece a los usuarios finales. Las redes vehiculares no están privadas de estas necesidades, debido a que en un corto periodo de tiempo un vehículo puede llegar a recorrer una gran distancia. Por esta razón es necesaria una infraestructura inalámbrica que permita la movilidad a lo largo del camino sin perder la conectividad.

Para proveer un escenario de movilidad para redes vehiculares, es necesario implementar una infraestructura que pueda garantizar un determinado nivel de calidad de servicio, en base al tipo de datos transmitido y el servicio contratado.

Otro requisito es la seguridad. Confidencialidad y autenticidad son una necesidad en este tipo de escenarios ya que las redes inalámbricas están expuestas a diferentes amenazas y vulnerabilidades que permite a cualquier usuario acceder y la posibilidad de manipular la información transmitida.

Para lograr el escenario mencionado anteriormente, se propone un escenario de prueba en el que un vehículo conectado a una red inalámbrica pueda moverse libremente, usando los diferentes puntos de acceso que se encuentren a lo largo del camino. Estos puntos de accesos podrían pertenecer a diferentes dominios y diferentes tecnologías inalámbricas, tales como Wi-Fi, WiMAX y UMTS. Como resultado de esto, diferentes tipos de handover pueden acontecer:

- Handover intra-dominio intra-tecnología: Se cambia de estación base sin cambiar de tecnología ni de dominio. Es el caso más sencillo de handover.
- Handover intra-dominio inter-tecnología: Se cambia de estación base cambiando sólo la tecnología. Se complica por hacer interoperar diferentes tecnologías con distintos comportamientos.
- Handover inter-dominio intra-tecnología: Se cambia de estación base cambiando sólo el dominio. Este handover se complica en el plano de la seguridad y la autenticación del usuario.
- Handover inter-dominio inter-tecnología: Se cambia de estación base y tecnología, siendo este el más complejo de los handovers.

Como hemos comentado, cada tipo posee un diferente nivel de complejidad. Nuestro enfoque será ir aumentando dicho nivel en el escenario de prueba paulatinamente, teniendo como objetivo el mejorar el rendimiento de procesos como por ejemplo, métodos de autenticación, tiempos de handover, etc.

III. Construyendo el escenario

El desafío que nos planteamos es el de crear una infraestructura de red inalámbrica basada conjuntamente en WiMAX y Wi-Fi para ofrecer un servicio de acceso a Internet provisto de control de acceso, método de autenticación extensible y confidencialidad de los datos, todo ello gracias a los protocolos IPsec[10], IKEv2[2] y EAP[4]. Además tendremos que proveer movilidad mediante el protocolo MIPv6[3] sin que interfiera con los servicios de seguridad anteriores.

A. Infraestructura inalámbrica

El primer paso que tenemos que dar es desplegar nuestra infraestructura WiMAX y Wi-Fi en un entorno real (Campus de Espinardo, Murcia) y realizar un análisis de cobertura para asegurar que se cumplen nuestros requisitos de cobertura y así poder efectuar nuestras pruebas. Las redes vehiculares tienen unos requisitos especiales que pueden cambiar dependiendo de la velocidad de los vehículos y del entorno que los rodea. Las tecnologías WiMAX y Wi-Fi son muy similares, pero cada una de ellas está pensada para diferentes escenarios:

- WiMAX es capaz de ofrecer un acceso NLOS de alta velocidad con una amplia cobertura. El estándar 802.16d para conexiones fijas puede alcanzar velocidades de 75 Mbps en un rango de 10 Kms. Sin embargo, el estándar 802.16e para conexiones móviles sólo se alcanzan unos 30 Mbps en un rango de 4 Kms. Las antenas suelen ser direccionales con un determinado ángulo de cobertura. Es el caso de nuestras estaciones base. Sin embargo, es recomendable que las antenas de los clientes sean omnidireccionales, pues al ir montadas en vehículos cambian

Fig. 2. Localización de las estaciones base en el Campus de Espinardo.

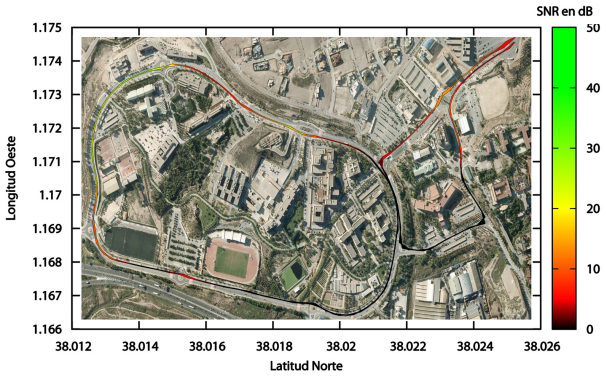


Fig. 3. Mapa de cobertura de algunas de las estaciones base WiMAX instaladas.

su dirección constantemente. No dispone de mecanismos de autenticación a nivel de enlace que soporten transporte EAP.

- Wi-Fi también ofrece acceso NLOS de alta velocidad, pero en un rango de cobertura más reducido, entorno a los 100 metros. Sin embargo sí existen mecanismos de autenticación a nivel de enlace que soporten el transporte de EAP, como es el caso de 802.1x.

La decisión que tenemos que tomar es dónde usar una y otra tecnología, teniendo en cuenta los requisitos de movilidad mencionados. Por un lado, como resultado de un estudio preliminar hemos decidido colocar las estaciones base WiMAX en las azoteas de aquellos edificios que por su posición en el Campus facilita la distribución de la cobertura. Se pueden observar dichas situaciones en la figura 2. Por otro lado, las antenas Wi-Fi ya han sido desplegadas en los interiores y cercanías de los edificios del Campus, formando parte de una infraestructura de acceso a Internet que ya se encuentra en funcionamiento.

En esta primera etapa de la implementación, no va a ser considerada la tecnología Wi-Fi en los resultados. Esto se debe a que es necesario resolver situaciones que pueden presentarse en el momento de realizar el handover entre tecnologías. Sin embargo se considera interesante el comentar el escenario completo de la implementación que es considerada como objetivo final.

Para estar seguros de que la cobertura WiMAX se ajusta a nuestras necesidades, tenemos que realizar un análisis de cobertura a lo largo del anillo perimetral del Campus, usando para ello un medidor de fuerza de señal incorporado el cada cliente WiMAX.

Tenemos colocadas 5 estaciones base sobre varias de las facultades del Campus, como hemos visto en la figura 2. También hemos adquirido 4 clientes para podernos conectar a las estaciones base y realizar pruebas. A pesar de que la frecuencia a la que trabajan estas antenas (4,9 GHz) es considerado como NLOS, es decir, que no tiene por qué existir linea de visión entre emisor y receptor para establecer la comunicación, hay obstáculos que no pueden ser salvados, como por ejemplo, los edificios y las colinas. Usaremos uno de los clientes montado en un coche para determinar el grado de cobertura a lo largo del anillo perimetral.

Todos los dispositivos WiMAX se pueden administrar remotamente a través de TELNET o SNMP. Mediante este tipo de acceso podemos consultar el nivel de potencia de la señal que se está recibiendo en cada momento, que facilita más aún su medida.

Para realizar el muestreo, hemos desarrollado un sistema automático de muestreo del nivel de señal, de la posición geográfica y de la marca de tiempo del momento de cada muestra. Esta información la almacenamos para posteriormente elaborar mapas de cobertura como el de la figura 3, que nos ayudarán a comprobar visualmente si las antenas se están usando eficientemente. Esto requiere el uso de un dispositivo GPS y un portátil conectado a un cliente WiMAX para determinar el nivel de señal recibido. Una configuración razonable para dicho muestreo sería tomar una muestra cada 20 metros, con una velocidad límite de 30 Km/h, ya que es el límite de velocidad en el Campus, lo que resulta en un periodo de 2.4 segundos.

El muestreo debe realizarse individualmente para cada estación base, deshabilitando el resto para evitar lecturas erróneas. De esta manera obtendremos un mapa de cobertura para cada estación base y así delimitar las zonas de cobertura, de solapamiento y de sombra, para posteriormente tomar las decisiones necesarias si no se ajusta a nuestras expectativas. En nuestro caso sería deseable disponer de todos los casos de handovers, y por tanto necesitamos zonas donde hayan cero, una o dos estaciones base presentes. En el caso de las zonas de solapamiento se pueden estudiar escenarios de preautenticación.

B. Hardware utilizado

El esenario esta compuesto por hardware que cumplen diferentes funciones, entre los más importantes se puede señalar las antenas Wimax y ordenadores. Tanto las estaciones bases (BS) como los clientes WiMax, son marca Alvarion. En la siguiente tabla se muestra las descripciones más importantes del hardware utilizado.

C. Seguridad en las comunicaciones

Existen varias alternativas para dotar de seguridad a las comunicaciones y establecer a su vez un mecanismo de control

Cantidad	Función	Descripción
5	BS WiMax	Marca Alvarion, direccionales, 3 de 120 y 2 de 90 grados de cobertura, tecnología pre-WiMax
1	Intenet Gateway	Procesaro Pentium 4 CPU 2.66GHz, cache 512 KB, RAM 2GB
1	SG1	Pentium 4 CPU 4GHz, RAM 1GB, Ubuntu 9.10
1	HA1	VIA 564MHz, RAM 512MB, Ubuntu 8.04
1	SG2	Pentium 4 CPU 2.66GHz, RAM 2GB, Ubuntu 9.10
1	HA2	VIA 1GHz, RAM 512MB, Ubuntu 8.04
1	AAA	VIA 564MHz, RAM 512MB, Ubuntu 8.04
1	MN	Pentium M 1.86GHz, RAM 1GB, Ubuntu 8.04

Tabla I
DESCRIPCIÓN DEL HARDWARE UTILIZADO

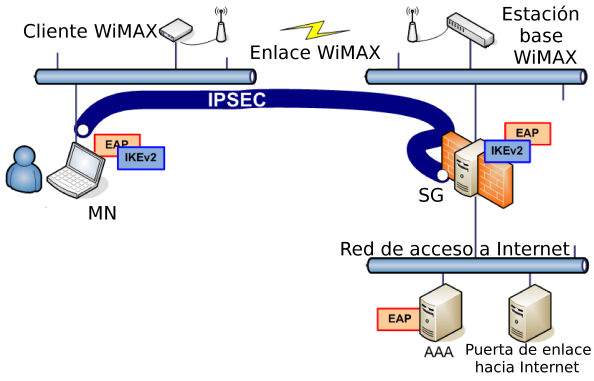


Fig. 4. Escenario "Road warrior" sobre una infraestructura WiMAX.

de acceso para el uso de Internet. Las siguientes son las dos alternativas más razonables:

- Usar encriptación simétrica a nivel de enlace basada en claves pre-compartidas. Esta alternativa no dispone de mecanismos de autenticación y control de acceso.
- Usar encriptación simétrica a nivel de red mediante IPsec, IKEv2 para el establecimiento del material criptográfico, establecimiento dinámico de IP y un mecanismo de autenticación basado en EAP que a la vez nos sirva de control de acceso.

Está claro que la segunda opción es la que más beneficios nos aporta, sobre todo el hecho de soportar mecanismos de autenticación basados en EAP, que nos permitirán investigar diferentes métodos de autenticación y comprobar sus comportamientos en escenarios donde la movilidad esté presente.

Necesitamos un elemento que permita establecer la seguridad y que no permita el acceso a equipos no autenticados. Se trata de un router que nos conecte con Internet y que disponga de un servicio IKEv2 instalado y configurado con una serie de políticas IPsec, al que llamaremos *puerta de enlace se seguridad* (Security Gateway, en adelante SG), como podemos ver en la figura 4. Por tanto dispondrá de dos interfaces de red, una hacia la red de acceso a Internet, y la otra a una red local aislada donde sólo estarán presentes las estaciones base WiMAX. Por otro lado, cada cliente WiMAX estará conectado a otra red local, en la que podrá haber una serie de equipos conectados. El enlace inalámbrico que se establece entre estación base y cliente WiMAX es a nivel de enlace, con lo que es transparente para los niveles superiores. Por tanto, las redes conectadas al cliente WiMAx y a la estación base se encontrarán unidas como si realmente fueran una sola.

En infraestructuras basadas en redes IPv6, se dispone de direcciones *link-local* generadas automáticamente para tener conectividad con los equipos dentro de una misma red. El SG no envía por el momento ningún tipo de anuncio de presencia de router. El equipo del usuario (Mobile Node, en adelante MN) se conecta a esta red extendida, obteniendo acceso directamente al SG. En esta implementación son utilizadas antenas direccionales de 90 y 120 grados de rango de cobertura, para extender dichas direcciones *link-local*. A pesar de ello el MN no conoce todavía la dirección IP *link-local* del SG, con lo que tendrá que realizar un ping a la dirección ff02::2 que representa a todos los routers presentes a nivel de enlace. Una vez le haya respondido, ya sabremos con quién iniciar el establecimiento del túnel IPsec que nos permitirá conectarnos a Internet. Esto hace necesario que en el MN también esté disponible el cliente IKEv2 configurado y listo para ser ejecutado en el momento que queramos conectividad a Internet. Este escenario es muy similar al típico y conocido escenario IPsec llamado *Road Warrior*, como hemos podido ver representado gráficamente en la figura 4.

Una vez decididos a conectarnos a Internet, lanzamos el cliente IKEv2 en el MN, lo que provocará que, por medio de una característica especial de OpenIKEv2[14] que permite autogenerar asociaciones de seguridad de una determinada política IPsec, comience la negociación IKEv2 para establecer un túnel de seguridad entre el MN y el SG a pesar de no haber todavía tráfico coincidente con dicha política. En esta negociación se generará el material criptográfico que protegerá los datos transmitidos por el túnel IPsec y la dirección IPv6 global que el MN podrá usar para conectarse a Internet.

Tanto en el MN como en el SG, OpenIKEv2 ha establecido las políticas necesarias para:

- permitir todo el trafico cuyas direcciones origen y destino sean *link-local*. Ya sabemos de antemano que no pueden ir más allá del SG.
- permitir el tráfico IKEv2 e ICMPv6, para permitir también con ello las negociaciones IKEv2 y mensajes ICMP, como el ping.
- proteger el tráfico con origen o destino aquellos MN que se hayan autenticado con éxito y hayan establecido un túnel IPsec.
- impedir que circule cualquier otro tráfico distinto al anterior.

Para el proceso de autenticación que acontece durante la negociación IKEv2 se ha utilizado como punto de partida el método de autenticación EAP-TLS[13]. Para ello necesitamos de una entidad más llamada *AAA*, que es simplemente un servidor *Radius*[18] (implementado con *Free Radius*[19]) que autenticará al usuario, en este caso mediante certificados, y

decidirá si le deja o no acceso a Internet. Se puede encontrar también dicho elemento en la figura 4.

D. Procedimiento de bootstrapping y handover

Los procedimientos de bootstrapping y handover se basan en conseguir aportar simultáneamente dos servicios: Seguridad y movilidad. Ambos servicios son ofrecidos por separado a través de sus respectivas implementaciones: openikev2 y mip6d. La forma de funcionar de cada servicio los hace incompatibles entre sí. Por tanto, se han realizado algunos cambios en el comportamiento normal de las entidades que conforman la red para poder ofrecer los dos servicios al mismo tiempo, sobre todo siguiendo la premisa de que dichas modificaciones sean transparentes al servicio de movilidad y centralizanlas en la implementación OpenIKEv2 del protocolo IKEv2, de la cual somos autores y mantenedores.

Supongamos primero que un nodo móvil acaba de encenderse y no está conectado a ninguna red. Como podemos ver en la figura 8 disponemos en nuestro escenario de movilidad una red home y dos redes visitadas para dicho nodo móvil, cada una de las redes visitadas pertenecientes a un dominio diferente y a su vez equipado cada uno con su puerta de enlace de seguridad (en adelante SG) correspondiente, que no son más que encaminadores con una serie de políticas de seguridad establecidas y un servicio IKEv2 para el establecimiento de túneles de seguridad con los nódos móviles. Los SG's permiten circular sólo al tráfico protegido por los túneles.

Además hemos realizado cambios en el comportamiento de estas puertas de enlace, como el deshabilitar el envío contínuo característico en redes IPv6 de "Router Advertisements" (RA's), mensajes broadcast que permiten que los nodos móviles adviertan la presencia de las puertas de enlace y así determinar en qué red se encuentran en cada momento. La responsabilidad del envío de este tipo de mensajes se ha incorporado en el demonio que ofrece el servicio de IKEv2, es decir, en nuestra implementación OpenIKEv2. De esta forma podemos controlar cuándo y a quién mandar dichos RA's, ya que pueden ser mandados en modo unicast justo después de haber establecido el túnel de seguridad con un nodo móvil. El servicio de movilidad se basa precisamente en la presencia de este tipo de mensajes para detectar un cambio de red que provocan el lanzamiento de los mecanismos de movilidad necesarios.

Como el envío periódico de RA's ha sido deshabilitado, corresponde a los nodos móviles preguntar por la presencia de SG's. Esto puede realizarse gracias a la herramienta "ping" y al grupo multicast IPv6 que representa a todas las puertas de enlace presentes en la red ff02::2. El nodo móvil realizará periódicamente un ping a dicha dirección para ver si hay algún SG disponible. Una ver que el SG ha sido detectado por el nodo móvil, una negociación IKEv2 comienza entre ellos para establecer el túnel de seguridad entre ellos para proteger el tráfico. Para ello usarán sus direcciones "link-local" siempre disponibles. En el establecimiento del túnel, además de producirse una negociación de autenticación basada en EAP, se le asigna al nodo móvil una dirección IPv6, que en

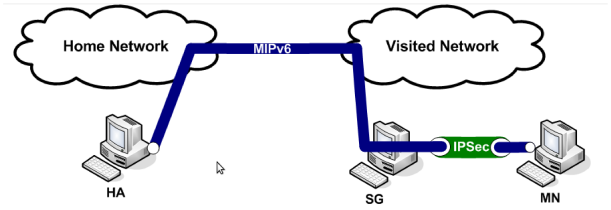


Fig. 5. Relación entre los túneles. Movilidad dentro de seguridad.

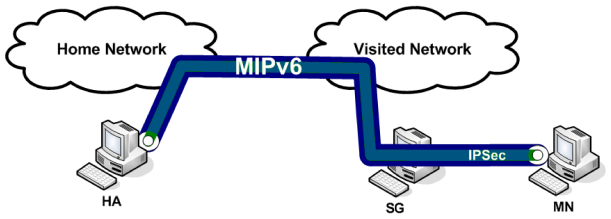


Fig. 6. Relación entre los túneles. Seguridad dentro de movilidad.

terminos de movilidad es llamada "care of address" (CoA), con la que poder conectarse y tener acceso a la red y sus servicios. Una vez establecido el túnel, el SG envía un RA unicast dirigido sólo al nodo móvil extremo del túnel. La recepción de este mensaje provoca que el mecanismo de autoconfiguración de IPv6 del nodo móvil configure la dirección IPv6 asignada y establezca la dirección de la puerta de enlace y las rutas necesarias. Al mismo tiempo, el servicio de movilidad situado en el nodo móvil detecta el RA y lanza el proceso de movilidad para cambiar de red, ya que es el primero de dicha red que recibe. Este servicio de movilidad notificará al "Home Agent" (HA) cual es su nueva CoA a través del mensaje "Binding Update" (BU). El HA responderá con un "Binding ACK" (BA), dando por terminado el proceso de movilidad.

Mediante este proceso de conexión a una red hemos establecido un mecanismo de control de acceso transparente para el servicio de movilidad, el cual no es consciente que todo el tráfico que circula entre el nodo móvil y el SG está siendo protegido por un túnel IPsec. Puede decirse en este caso que el túnel de movilidad va por dentro del túnel de seguridad, como se puede apreciar en la figura 5.

Por otra parte, es importante hacer notar aquí la diferencia entre este mecanismo y el mecanismo ya disponible en la implementación usada de MIPv6 para proteger el tráfico entre el nodo móvil y el HA. Este otro tipo de mecanismo establece un tunel de seguridad entre el nodo móvil y el HA usando la dirección "home address" (HoA). Esto hace que el tunel sólo tiene que ser creado una vez y no cambiará nunca a pesar de que el nodo móvil cambie de red y por tanto de CoA. Sin embargo este último mecanismo no tiene la posibilidad de establecer un mecanismo de control de acceso entre el nodo móvil y la red visitada, y por tanto permitir a los administradores de la red visitada decidir qué nodos móviles tendrán acceso a la misma y cuáles no. Puede decirse en este otro caso que el tunel de seguridad va por dentro del núnel de movilidad, como se puede apreciar en la figura 6.

El anidamiento de ambos túneles puede ser realizado gracias a los dos grupos de políticas existentes en implementaciones como las incorporadas en los núcleos habituales de Linux, que son las que estamos utilizando. Estos dos grupos de políticas se llaman *SUB* y *MAIN*. En contreto, en el grupo *SUB* residen las políticas de movilidad, y en el grupo *MAIN* las de seguridad IPsec. Estos grupos de políticas tienen la peculiaridad de que son grupos independientes entre sí, y por tanto un tipo de tráfico puede coincidir con los selectores de las políticas tanto de un grupo como del otro. Por tanto, la finalidad de esta separación es que se pueda aplicar para cada paquete de tráfico una política de MAIN y otra de SUB. Así se podrá aplicar hasta dos políticas a un tipo de tráfico, y por tanto poder aportar seguridad y movilidad al mismo tiempo.

Por otro lado, el procedimiento de handover es iniciado cuando el nodo móvil detecta que un SG diferente está disponible. En este caso, el nodo móvil establece una negociación IKEv2 completa contra el nuevo SG, estableciendo un nuevo túnel de seguridad, y por tanto una nueva CoA. El nuevo SG envía un RA al nodo móvil para desencadenar el proceso de movilidad que notificará al HA del cambio, a la vez que provocará la autoconfiguración del nuevo número IP y la puerta de enlace. Este proceso de handover puede ser mejorado usando un esquema de pre-autenticación donde las negociaciones IKEv2 puedan ser efectuadas con adelanto utilizando la conectividad disponible antes de efectuar el salto. También puede mejorarse el tiempo de handover estableciendo nuevos y mejores métodos de autenticación EAP que generen menor número de intercambios. El método EAP utilizado como referencia es el denominado EAP-TLS.

E. Movilidad de las comunicaciones

Imaginemos un vehículo en movimiento, conectado a la red de un proveedor de servicios. El vehículo tiene asignada una dirección IP para acceder a los servicios de la red, como puede ser el acceso a Internet. Durante el recorrido, el coche necesita cambiar de punto de acceso (AP) debido al limitado rango de cobertura que posee cada AP. Cuando se realiza el cambio, la infraestructura asigna una nueva dirección IP, siendo esta última diferente de la anterior, lo que da como resultado una perdida de conexión durante un periodo de tiempo. Las aplicaciones interrumpen las sesiones abiertas y será necesario crear nuevas sesiones desde cero, utilizando la nueva dirección IP asignada. Por tanto el handover no es transparente a la capa de aplicación en este caso, como se ilustra en la figura 7.

Para resolver este problema, es utilizado el Protocolo de Internet Móvil para IPv6 (MIPv6)[3], cuyo objetivo es crear un escenario en el cual, a nivel de aplicación, el cliente mantendrá siempre la misma IP, mientras que a nivel de red puede ir cambiando, en base a la IP asignada por los puntos de accesos a los cuales se vaya uniendo. En la terminología MIPv6, la dirección IP utilizada a nivel de aplicación es la *Home Address* (en HoA), y la IP que será cambiada y asignada al visitante de la red es la *Care of Address* (CoA). Este protocolo de movilidad necesita la presencia de un componente extra en

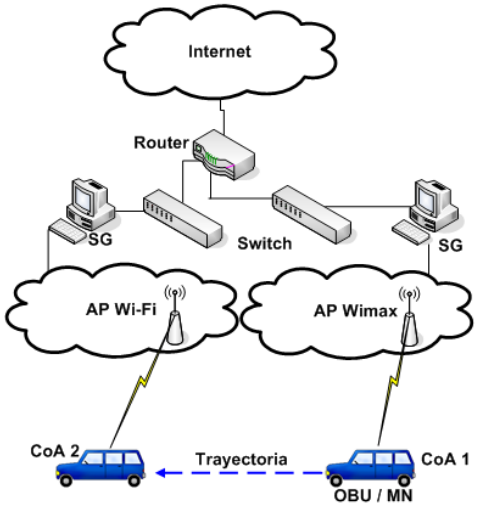


Fig. 7. Escenario de red vehicular sin soporte a la movilidad.

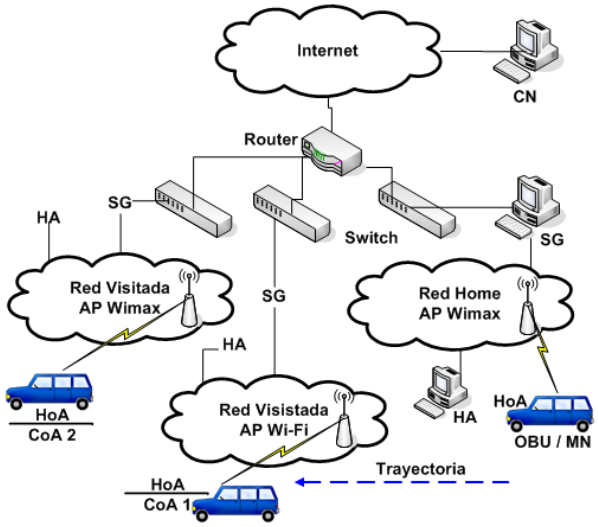


Fig. 8. Soporte de movilidad para una red vehicular.

la red *home*, llamado *Home Agent* (HA). Este escenario de movilidad se ilustra en la figura 8.

Hay que comentar que IKEv2 y MIPv6 no son suficientes para asegurar un handover transparente. Es necesario un mecanismo que realice la autenticación considerando el siguiente paso en el proceso de handover, con el objetivo de reducir los tiempos en el proceso global. La solución a esta situación es el Protocolo de Autenticación Extensible (EAP), ya que la fase de autenticación puede ser adelantada tomando en cuenta el nivel de fuerza de la señal. Cuando el nivel de la señal alcance un umbral mínimo, el método de pre-autenticación puede ser iniciado contra el nuevo punto de acceso, utilizando el enlace actual, realizando todo el proceso de autenticación antes de que se pierda la señal por completo.

Existen determinados métodos de autenticación que han sido diseñados para reducir el tiempo de autenticación al mínimo. Este es el caso del *Método de Re-autenticación*

Rápido EAP (EAP-FRM)[20], desarrollado también por investigadores de la Universidad de Murcia.

1) Disponibilidad del servicio: Hoy en día es bastante común encontrar dispositivos de comunicación que dispongan de varias interfaces con diferentes tecnologías. Este hecho permite al usuario final utilizar diferentes alternativas para conectarse a la red con un mismo dispositivo. Por tanto, esto permite a los proveedores de servicios de red ofrecer sus servicios a través de estas tecnologías.

Como resultado de tener más de una interfaz de red con diferentes tecnologías, la disponibilidad del servicio es mayor. Es también más eficiente ya que en cada situación la interfaz de red empleada será aquella que obtenga la mejor calidad de la señal o la que menor coste nos suponga económicamente.

Por ejemplo, durante el recorrido que realiza un vehículo podemos encontrar diferentes orografías, desde un campo abierto hasta un entorno urbano, cada una con sus características especificas. En un campo abierto nos encontramos con una orografía plana, así que es más fácil conseguir comunicaciones entre emisor y receptor con línea de visión directa (LOS). Esta situación permite implantar infraestructuras de redes utilizando pocos recursos para conseguir un gran área de cobertura. Sin embargo, en un área urbana encontramos una gran cantidad de edificaciones y otros tipos de obstáculos que no nos permiten una línea de visión directa entre emisor y receptor, con lo que es preciso utilizar comunicaciones que no la requieran(NLOS), lo que además implica el despliegue de dispositivos inalámbricos de corto alcance, que por otro lado implica el uso de más recursos.

Cada tecnología inalámbrica tiene características que pueden ser consideradas una ventaja o desventaja, pero eso dependerá del área donde sea desplegada la infraestructura. Por esta razón se justifica el uso de diferentes tecnologías, dependiendo de las características de la zona donde va a ser desplegada. Por ejemplo WiMAX[1] es la mejor selección para zonas abiertas y donde el vehículo puede recorrer distancias largas en un corto espacio de tiempo. Sin embargo, UMTS es la mejor opción si el vehículo se mueve a través de una zona con muchos obstáculos a su alrededor.

Finalmente, WiFi[6] puede ser considerado como la mejor opción dentro de entornos urbanos, donde encontramos muchas edificaciones y una gran densidad de usuarios. Seleccionando la tecnología propuesta en cada caso se ofrece un mejor empleo de la señal y como resultado se hará un uso más eficiente de la energía. Debido a esto, es importante encontrar una relación equilibrada entre la tecnología empleada y el entorno en el cual se encuentra localizado el usuario final.

Por ejemplo, imaginemos el caso de un vehículo que esta viajando a través de una autopista, y por tanto ha tenido que pagar un peaje por ello. Este peaje puede incluir el servicio de conexión a Internet que se ofrece a lo largo del trayecto. La tecnología WiMAX parece la más indicada para cubrir este trayecto. Sin embargo, en áreas de servicio, el acceso a Internet será ofrecido en mejores condiciones mediante la tecnología Wi-Fi, debido a su mayor ancho de banda.

El vehículo debe estar equipado con una *Unidad de Abordo* (OBU), la cual busca los servicios ofrecidos en el entorno y hace uso de aquel que tenga permiso y que tenga mejor calidad y prestaciones. Esta selección debe ser transparente para el usuario, quien está ocupado conduciendo el coche. Para permitir esta transparencia, un conjunto de reglas deben ser establecidas previamente en la OBU para establecer el comportamiento de esta selección dinámica de servicios.

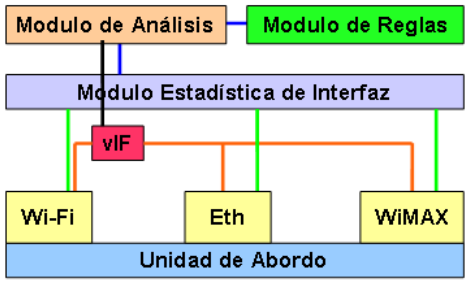


Fig. 9. Diagrama de la estructura de la OBU.

2) Unidad de Abordo: Cada vez es más común encontrarnos con que los vehículos vienen provistos con ordenador de abordo, con unas capacidades de procesamiento más que aceptables para implementar una amplia gama de servicios, además de poder disponer de múltiples interfaces de distintas tecnologías inalámbricas. Gracias a esto es posible nuestra implementación de la OBU.

La parte software, como se puede observar en la figura 9, esta dividida en:

- Interfaz Virtual (vIF): es a través de la cual la OBU se conecta a la red, empleando de modo transparente, una interfaz física disponible. Esta interfaz es creada en el momento de iniciar una nueva conexión sobre esta interfaz física.
- Módulo de Estadística de Interfaz (IM): Su principal tarea es la de reunir información de las diferentes interfaces físicas. Entre la información reunida está la disponibilidad de punto de acceso, fuerza de la señal, protocolo de seguridad, etc. Esta información será procesada para tomar decisiones en base a las reglas pre-establecidas.
- Módulo de Reglas (RM): contiene las reglas que serán consideradas cuando la OBU tenga que realizar alguna acción, por ejemplo, seleccionar el mejor punto de acceso.
- Módulo de Análisis (AM): emplea la información reunida por el IM, tomando en cuenta las reglas en RM para tomar decisiones y llevar a cabo las acciones necesarias para hacerlas efectivas.

Algunas de la reglas a ser consideradas son:

- El proveedor de servicios.
- Interfaz utilizada.
- Fuerza y calidad de la señal.
- Parámetros para el handover intra-tecnologías.
- Parámetros para el handover inter-tecnologías.

En este escenario la OBU puede ser considerado como un nodo móvil (MN), el cual inicia con una comunicación

establecida. De manera transparente al usuario, la OBU puede cambiar de punto de acceso (AP), basándose en la infraestructura disponible. Una de las características que debe satisfacer la AM es la capacidad de anticiparse a los cambios futuros de AP, para reducir el tiempo en que se pueda interrumpir la comunicación (escenario de pre-autenticación). Como se muestra en la figura 8, durante el viaje el vehículo realizará cambios de AP en varias ocasiones y se le asignará en cada ocasión una IP diferente.

El handover entre AP's tiene dos enfoques:

- Donde la tecnología de ambos AP's son iguales, siendo un handover intra-tecnología.
- Donde la tecnología de los AP's son diferentes, siendo un handover inter-tecnología.

En ambas situaciones descritas, es necesario que la aplicación pueda continuar transmitiendo sin problemas, por lo que es necesario diseñar un procedimiento que realice el handover entre los AP's sin que se interrumpa la comunicación que mantienen los protocolos de la capa de red y superiores. Para resolver esta situación se hace uso de la movilidad para IPv6, la cual permite a un MN mantener la misma dirección IP(HoA), a nivel de aplicación, mientras usa simultáneamente otra dirección IP(CoA), que puede ir cambiando sin problemas, proporcionándole la conectividad a Internet.

En el momento en que ocurra un handover, si es intra-tecnología, las modificaciones son realizadas en la actual vIF. Sin embargo, si el handover es inter-tecnología, una nueva vIF es creada ya que se emplea una nueva interfaz, siendo necesario establecer nuevas políticas de seguridad.

IV. Conclusiones y futuras líneas de trabajo

Las herramientas diseñadas para realizar el muestreo y análisis de cobertura nos ha facilitado encontrar una configuración óptima de las antenas para alcanzar el máximo rango de cobertura posible. Este desarrollo de una infraestructura basada en WiMAX[1] es ciertamente un primer paso necesario para abrir diversas líneas de investigación, actuando como un gran banco de pruebas en un entorno real para determinar el rendimiento tanto de la propia tecnología WiMAX como también de diversos protocolos en situaciones donde la movilidad y la seguridad son requisitos fundamentales. Este es el caso de los métodos de autenticación basados en EAP, que tienen aquí un entorno perfecto para medir su rendimiento en comparación con otros métodos ya suficientemente establecidos, como es el caso de EAP-TLS[13].

Gracias a la infraestructura de seguridad basada en IPsec[10] e IKEv2[2] que establece túneles de seguridad para proteger el tráfico, es la oportunidad perfecta para que OpenIKEv2[14], nuestra implementación de código abierto del protocolo IKEv2, continúe mejorando en funcionalidad y prestaciones al ser puesto a prueba en un escenario real. En el resarrollo del presente escenario se han mejorado y probado funcionalidades como la asignación dinámica de direcciones IP y el transporte de mensajes EAP[4], además de incorporar nuevas como la autogeneración de asociaciones de seguridad.

El despliegue de una infraestructura inalámbrica de este calibre debería realizarse tomando en consideración las circunstancias específicas y del entorno que nos rodea, usando en cada caso la tecnología inalámbrica más apropiada de la que dispongamos. Para el usuario este hecho debe ser transparente, y dejar la responsabilidad de elegir que tecnología usar en cada momento a un agente de su equipo que basándose en una serie de reglas preestablecidas, elegirá en todo momento la interfaz más apropiada en cada entorno o circunstancia.

Por último, decir que las redes vehiculares[5] son un excelente escenario para investigar el comportamiento de protocolos cuando la característica fundamental a potenciar es la movilidad.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el CICYT TIN2008-06441-C02-02 bajo el "Programa de ayuda a los grupos de excelencia de la fundación Séneca 04552/GERM/06".

Referencias

[1] IEEE 802.16, http://wirelessman.org/
[2] C.Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306, 2006.
[3] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6" IETF RFC 3775, 2004. http://www.ietf.org/rfc/rfc3775.txt
[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H Levkowetz, "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.
[5] Stephan Olariu, Michele C. Weigle, "Vehicular Networks from Theory to Practice", ISBN: 978-1-4200-8588-4 ,2009
[6] IEEE 802.11, http://standards.ieee.org/getieee802/802.11.html
[7] IEEE 802.15, http://www.ieee802.org/15/
[8] Descripción del protocolo GPRS http://www.protocols.com/pbook/gprs.htm
[9] Descripción del protocolo UMTS http://www.protocols.com/pbook/umts.htm
[10] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, 1998. http://www.ietf.org/rfc/rfc2401.txt
[11] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)," IETF RFC 2409, 1998 http://www.ietf.org/rfc/rfc2401.txt
[12] V. Devarapalli, F. Dupont, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture" IETF draft (2006)
[13] D. Simon, B. Aboba, R. Hurst, "The EAP-TLS authentication protocol", IETF RFC 2716, 2008 http://www.ietf.org/rfc/rfc2716.txt
[14] OpenIKEv2, http://openikev2.sourceforge.net/
[15] Nautilus 6 Project, http://www.nautilus6.org/
[16] WIDE Project, http://www.wide.ad.jp/
[17] MIPL Mobile IPv6, http://mobile-ipv6.org/
[18] C. Rigney, S. Willens, A. Rubens, W. Simpson., "Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2865, Jun 2000.
[19] Free Radius, http://freeradius.org/
[20] R. Marín, F. Pereñiquez, F. Bernal, A. Skarmeta, "Architecture for Fast EAP Re-authentication based on a new EAP method (EAP-FRM) working on standalone mode", IETF draft, 2009 http://tools.ietf.org/html/draft-marin-eap-frm-fastreauth-00

Aplicación de técnicas de programación lineal en la asignación óptima de recursos en redes inalámbricas heterogéneas

Ramón Agüero, Johnny Choque, Eva-María Hortigüela, Luis Muñoz
Departamento de Ingeniería de Comunicaciones
Universidad de Cantabria
Plaza de la Ciencia s/n, Santander
{ramon, jchoque, luis}@tlmat.unican.es

***Resumen*—En este artículo se estudian las posibilidades que la aplicación de técnicas de programación lineal tiene en el ámbito de la selección de acceso en entornos de red heterogéneos. Se presenta una herramienta implementada a partir de la librería *GLPK* que, a partir de un modelo de red, permite obtener la asignación de elementos de acceso óptima. Para ello se define una función de coste (*utilidad*) flexible, que permite modular la importancia otorgada a diferentes aspectos que se pueden considerar a la hora de acometer los procesos de selección de acceso: conexión con operador preferente, calidad del enlace inalámbrico, minimización del número de traspasos, entre otros. Dicha herramienta se emplea, posteriormente, para analizar un conjunto canónico de estrategias de selección de acceso, lo que permite establecer la combinación de parámetros de la función de utilidad que ofrezca mejores resultados.**

I. Introducción

La reciente proliferación de tecnologías radio, así como los avances en la miniaturización electrónica, hace que cada vez sea más habitual disponer de dispositivos capaces de comunicarse con varias tecnologías. Los escenarios de comunicaciones en un futuro cercano (aquello que se ha venido a llamar como 4G) estarán caracterizadas por un número elevado de alternativas de acceso, no sólo desde el punto de vista tecnológico, sino también teniendo en cuenta el número de entidades que operan las redes disponibles para el usuario final.

En el marco anteriormente bosquejado es necesario considerar los nuevos retos que aparecen en los procesos de selección de acceso, que actualmente se basan (casi en su totalidad) en procedimientos no automáticos con la participación activa del usuario. Es necesario desarrollar mecanismos que automaticen los procedimientos subyacentes, de manera que el usuario siempre pueda contar con el acceso óptimo, teniendo en cuenta sus preferencias personales, la situación puntual de la red, así como los requerimientos concretos de los servicios que esté utilizando en cada momento.

Para llegar a conseguir este comportamiento es necesario que las diferentes entidades de la red cooperen entre ellas (diferentes estaciones base, puntos de acceso, usuarios, operadores, etc) y que se establezcan mecanismos de señalización que permitan transportar la información de control necesaria para tomar la decisión óptima. Evidentemente, esta información tendrá una naturaleza 'local', esto es, limitada al usuario, en tanto en cuanto éste no podrá conocer las posibles consecuencias de su decisión sobre otros nodos de la red. Adicionalmente, para poder establecer la idoneidad de los mecanismos de selección de acceso empleados, se hace necesario disponer del mejor comportamiento que es posible alcanzar.

En este trabajo se trata de analizar dicho comportamiento óptimo, para lo que se propone utilizar técnicas de programación lineal. Para ello se modela un escenario de comunicaciones heterogéneo (con varias tecnologías y operadores) como un problema de optimización, utilizando una función de *utilidad* u objetivo que permite modular el peso dado a diferentes parámetros de mérito. Para resolver dicho problema se utiliza la librería *GNU Linear Programming Kit (GLPK)* [1]. Los resultados obtenidos permiten establecer, entre otras cosas, cuál debe ser la combinación de pesos a emplear por parte de los algoritmos de selección de acceso para garantizar un comportamiento óptimo.

Para cubrir el objetivo anteriormente establecido, el artículo se ha estructurado en los siguientes puntos: la Sección II ofrece una perspectiva del trabajo relacionado y que se encuentra en la literatura actual, estableciendo las diferencias principales. La Sección III presenta el problema de optimización que se plantea, el cual se resuelve con la herramienta descrita en la Sección IV. La Sección V describe el escenario que se utilizará para analizar una serie de estrategias de acceso, cuyas prestaciones se presentan en la Sección VI. Finalmente, la Sección VII concluye el artículo, identificando varias líneas que se abren a partir del trabajo.

II. Trabajo relacionado

Como ya se ha adelantado anteriormente, el amplio abanico de tecnologías de acceso radio que actualmente existen, junto con la proliferación de terminales que incorporan un conjunto de ellos, son algunos de los aspectos que establecen el camino hacia futuros sistemas de acceso inalámbricos, caracterizados principalmente por su heterogeneidad desde el punto de vista tecnológico. En este tipo de escenarios, los procedimientos empleados en la actualidad para acometer la selección del acceso a utilizar (principalmente estáticos, requiriendo la intervención directa del usuario) dejan de ser válidos; como alternativa, la comunidad científica está, en los últimos tiempos, llevando a cabo una serie de propuestas encaminadas a lograr, como principal objetivo, el paradigma *Always Best Connected*, teniendo en cuenta, entre otros aspectos, las preferencias de los usuarios, los requerimientos de los servicios y la situación

en particular de la red. Como muestra del interés que este tipo de propuestas ha adquirido recientemente, se puede citar el hecho de que no sólo ha suscitado la atención de la comunidad científica, sino que los propios organismos de estandarización trabajan en la especificación de normas y procedimientos para fomentar la interoperabilidad entre redes heterogéneas; en este sentido hay que destacar principalmente el papel desempeñado por el grupo de trabajo IEEE 802.21 [2], [3], que ha definido un marco para favorecer los traspasos entre tecnologías de red heterogéneas (*Media Independent Handover Framework, MIHF*).

La posibilidad de emplear diferentes tecnologías radio tiene, como principal ventaja, la posibilidad que se abre de utilizar, en cada caso, las características de cada una de ellas en momentos determinados; por otro lado, también introduce una serie de inconvenientes, derivados de la complejidad que introduce en el sistema, ya que es necesario gestionar un conjunto más amplio de parámetros. En este sentido existe una serie de trabajos que plantean propuestas para resolver los retos que aparecen desde diferentes puntos de vista. Así, por ejemplo, los autores en [4] presentan su *Common Radio Resource Management, CRRM*, evolución de *Joint Radio Resource Management, JRRM* [5], y apuestan por la gestión conjunta de los recursos radio disponibles, asumiendo un solapamiento completo de las áreas de cobertura de las estaciones base, como también se asume en [6], y otorgando la gestión completa de los recursos a la red, haciendo uso de un esquema claramente centralizado. Una arquitectura que comparte muchas de las características del *CCRM* es el *Multi-Radio Resource Management, MRRM* [7], en la que se podría destacar, como elemento diferenciador, la relevancia otorgada a las diferentes estrategias de cooperación entre operadores [8]. En la misma línea, se han propuesto diferentes algoritmos para mejorar la asignación de recursos en base a parámetros específicos de cada tecnología radio [9], [5], o también en base a perfiles micro/macro económicos del usuario [10] o la red [11].

En el presente trabajo se propone ir más allá, teniendo en cuenta no sólo la red, sino también (y además de manera prioritaria) al terminal/usuario a la hora de gestionar los recursos radio. Utilizando técnicas de programación lineal el objetivo que se busca es doble: por un lado ser capaces de establecer unos límites superiores en cuanto a las prestaciones que es posible alcanzar con este tipo de sistemas, lo que permitirá comparar diferentes estrategias de selección de acceso; por otra parte, definiendo funciones de utilidad con un conjunto amplio de parámetros, estudiar las posibles combinaciones que ofrezcan unas prestaciones óptimas. A pesar de que la utilización de técnicas de optimización para este tipo de problemas pudiera parecer lógico, los autores no conocen muchos trabajos que hayan explorado sus posibilidades. Algunos de los que existen, por ejemplo [12], [13], [14] emplean un conjunto reducido de parámetros para definir la función a optimizar, sensiblemente más bajo que el que aquí se propone. Por otro lado, se puede también destacar otros trabajos que hacen uso de técnicas *Multi-Attribute Decision Making, MADM* como, por ejemplo, [15], [16], [17]. La diferencia fundamental es que se pueden ejecutar con la información sesgada que dispongan elementos aislados de la red (esto es, como posibles alternativas de algoritmos de selección de acceso), ya que son computacionalmente eficientes; sin embargo, no pueden usarse para encontrar el comportamiento óptimo de una red, que es precisamente, el principal objetivo buscado en este trabajo; de hecho, a raíz de las conclusiones que puedan extraerse al usar el marco presentado en este artículo, se podrían establecer los criterios a tener en cuenta a la hora de acometer la selección de acceso basándose en *MADM*.

III. Modelo del problema de optimización

Se cuenta con un escenario de red concreto en el que se despliegan M elementos de acceso (estaciones base o puntos de acceso), que contarán con alguna tecnología radio (*Radio Access Technology, RAT*) concreta y que disponen de una capacidad ϕ_j en cuanto al número máximo de usuarios a los que pueden dar servicio [1]; además, en el mismo escenario hay N usuarios, que tratan de establecer una conexión con uno de esos elementos de acceso, a través de terminales capaces de emplear cualquiera de las RATs presentes en el escenario. Se supone, por otro lado, que hay un número de operadores presentes en el área bajo análisis, por lo que cada uno de los elementos de acceso (j) tendrá un operador asociado (ζ_j) y cada usuario (i) tendrá asimismo un operador preferente (η_i).

Se define el conjunto de variables básico x_{ij}, de tal manera que:

$$x_{ij} = \begin{cases} 1 & \text{si usuario } i \text{ está conectado al acceso } j \\ 0 & \text{en caso contrario} \end{cases} \quad (1)$$

A partir de esta única variable básica[2], se establece un número de parámetros que se tratarán de potenciar a la hora de llevar a cabo la optimización. Estos aspectos tienen que ver principalmente con las preferencias que un usuario podría tener a la hora de decantarse por una alternativa u otra. En particular, se han contemplado los elementos que se presentan seguidamente.

- *Conectividad.* En este caso simplemente se modela la posibilidad que tiene el usuario de estar conectado a la red. Se utilizará el parámetro σ_{ij}, definido tal y como sigue:

$$\sigma_{ij} = \begin{cases} 1 & \text{si usuario } i \in \text{ cobertura acceso } j \\ 0 & \text{en caso contrario} \end{cases} \quad (2)$$

- *Operador preferente.* Con este parámetro se pretende reflejar la predisposición que los usuarios tienen a conectarse, en caso de que sea posible, con un operador preferente (existencia de contrato, mejores tarifas, etc). Se utilizará ψ_{ij} para modelar este parámetro, definida como:

$$\psi_{ij} = \begin{cases} 1 & \text{si } \eta_i = \zeta_j \\ 0 & \text{en caso contrario} \end{cases} \quad (3)$$

- *Traspasos.* Una vez que un usuario esté conectado a un elemento de acceso, preferirá mantener la conexión con

[1] En algunos trabajos se utilizan otro tipo de abstracción para la capacidad y la carga [18], [19]; en este caso, la abstracción se realiza en base al número de usuarios conectados.

[2] Como se puede ver las variables básicas del problema sólo puede tomar valores de 1 ó 0, con lo que para ser más específicos, se debería definir el problema como *Programación Entera Binaria*.

el mismo el máximo tiempo posible, de manera que no se incurra en la degradación (sobrecarga) que podría generar un proceso de traspaso. De esta manera, conociendo el acceso al que el usuario se había conectado previamente, se define el parámetro λ_{ij} como:

$$\lambda_{ij} = \begin{cases} 1 & \text{si usuario } i \text{ tenía conexión con acceso } j \\ 0 & \text{en caso contrario} \end{cases} \tag{4}$$

- *Calidad del enlace.* A la hora de seleccionar entre varias alternativas de acceso, uno de los aspectos que tradicionalmente más se han empleado es la calidad del enlace radio. Evidentemente se trata de un aspecto que depende fuertemente de la tecnología radio y del modelo de propagación empleados. En general, se puede asegurar que se corresponde con una función decreciente con la distancia al elemento de acceso[3]; en este caso, se utilizará una función triángulo, que tome el valor máximo (1) en la posición del elemento de acceso y el mínimo (0), justo en el límite de su área de cobertura, de tal manera que se define el parámetro θ_{ij}:

$$\theta_{ij} = \begin{cases} 1 - \dfrac{d_{ij}}{\omega_j} & \text{si } d_{ij} < \omega_j \\ 0 & \text{en caso contrario} \end{cases} \tag{5}$$

  donde ω_j es la cobertura de la RAT del elemento de acceso j y d_{ij} la distancia con el usuario i.

A partir de los elementos anteriores, se define una función de utilidad (u_{ij}), que los combina, permitiendo establecer una clasificación de los elementos de acceso disponibles. Como se puede ver, si no hay posibilidad de conexión entre el usuario i y el elemento de acceso j (σ_{ij}), la función de utilidad toma un valor nulo.

$$u_{ij} = [\alpha + \beta \cdot \psi_{ij} + \gamma \cdot \lambda_{ij} + \delta \cdot \theta_{ij}]\, \sigma_{ij} \tag{6}$$

Para que dicha función de utilidad sea lo más flexible posible, se modula cada uno de los aspectos anteriormente mencionados por un peso; así, α promueve la conexión con un elemento cualesquiera; β que se emplee un acceso del operador preferente; γ se utiliza para minimizar la necesidad de cambiar de elemento de acceso; finalmente δ modula el parámetro correspondiente a la calidad del enlace radio. En las definiciones anteriores se puede comprobar que todos las variables que se han definido están acotadas en $[0, 1]$, por lo que si se fija que la suma de los cuatro pesos sea igual a la unidad, $\alpha+\beta+\gamma+\delta = 1$, se puede acotar asimismo el valor de la *utilidad* de conexión entre el usuario i y el elemento de acceso j en el mismo intervalo. Además, de esta manera, se puede modificar fácilmente el peso otorgado a cada parámetro, permitiendo establecer diferentes políticas en el algoritmo de selección de acceso.

Con todo ello, se plantea el siguiente problema de optimización:

$$\begin{aligned} \textbf{Max.} \quad & \sum_{i=0,j=0}^{N-1,M-1} u_{ij} \cdot x_{ij} \\ \textbf{s.t.} \quad & \sum_{j=0}^{M-1} x_{ij} \leq 1 \qquad i = 0 \ldots N-1 \\ & \sum_{i=0}^{N-1} x_{ij} \leq \phi_j \qquad j = 0 \ldots M-1 \end{aligned} \tag{7}$$

El primer conjunto de restricciones establece que un usuario sólo pueda conectarse a un elemento de acceso, mientras que el segundo bloque limita el número de usuarios conectados a un acceso a la capacidad de éste último (ϕ_j). Es importante destacar que, para un despliegue de red concreto, todos los elementos que forman parte de u_{ij} dependen exclusivamente del escenario particular y que, por tanto, las únicas variables que se tienen que considerar a la hora de acometer la optimización son las x_{ij}.

IV. Diseño e implementación de una herramienta para resolver el problema de optimización

Como ya se ha adelantado, se hará uso de la librería *GLPK* para resolver el problema que se ha planteado anteriormente. Se ha seleccionado esta plataforma ya que su API se puede utilizar desde otras aplicaciones, lo que facilita sobremanera la integración del módulo de optimización (*solver*). Por otro lado la dimensión del problema a resolver está dentro de los límites que maneja *GLPK*, ya que el número de variables se sitúa por debajo de 10^4 y, además, muchos de los coeficientes (tanto de la función objetivo como de las restricciones) son 0.

Así, se desarrollará una herramienta que ejecute las siguientes acciones:

1) Leer parámetros de la red desde un fichero de configuración.
2) Desplegar las estaciones base a partir de un fichero.
3) Desplegar los usuarios a partir de un fichero.
4) Generar y procesar la red: obtención de todos los coeficientes u_{ij}.
5) Resolución del problema utilizando la API del *GLPK*.
6) Procesar la solución.

Como se ha visto anteriormente, uno de los aspectos que se tienen en cuenta a la hora de establecer los coeficientes u_{ij} es la conexión previa del usuario (para reducir, si fuera posible, el número de traspasos a realizar). En este caso se asume que la posición de los usuarios varía (en función de algún modelo de movilidad establecido) y que, por tanto, el programa principal deberá barrer un conjunto de ficheros de usuarios (*snapshots*) en los que la posición haya variado. En cada iteración se deberá asimismo utilizar el resultado anterior, para poder determinar el valor de λ_{ij}.

La Figura 1 presenta el diagrama de ejecución de todo el proceso.

A pesar de que la herramienta está diseñada para que el despliegue de los elementos de acceso y de los usuarios se pueda llevar a cabo de manera aleatoria, se utiliza principalmente la lectura de ficheros, ya que, establecido el formato correspondiente, es fácil integrar esta plataforma con otras

[3]Hay que destacar que el objetivo de este trabajo no es modelar de manera precisa el canal de propagación, sino que se centra en la selección óptima de un acceso, tal y como también realizan Lucas-Estan *et al.* [12]. De todas maneras, la implementación se ha llevado a cabo de manera que incorporar modelos de propagación empíricos más complejos resultaría relativamente sencillo.

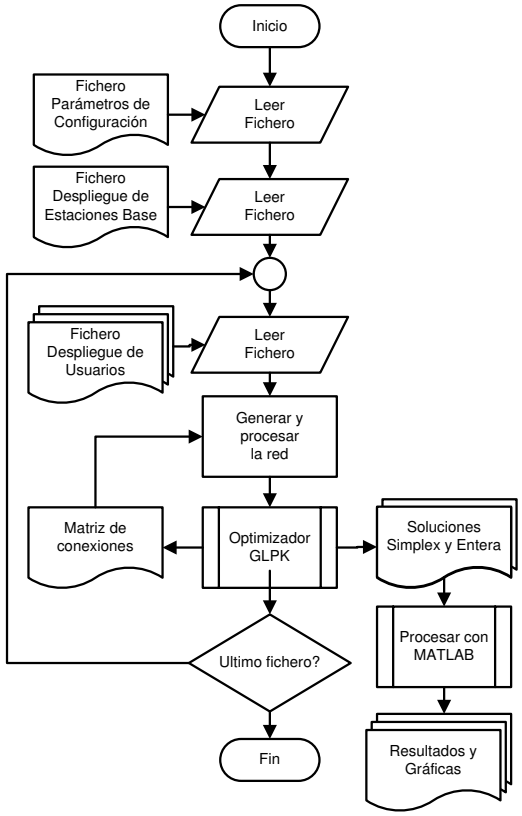


Fig. 1. Diagrama de bloques de la herramienta

herramientas que lleven a cabo análisis complementarios, utilizando el mismo escenario de red e idénticas trazas de movimiento, de manera que se pueda llevar a cabo una comparativa más precisa.

V. Escenario de red a analizar

Como se ha dicho anteriormente, se trata de analizar diferentes estrategias para acometer la selección (óptima) de acceso en un entorno de red heterogéneo. La heterogeneidad, además, no se debe limitar a las tecnologías presentes en el escenario, sino también a la presencia de varios operadores. Para cubrir dichos requerimientos se utilizarán tres tipos diferentes de elementos de acceso, cuyas características se resumen en la Tabla I. El primero de ellos *emula* una tecnología de características más similares a las comunicaciones inalámbricas tradicionales (GSM), pues consta de una cobertura sensiblemente mayor y, además, también presenta una capacidad mayor. Los otros dos elementos de acceso están más cerca de los puntos de acceso WLAN, con un alcance y una capacidad claramente inferiores[4]. Recordar que para modelar la capacidad se utiliza, de manera genérica, el número de usuarios máximos que puede conectarse a cada elemento de acceso, independientemente del tráfico subyacente.

Se supone, además, que coexisten dos operadores. El primero de ellos (A) es el operador incumbente, que gestiona los elementos de acceso de la tecnología típicamente celular (ρ_0), mientras que el segundo (B) sería el nuevo operador,

[4]El uso de tecnologías radio diferentes es relativamente sencillo, ya que únicamente se tiene que especificar su capacidad y alcance.

Tabla I
Tecnologías empleadas durante el análisis

ID	Cobertura (m)	Capacidad	# Elementos
ρ_0	600	20	4
ρ_1	80	5	16
ρ_2	60	5	20

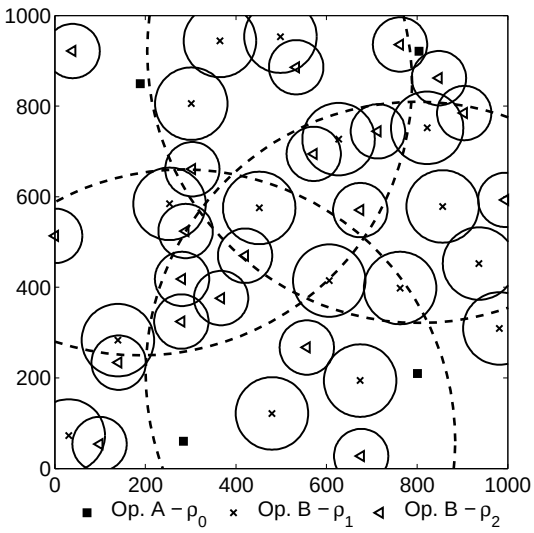


Fig. 2. Despliegue de red empleado durante el análisis

que ofrece un acceso menos convencional, a través de los elementos de acceso de tecnologías ρ_1 y ρ_2.

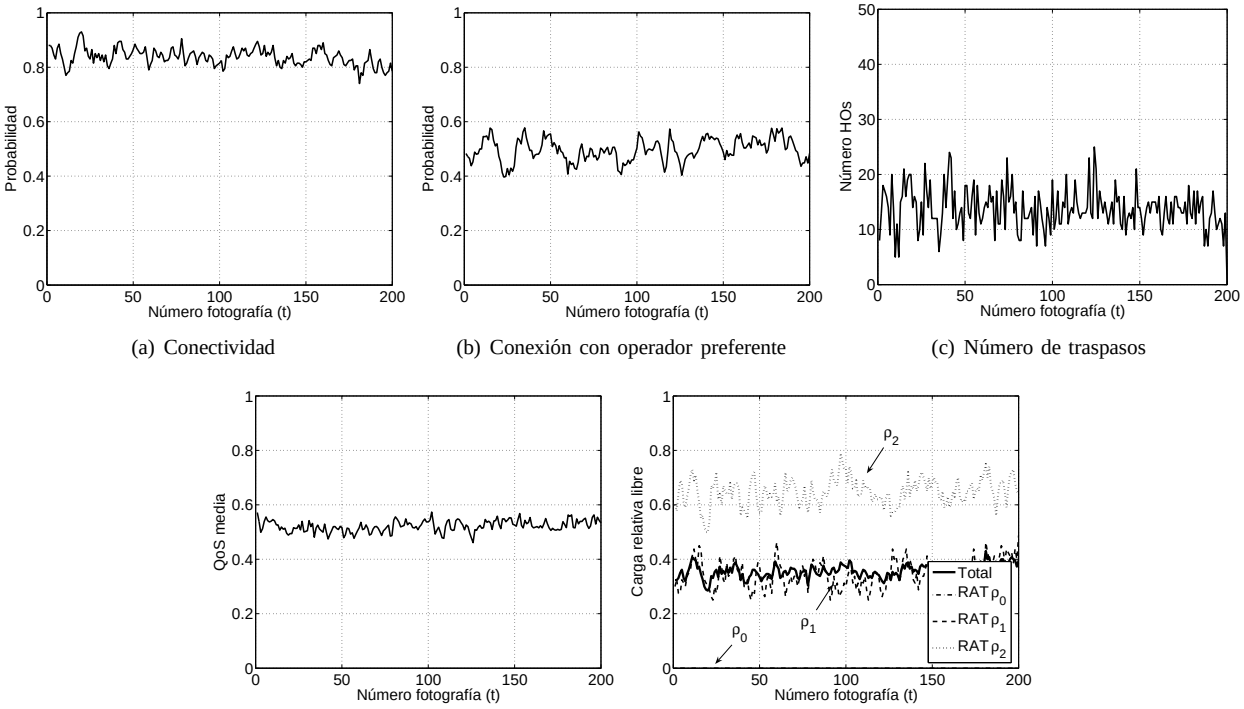
Se considera además un área de $1000 \times 1000\ m^2$, en el que los elementos de acceso se despliegan sin una planificación previa, según un despliegue aleatorio, aunque se limita la distancia entre ellos (siempre que sean del mismo operador y de la misma tecnología). Con todo esto, la red que se analizará es la que se muestra en la Figura 2, en la que se puede ver que los 4 elementos de acceso ρ_0 cubren completamente todo el área bajo análisis, existiendo diferentes zonas con un notable grado de solapamiento. El área cubierta por el operador (B) es sensiblemente menor.

Se despliegan 200 usuarios, de los que se asume que el 60% son clientes del operador A, mientras que el resto lo son del menos tradicional, B. Se supone además que todos los usuarios son capaces de utilizar cualquiera de las tecnologías presentes en el escenario. Los usuarios inicialmente se sitúan aleatoriamente en el área bajo análisis y posteriormente se mueven libremente según el modelo *Random Waypoint* [20], con las características que se resumen en la Tabla II.

Una vez presentado el escenario sobre el que se llevará a cabo el análisis, la Tabla III presenta las diferentes estrategias de selección de acceso. Como se puede ver, se va modificando el valor que se le otorga a cada peso, de manera que cada

Tabla II
Características del modelo *Random Waypoint* empleado en el análisis

Característica	Valor
Velocidad	$\mathbb{U}[2,3]\ m/s$
Tiempo de movimiento	$\mathbb{U}[100,120]\ m/s$
Tiempo de pausa	$\mathbb{U}[5,10]\ s$
Estrategia en los límites	Reflexión



(a) Conectividad (b) Conexión con operador preferente (c) Número de traspasos

(d) Calidad media (e) Carga relativa libre

Fig. 3. Evolución temporal de los parámetros de mérito en la estrategia de selección de acceso **G**

Tabla III
ESTRATEGIAS DE SELECCIÓN DE ACCESO ANALIZADAS

Parámetro	A	B	C	D	E	F	G
α	1.0	0.6	0.4	0.1	0.1	0.1	0.1
β	0.0	0.2	0.2	0.9	0.0	0.0	0.0
γ	0.0	0.0	0.2	0.0	0.9	0.0	0.7
δ	0.0	0.2	0.2	0.0	0.0	0.9	0.2

estrategia dará prioridad a alguno de los parámetros que se han presentado anteriormente. La estrategia **A** tiene como único objetivo maximizar el número de usuarios conectados; en el caso **B** se favorece ligeramente las conexiones con el operador preferente y la calidad del enlace, mientras que en **C** también se otorga relevancia a la minimización del número de traspasos. Las estrategias **D**, **E** y **F** priorizan únicamente uno los tres parámetros que se han presentado anteriormente (operador preferente, número de traspasos y calidad del enlace, respectivamente), dando una importancia residual a la probabilidad de conexión. Finalmente, la estrategia **G** busca principalmente minimizar el número de traspasos, pero tiene asimismo en cuenta la calidad del enlace.

VI. RESULTADOS

A continuación se describen los resultados obtenidos al emplear las 7 estrategias de selección de acceso que se han presentado previamente. La simulación tiene una duración de 2000 segundos, tomando *'fotografías'* de la posición de los usuarios con una periodicidad de 10 s, con lo que cada escenario concreto conlleva la resolución de 200 problemas de optimización.

Para valorar el comportamiento de las diferentes alternativas, se analizarán un conjunto de métricas, que se describen seguidamente.

- *Probabilidad de conexión.* Se trata del parámetro básico, en el que únicamente se considera si un usuario se ha podido conectar a la red o no.
- *Conexión con el operador preferente.* Se tiene en cuenta si la conexión de un usuario es con un elemento de acceso que pertenezca a su operador preferente.
- *Número de traspasos.* Permite estudiar el número de cambios de elemento de acceso que se tiene que llevar a cabo.
- *Calidad media*. Promedia la calidad de los enlaces que se establecen en la red, empleando la función que se presentó en la Sección III.
- *Carga libre.* Se utiliza para estudiar cuál es la capacidad libre que existe (por tipo de elemento de acceso); este es un parámetro que permitirá establecer la posibilidad de incorporar o no nuevos usuarios.
- *Tráfico cursado por operador.* En este caso se analizará cuál es el tráfico cursado[5] por cada uno de los operadores, así como el porcentaje de usuarios del otro operador que se conectan, lo que permitiría estimar, por ejemplo, ingresos por *roaming*.

En una primera aproximación, se estudiará la variación temporal de alguno de los parámetros mencionados anteriormente, con el objetivo de comprobar la estabilidad a lo largo de un escenario en particular (conjunto de *'snapshots'* o fotografías con una única traza de movimiento) y para una estrategia de acceso concreta. Posteriormente se realizarán 10 simulaciones independientes por cada configuración, promediando el resultado final, para comparar las siete combinaciones de los pesos que se han planteado en la Sección V.

[5]En este caso el tráfico cursado se corresponde realmente con el número de usuarios conectados.

La Figura 3 presenta la probabilidad de conexión total, la de conexión con el operador preference, el número de traspasos, la calidad media en las comunicaciones que se establecen y la capacidad disponible en la red (diferenciando entre los tres tipos de RAT en este último caso) para la estrategia **G**. Como se puede ver, en ninguno de los casos se observa una desviación notable en torno al valor medio. La probabilidad de conexión global alcanza un valor cercano al 85%, mientras que únicamente el 50% de las conexiones lo son con el operador preferente; hay que tener en cuenta el peso otorgado a dicho parámetro en la estrategia **G** (nulo), así como el reparto de los usuarios según el *Market Share* (distribución de los usuarios por operador) establecido. Se observa que la ejecución de traspasos es el parámetro en el que aparece una mayor variabilidad, aunque su valor (para esta estrategia concreta) no es elevado (menor del 10%). En cuanto a la calidad media se sitúa, de manera muy estable, en torno al 50%.

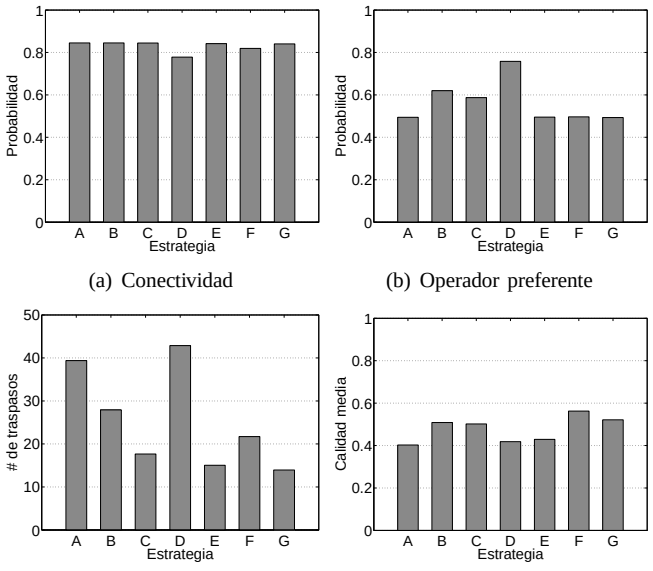
Más interesante si cabe es el análisis de la capacidad disponible en función del tipo de elemento de acceso. Se puede ver que la capacidad libre de la red se sitúa ligeramente por debajo del 40% de su capacidad. Aunque pudiera parecer extraño, a la vista de los resultados de conectividad, hay que tener en cuenta que los elementos de acceso de RATs ρ_1 y ρ_2, tienen, en global, una capacidad notable ($80 + 100$), siendo incluso mayor que la atesorada por ρ_0 (100), pero cubren un porcentaje escaso del área bajo análisis. La consecuencia es que no hay suficientes usuarios en las zonas cubiertas por estos elementos. De hecho, se pone de manifiesto el mayor alcance de ρ_1, ya que la capacidad disponible es menor de la que se observa para ρ_2, pudiéndose asegurar que su factor de utilización es relativamente bajo. Finalmente, se comprueba que los elementos de acceso pertenecientes a ρ_0 están completamente al límite de su carga, ya que como se vio anteriormente, cubren completamente todo el área bajo análisis y, consecuentemente, es bastante probable que haya usuarios cuya única alternativa de conexión sea, precisamente, conectarse a dicha RAT.

A pesar de que los resultados instantáneos permiten adquirir una primera idea acerca del comportamiento de las diferentes estrategias de selección de acceso, es más interesante poder compararlas entre ellas, para así analizar las ventajas y desventajas que se desprenden de utilizar una u otra en particular. Eventualmente, si se hiciera un barrido de los valores asignados a cada uno de los pesos empleados, se podría llegar a estudiar cuál es la combinación que proporciona un comportamiento más óptimo. En nuestro caso se utilizarán las 7 estrategias que se presentaron en la Tabla III, haciendo, para cada una de ellas, 10 medidas independientes, cuyos resultados serán promediados, para obtener el comportamiento final.

En primer lugar, la Figura 4(a) presenta la probabilidad de conexión que se obtuvo para cada una de las 7 estrategias analizadas; se comprueba que las diferentes combinaciones de pesos no tienen una influencia muy determinante en los resultados alcanzados, pues se observa que en todas las estrategias, la probabilidad de conexión se sitúa en valores cercanos al 80%. Se puede ver, sin embargo, una ligera disminución en las estrategias **D** y **F** (algo mayor en la primera de ellas); en **D** se favorece la conexión con el operador preferente, lo que hace que los elementos de acceso ρ_0, que pertenecen al operador dominante, completen su capacidad con mayor facilidad, lo que, unido al hecho de que la conexión con los otros dos grupos de elementos de acceso es menos probable (cubren un porcentaje menor del área bajo análisis), se traduce en la disminución observada, que en cualquier caso no llega al 10%. La disminución es aún menos significativa para la estrategia **F**, debiéndose, en esta ocasión, al hecho de que se favorezca la calidad de los enlaces, lo que también incrementa la probabilidad de conexión con los elementos de acceso con RAT ρ_0.

Sin embargo, se puede ver en la Figura 4(b) que, en lo que se refiere a las conexiones con elementos de acceso del operador preferente, sí que existen diferencias relevantes en función de la estrategia de selección de acceso empleada. En aquellas combinaciones en las que el peso dado al parámetro β en la *función utilidad* es 0, la probabilidad de conexión con el operador preferente no varía, situándose en valores cercanos al 50%; hay que tener en cuenta que el 60% de los usuarios son *clientes* del operador que gestiona los elementos de acceso con mayor cobertura (ρ_0). Por su parte, al comparar las estrategias **B**, **C** y **D** se puede ver que la ganancia obtenida al incrementar β desde 0.2 (en las dos primeras) hasta 0.9 (en la última) es del 15%; además, la probabilidad de conexión al operador preferente en la estrategia **C** es ligeramente inferior a la que se observa en la **B**, ya que en aquélla se da cierta relevancia, además, a la calidad del enlace con la estación base, lo que disminuye ligeramente el número de conexiones con el operador preferente.

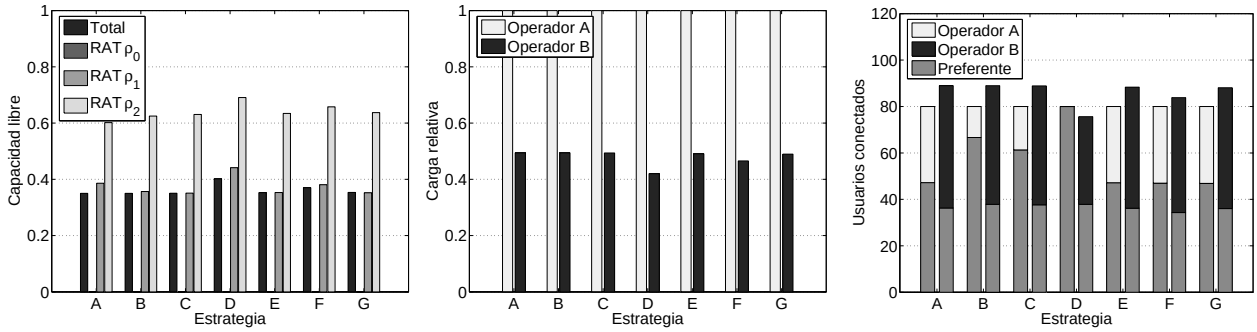
Las Figuras 4(c) y 4(d) muestran los resultados obtenidos tanto para el número de traspasos como para la calidad media de los enlaces empleados, respectivamente, para las 7 estrategias de acceso analizadas. En primer lugar se puede ver que en este caso existe una relación clara entre ambos parámetros. Así, si se comparan los resultados entre las estrategias **A** y **B** (en las que el valor de γ, peso que favorece



(a) Conectividad (b) Operador preferente

(c) Número de traspasos (d) Calidad media

Fig. 4. Prestaciones de las diferentes estrategias de acceso



(a) Carga libre por RAT (b) Capacidad por operador (c) Número de usuarios conectados

Fig. 5. Prestaciones de las estrategias de acceso - capacidad y carga libre

reducir el número de cambios de elemento de acceso, toma el mismo valor) se puede ver que el número de traspasos observados al usar la primera estrategia es sensiblemente mayor ($\gtrsim 25\%$); esto se debe al hecho de que al favorecer los enlaces con una calidad mayor ($\delta = 0.2$ en la estrategia **B**) es más probable seleccionar elementos de acceso a una distancia menor, con la consecuencia de que será menos probable llevar a cabo un traspaso en los siguientes instantes temporales. De alguna manera, este aspecto se vuelve a plasmar al comparar los resultados de las estrategias **E** y **G**; en la primera, se favorece exclusivamente reducir el número de traspasos a realizar ($\gamma = 0.9$), mientras que en la segunda se reduce γ un 20%, para incrementar el peso correspondiente a la calidad del enlace $\delta = 0.2$; como se puede ver, la consecuencia es que se logra incrementar sensiblemente la calidad media de todas las conexiones (alrededor del 10%), sin afectar negativamente al número de traspasos que, incluso, se reduce ligeramente (a pesar de que se ha bajado el valor de γ).

Por otro lado, la Figura 5 permite analizar cuál es la influencia de las diferentes combinaciones de pesos analizadas en lo que se refiere a la capacidad disponible en la red, tanto a nivel de RAT como de operador. Como se pudo comprobar anteriormente, los elementos de acceso de la RAT ρ_0 (que coinciden con la capacidad total del operador *A*) agotan completamente sus recursos, lo que sucede con todas las estrategias de selección de acceso estudiadas. Lógicamente, los resultados de conectividad (Figura 4(a)) se corresponden totalmente con los de la carga libre, y es únicamente en la estrategia **D** en la que se observa una mayor capacidad disponible en la red, ya que los elementos de acceso gestionados por el operador *B* reducen ligeramente su carga. En clara relación con estos resultados, la Figura 5(c) presenta el número de usuarios conectados por operador, destacándose además, aquellos que son *clientes* de su operador preferente; en este caso se pone de manifiesto la influencia del parámetro β, ya que en las estrategias en las que toma un valor superior a 0 (**B**, **C** y **D**), el número de usuarios conectados a su operador preferente se incrementa. Se observa, por otro lado, que esto exclusivamente afecta al operador dominante, ya que el número de usuarios que, siendo clientes de *B*, se pueden conectar a su operador preferente se mantiene constante (algo menos de 40 usuarios) para todas las estrategias. La consecuencia, en la estrategia **D**, es que todos los usuarios que se conectan al operador *A* (80, que equivale a su capacidad total) lo tienen como operador preferente, lo que reduce el tráfico que cursaría el operador *B*. Evidentemente, a la vista de los valores obtenidos, se podrían establecer diferentes mecanismos de cooperación entre los operadores para incrementar los beneficios, aplicando tarifas diferenciadas para el tráfico proveniente de los clientes propios o de *roaming*.

VII. Conclusiones

En este trabajo se ha puesto de manifiesto las posibilidades que la aplicación de técnicas de programación lineal abren a la hora de analizar estrategias de selección de acceso, en despliegues de red heterogéneos, tanto a nivel de tecnologías radio como de operadores. Se ha definido un problema de optimización, en el que la función objetivo (a maximizar) se puede adaptar en función de un conjunto de parámetros que determinan las posibles prioridades que un usuario puede tener a la hora de decantarse por un acceso u otro.

Para resolver el problema planteado se ha diseñado e implementado una aplicación, que hace uso de la librería *GLPK*. Dicho marco se ha utilizado para analizar un conjunto de estrategias de selección de acceso, en las que se ha ido variando el peso dado a los diferentes aspectos, para comprobar cuál es la influencia de los mismos. Utilizando un escenario con dos operadores y una heterogeneidad (a nivel de tecnologías radio) relevante se ha puesto de manifiesto que hay ciertas combinaciones que ofrecen mejores prestaciones que otras (al menos en términos del número de traspasos y de la calidad de los enlaces radio establecidos). Se ha comprobado, por ejemplo, que el favorecer la elección de enlaces radio con una calidad mayor conlleva una disminución del número de traspasos. También se ha analizado la influencia de los diferentes parámetros en cómo la carga se distribuye entre los diferentes tipos de elementos de acceso (y operadores).

El trabajo presentado permite establecer un notable número de líneas de actuación; en primer lugar, la definición de la *utilidad* es muy flexible, lo que permitiría incluir nuevas métricas en el proceso de selección o modificar sus pesos. Esta flexibilidad se puede aprovechar, por ejemplo, para llevar a cabo un barrido más fino, permitiendo establecer la combinación óptima. Además, los resultados obtenidos a partir de este análisis, entendidos como los mejores a los que se puede llegar para un despliegue de red concreto, se podrán comparar con otro tipo de estudios, en los que únicamente se tenga en cuenta la información (de carácter más local) circunscrita en

el entorno del usuario. También se podrían utilizar modelos de tráfico más realistas, en los que además se pueda variar la capacidad requerida al establecer una conexión. Finalmente, se podrían modificar los parámetros del escenario, en cuanto a cuota de mercado, número de usuarios, distribución de los elementos de acceso, etc., con el fin de comprobar la influencia de todos estos parámetros sobre el comportamiento final del sistema.

AGRADECIMIENTOS

Los autores querrían expresar su agradecimiento al Gobierno de España por su financiación en los siguientes proyectos: Mobilia - Programa CELTIC (Avanza I+D TSI-020400-2008-82) y "Comunicaciones Cognitivas y Cooperativas sobre Entornos Heterogéneos", C3SEM (TEC2009-14598-C02-01)

REFERENCIAS

[1] GLPK (GNU linear programming kit). http://www.gnu.org/software/glpk/.

[2] IEEE standard for local and metropolitan area networks- part 21: Media independent handover. *IEEE Std 802.21-2008*, 2009.

[3] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik y D. Famolari. IEEE 802.21: Media independent handover: Features, applicability, and realization. *Communications Magazine, IEEE*, 47(1):112 –120, january 2009.

[4] J. Perez-Romero, O. Sallent, R. Agusti, P. Karlsson, A. Barbaresi, L. Wang, F. Casadevall, M. Dohler, H. Gonzalez y F. Cabral-Pinto. Common radio resource management: functional models and implementation requirements. En *Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on*. 2005.

[5] L. Giupponi, R. Agusti, J. Perez-Romero y O. Sallent. Joint radio resource management algorithm for multi-RAT networks. En *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, tomo 6. dec. 2005.

[6] B. Chen y M. Chan. Resource management in heterogenous wireless networks with overlapping coverage. En *Communication System Software and Middleware, 2006. Comsware 2006. First International Conference on*. 2006.

[7] J. Sachs, R. Aguero, K. Daoud, J. Gebert, G. Koudouridis, F. Meago, M. Prytz, T. Rinta-aho y H. Tang. Generic abstraction of access performance and resources for multi-radio access management. En *Mobile and Wireless Communications Summit, 2007. 16th IST*. july 2007.

[8] L. Ho, J. Markendahl y M. Berg. Business aspects of advertising and discovery concepts in ambient networks. En *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*. 2006.

[9] A. Tolli, P. Hakalin y H. Holma. Performance evaluation of common radio resource management (CRRM). En *Communications, 2002. ICC 2002. IEEE International Conference on*, tomo 5. 2002.

[10] L. Giupponi, R. Agusti, J. Perez-Romero y O. Salient. Wlc05-2: An economic-driven joint radio resource management with user profile differentiation in a beyond 3G cognitive network. En *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*. 2006.

[11] L. Giupponi, R. Agusti, J. Perez-Romero y O. Salient. Improved revenue and radio resource usage through inter-operator joint radio resource management. En *Communications, 2007. ICC '07. IEEE International Conference on*. june 2007.

[12] M. Lucas-Estan, J. Gozalvez y J. Sanchez-Soriano. Common radio resource management policy for multimedia traffic in beyond 3G heterogeneous wireless systems. En *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*. sept. 2008.

[13] O. Falowo y H. Anthony Chan. Optimal joint radio resource management to improve connection-level qos in next generation wireless networks. En *Radio and Wireless Symposium, 2008 IEEE*. 2008.

[14] N. Karthikeyan Krishnasamy y P. Narayanasamy Palanisamy. Bandwidth allocation scheme for multimedia mobile networks using optimization techniques. En *Cybernetics and Intelligent Systems, 2006 IEEE Conference on*. june 2006.

[15] C. Gu, Y. Zhang, W. Ma, N. Liu y Y. Man. Universal modeling and optimization for multi-radio access selection. En *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*. 2009.

[16] B. Xing y N. Venkatasubramanian. Multi-constraint dynamic access selection in always best connected networks. En *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*. july 2005.

[17] H. Hu, W. Zhou, S. Zhang y J. Song. A novel network selection algorithm in next generation heterogeneous network for modern service industry. En *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*. dec. 2008.

[18] W. Shen y Q.-A. Zeng. Resource management schemes for multiple traffic in integrated heterogeneous wireless and mobile networks. En *Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on*. 2008.

[19] N. Nasser y H. Hassanein. Dynamic threshold-based call admission framework for prioritized multimedia traffic in wireless cellular networks. En *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE*, tomo 2, páginas 644 – 649 Vol.2. 29 2004.

[20] T. Camp, J. Boleng y V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications*, 2(5):483–502, 2002.

Diseño intercapas aplicado a la asignación adaptativa de recursos en sistemas MIMO-OFDMA

Borja Dañobeitia, Guillem Femenias
Grupo de Comunicaciones Móviles - Universitat de les Illes Balears (UIB)
Ctra. Valldemossa km. 7.5 - 07122 - Palma - SPAIN
Email: {borja.danobeitia,guillem.femenias}@uib.es

***Resumen*—En este trabajo se proponen algoritmos para la asignación eficiente de recursos en el canal descendente de un sistema MIMO-OFDMA. Se recurre a la programación matemática para resolver el problema de la maximización de la tasa de transmisión global del sistema con restricciones sobre la potencia total disponible. Además, para llevar a cabo un proceso de optimización intercapas, se analiza el comportamiento de las colas de paquetes en la capa DLC y se incorporan restricciones sobre métricas de QoS como la probabilidad de pérdida de paquetes o el retardo medio por paquete. Dada la naturaleza combinatoria y no convexa de este tipo de problemas, se plantea la optimización en el dominio dual recurriendo al método del subgradiente para diseñar algoritmos de reducida complejidad. Los resultados obtenidos demuestran que el uso de requerimientos de QoS en el planteamiento del problema permite asignar recursos de manera eficiente y equitativa.**

I. Introducción

Los sistemas de comunicaciones móviles de tercera generación, conocidos bajo el nombre genérico de sistemas IMT-2000 (*International Mobile Communications 2000*), están evolucionando hacia los sistemas de cuarta generación, también conocidos bajo el nombre genérico de sistemas IMT-*Advanced*. Los grupos de trabajo del 3GPP (*3rd Generation Partnership Project*) y del IEEE/WiMAX Forum que trabajan actualmente en el proceso de estandarización de estos sistemas, coinciden en que los pilares tecnológicos que dan soporte a los sistemas IMT-2000 – acceso múltiple OFDMA (*Orthogonal Frequency Division Multiple Access*), esquemas de transmisión MIMO (*Multiple-Input Multiple-Output*), sistemas de modulación y codificación adaptativa combinados con esquemas HARQ (*Hybrid Automatic Repeat reQuest*), y algoritmos de asignación dinámica de recursos con soporte de QoS (*Quality of Service*) – continuarán dando soporte a los sistemas IMT-*Advanced*. También coinciden en que, para cumplir con los requerimientos especificados por la ITU (*International Telecommunications Union*) para los sistemas IMT-*Advanced*, estos deberán incorporar propuestas tecnológicas que permitan mejorar las prestaciones de las últimas versiones de los sistemas IMT-2000. Algunas de las propuestas de mejora que han ido apareciendo incluyen, entre otras: el uso de estaciones base y estaciones repetidoras cooperativas (diversidad cooperativa o virtual-MIMO), el uso de esquemas avanzados de explotación de técnicas MU-MIMO (*Multiuser MIMO*) o el uso de técnicas de diseño intercapas (*cross-layer design*) en los algoritmos de asignación de recursos que permitan explotar, simultáneamente, la denominada *diversidad multiusuario* propia de canales que presentan selectividad espacio-temporal y la heterogeneidad de requerimientos de QoS propia de los diferentes servicios que soportarán los sistemas IMT-*Advanced*.

Dentro de este marco general y partiendo de los modelos analíticos propuestos por Seong *et al.* [1] y Kong *et al.* [2], que suponen la disponibilidad de información sobre el estado del canal (CSI - *Channel State Information*) tanto en la estación base (BS - *Base Station*) como en las estaciones móviles (MSs - *Mobile Stations*), el objetivo de este artículo es proponer y analizar algoritmos para la asignación eficiente de recursos en el canal descendente de un sistema MIMO-OFDMA basado en el uso de precodificación lineal óptima en transmisión. Se considera el uso de programación matemática para resolver el problema de la maximización de la tasa de transmisión global de sistemas MIMO-OFDMA con restricciones sobre la potencia total disponible. A diferencia de la mayoría de propuestas anteriores, que no incorporan restricciones sobre métricas de QoS propias de la capa DLC como la probabilidad de pérdida de paquetes (PDP - *Packet Dropping Probability*) o el retardo de paquete, en este artículo se analiza el comportamiento de las colas de paquetes en la capa DLC, correspondientes a servicios heterogéneos caracterizados por diferentes requerimientos de QoS, con el fin de llevar a cabo un proceso de asignación de recursos basado en el diseño intercapas. De esta forma, los procesos de planificación (*scheduling*) de paquetes en la capa DLC y los algoritmos de asignación de potencia, subportadoras y tasas de transmisión (modos de transmisión del esquema de modulación y codificación adaptativa) en la capa PHY estarán relacionados no solamente con la CSI observada en la capa PHY sino también con la información sobre el estado de las colas (QSI - *Queue State Information*) observada en la capa DLC.

El problema de la asignación de recursos en sistemas MIMO-OFDMA es, en esencia, combinatorio y *no* convexo y, en consecuencia, su complejidad crece exponencialmente con el número total de usuarios y subportadoras del sistema [3] y no permite la utilización de métodos eficientes de optimización convexa. De todas formas, en [4] Yu y Lui demuestran que se puede utilizar el método de descomposición dual de Lagrange para determinar una solución cuasi-óptima, teniendo en cuenta que el *duality gap*, es decir, la diferencia entre la solución dual y la solución óptima, tiende a cero cuando el número de subportadoras tiende a infinito. Así pues, en este artículo utilizamos los resultados de Yu y Lui para plantear el problema de optimización en el dominio dual y recurrimos posteriormente al método del subgradiente [5] para diseñar algoritmos de reducida complejidad que permiten ofrecer una solución global y eficaz al problema de asignación adaptativa de recursos en sistemas multiportadora.

II. MODELO DEL SISTEMA

Este trabajo se centra en el estudio del enlace descendente de un sistema MIMO-OFDMA. Con el fin de simplificar el problema, se supone que pueden ignorarse los efectos de la interferencia intercelular, bien debido a que existe una separación suficiente entre estaciones base que utilizan frecuencias co-canal o bien debido a que se utiliza la hipótesis Gaussiana sobre las interferencias y por tanto la potencia interferente únicamente supone un incremento de la varianza del ruido Gaussiano blanco aditivo. Así pues, se considerará una red unicelular con una estación base equipada con N_T antenas transmisoras y ubicada en el centro de la célula, que proporciona servicio a K estaciones móviles activas, equipadas con N_R antenas receptoras, a través de un esquema OFDMA que dispone de N subportadoras útiles[1]. Subportadoras y estaciones móviles se indexan, respectivamente, a través de los conjuntos $\mathcal{N} = \{0, \ldots, N-1\}$ y $\mathcal{K} = \{0, \ldots, K-1\}$. Para analizar las prestaciones de QoS para servicios móviles multimedia, supondremos que el servicio ofrecido al usuario k pertenece a un perfil de QoS caracterizado por los parámetros $\{\mu_k, d_k\}$, donde μ_k y d_k representan los máximos valores permitidos de probabilidad media de pérdida de paquetes y retardo, respectivamente.

En la BS, los paquetes generados en las capas superiores de la pila de protocolos se almacenan en las K colas FIFO (*First-In First-Out*) disponibles en la capa DLC. En este trabajo, con el fin de simplificar el tratamiento algebraico del problema, supondremos paquetes de longitud fija igual a N_p bits/paquete y colas FIFO con una capacidad máxima de B paquetes/cola. Asumiremos, también, que el proceso de planificación de paquetes se organiza en tramas de duración T_0 segundos, de manera que, al principio de cada trama y en función de la CSI/QSI disponible, el planificador selecciona algunos de los paquetes contenidos en las colas para que sean transmitidos a través del sistema OFDM, que incluirá los procesos de asignación adaptativa de potencias y subportadoras, modulación y codificación adaptativa, procesado MIMO, IFFT (*Inverse Fast Fourier Transform*) e inserción del intérvalo de guarda o prefijo cíclico.

II-A. Modelización de la capa PHY

La tecnología MIMO proporciona una gran variedad de técnicas que permiten explotar la presencia de múltiples caminos de propagación entre las N_T antenas transmisoras y las N_R antenas receptoras. Concretamente, cuando se dispone de información ideal sobre el estado del canal en transmisión (CSIT - *Channel State Information at the Transmitter*) y no se utiliza multiplexación en el dominio espacial, la estrategia MRT (*Maximum Ratio Transmission*) [6] proporciona prestaciones óptimas, en el sentido de que maximiza la relación señal a ruido (SNR - *Signal to Noise Ratio*) a la entrada del detector.

[1]En general, una estación base dispone de N_{FFT} subportadoras y esta es la dimensión de las transformadas de Fourier discretas (IFFT/FFT) que se llevan a cabo en emisión y recepción. Algunas de estas subportadoras no se utilizan y constituyen las denominadas bandas de guarda del sistema, otras subportadoras se utilizan para transmitir pilotos que permiten, entre otras cosas, llevar a cabo la estimación del canal en recepción, finalmente, las subportadoras restantes se utilizan para transmitir datos, son las denominadas subportadoras útiles.

Supongamos que al usuario k se le asigna la subportadora n y que la estación base utiliza un esquema MRT para explotar la diversidad espacial del canal MIMO. El canal de propagación entre la estación base y el usuario k se caracteriza por un perfil de retardo de potencia (*power delay profile*) [7]

$$S_k(\tau) = \sum_{l=0}^{L_p-1} \sigma_{k,l}^2 \delta(\tau - \tau_l), \tag{1}$$

donde L_p representa el número de caminos de propagación independientes, y $\sigma_{k,l}^2$ y τ_l son, respectivamente, la potencia y el retardo correspondientes al camino de propagación l-ésimo[2]. Así pues, suponiendo que el tiempo de coherencia del canal es mayor que T_0, la respuesta impulsional del canal entre la antena n_T de la BS y la antena receptora n_R del usuario k en el período de trama t puede expresarse como

$$h_{k,t}^{n_T,n_R}(\tau) = \sum_{l=0}^{L_p-1} g_{k,t,l}^{n_T,n_R} \delta(\tau - \tau_l), \tag{2}$$

donde $\mathbb{E}\{|g_{k,t,l}^{n_T,n_R}|^2\} = \sigma_{k,l}^2$. La respuesta frecuencial del canal, cuando se evalúa sobre la subportadora n, proporciona la ganancia compleja, en el dominio frecuencial,

$$H_{k,n,t}^{n_T,n_R} = \sum_{l=0}^{L_p-1} g_{k,t,l}^{n_T,n_R} e^{-j2\pi f_n \tau_l}. \tag{3}$$

Así pues, en el período de trama t, el canal entre la BS y el usuario k, correspondiente a la subportadora n, estará totalmente caracterizado a través de la matriz

$$\boldsymbol{H}_{k,n,t} = \left[H_{k,n,t}^{n_T,n_R}\right] \in \mathbb{C}^{N_R \times N_T}. \tag{4}$$

En el receptor, si se supone, como resulta habitual, que los procesos de sincronización y muestreo son ideales y que la duración del prefijo cíclico es mayor que la duración máxima de la respuesta impulsional del canal, el vector de muestras de señal recibidas en las N_R antenas receptoras correspondiente al usuario k sobre la subportadora n durante un período de señalización arbitrario de la trama t puede expresarse como

$$\boldsymbol{y}_{k,n,t} = \sqrt{p_{k,n,t}}\ \boldsymbol{H}_{k,n,t}\boldsymbol{v}_{k,n,t}z_{k,n,t} + \boldsymbol{\nu}_{k,n,t} \in \mathbb{C}^{N_R \times 1}, \tag{5}$$

donde $p_{k,n,t}$ es la potencia asignada al usuario k sobre la subportadora n durante la trama t, $\boldsymbol{v}_{k,n,t} \in \mathbb{C}^{N_T \times 1}$ representa el filtro lineal utilizado en el transmisor, $z_{k,n,t}$ es el símbolo transmitido por el usuario k sobre la subportadora n en un período de señalización arbitrario de la trama t, obtenido a partir de una constelación compleja $\mathcal{A}$ cuya energía media es $\mathbb{E}\{|z_{k,n}|^2\} = 1$, y $\boldsymbol{\nu}_{k,n,t} \in \mathbb{C}^{N_R \times 1}$ es un vector de muestras de ruido Gaussiano blanco aditivo (AWGN - *Additive White Gaussian Noise*) de media cero y matriz de varianza $E\{\boldsymbol{\nu}_{k,n,t}\boldsymbol{\nu}_{k,n,t}^H\} = \sigma_\nu^2 \boldsymbol{I}_{N_R}$.

Cuando se dispone de CSI ideal tanto en el transmisor como en el receptor, el filtro de transmisión $\boldsymbol{v}_{k,n,t}$ que maximiza la SNR en el receptor coincide con el vector singular derecho $\boldsymbol{u}_{k,n,t}$ de la matriz $\boldsymbol{H}_{k,n,t}$ asociado a su valor singular máximo, identificado como $\sigma_{\text{máx}}(\boldsymbol{H}_{k,n,t})$. En este caso, la

[2]Con el objetivo de simplificar esta presentación, y sin pérdida de generalidad, se supone que los parámetros L_p y $\{\tau_l\}_{l=0}^{L_p-1}$ son independientes del usuario k.

combinación MRC de las N_R muestras de señal recibidas proporciona

$$\begin{aligned}\tilde{z}_{k,n} &= \boldsymbol{u}_{k,n,t}^H \boldsymbol{H}_{k,n,t}^H \boldsymbol{y}_{k,n,t} \\ &= \sqrt{p_{k,n,t}}\ \boldsymbol{u}_{k,n,t}^H \boldsymbol{H}_{k,n,t}^H \left(\boldsymbol{H}_{k,n,t}\boldsymbol{u}_{k,n,t} z_{k,n} + \boldsymbol{\nu}_{k,n,t}\right).\end{aligned} \tag{6}$$

Así pues, la SNR instantánea del esquema MRT con CSI ideal para el usuario k sobre la subportadora n durante la trama t puede expresarse como

$$\gamma_{k,n,t} = \frac{p_{k,n,t}\delta_{k,n,t}}{\sigma_\nu^2}, \tag{7}$$

donde $\delta_{k,n,t} = \sigma^2_{\text{máx}}(\boldsymbol{H}_{k,n,t})$.

II-B. Modelización de la capa DLC

Para caracterizar el comportamiento de las colas de paquetes en la capa de control del enlace de datos utilizaremos una versión ligeramente modificada del modelo propuesto por Kong *et al.* en [2, Sección IV.A]. Supongamos que al inicio de la trama t el tamaño de la cola del usuario k es $Q_{k,t}$ y que el número de paquetes que deben ser eliminados de la cola debido a que su retardo ha superado el límite máximo permitido es igual a $\pi_{k,t}$. El planificador de paquetes, de acuerdo con la CSI/QSI disponible y suponiendo que quiere evitar una provisión de servicio superior a la cantidad de información contenida en la cola, proporcionará servicio al usuario k con una tasa de transmisión de $r_{k,t}$ bits/segundo que deberá satisfacer la condición

$$r_{k,t} \leq \frac{[Q_{k,t} - \pi_{k,t}]N_p}{T_0} \triangleq r_{k,t}^{\max}. \tag{8}$$

Si el proceso de llegadas introduce $\nu_{k,t}$ nuevos paquetes en la cola durante el período de trama t, la longitud de la cola al final de esta trama, sin tener en cuenta su capacidad máxima, podrá expresarse como

$$U_{k,t+1} = Q_{k,t} - \pi_{k,t} - \frac{r_{k,t}\ T_0}{N_p} + \nu_{k,t}. \tag{9}$$

Así pues, si se toma en consideración su capacidad máxima, el tamaño de la cola del usuario k al inicio de la trama $t+1$ será

$$Q_{k,t+1} = \text{mín}\left\{B, U_{k,t+1}\right\} \tag{10}$$

y, por tanto, el número de paquetes eliminados por desbordamiento (*overflow*) de la cola al final de la trama t será

$$D_{k,t+1} = \text{máx}\left\{0, U_{k,t+1} - B\right\}. \tag{11}$$

A partir de este modelo analizaremos el valor medio de la probabilidad de pérdida de paquetes y el valor medio del retardo de transmisión por paquete. Las posibles causas de la pérdida de paquetes son el *overflow* o desbordamiento de la cola y la superación del retardo máximo permitido. Sin tener en cuenta el límite de las colas, la longitud media de la cola al final de la trama t, promediada sobre una ventana de duración t_c, puede calcularse como

$$\overline{U_{k,t+1}} = \left(1 - \frac{1}{t_c}\right)\ \overline{U_{k,t}} + \frac{1}{t_c}\ U_{k,t+1}. \tag{12}$$

En consecuencia, al inicio de la trama t, conocidas $\overline{U_{k,t}}$ y $Q_{k,t}$, el número de paquetes eliminados $\pi_{k,t}$ por exceder el retardo máximo permitido y la tasa media de llegada paquetes $\text{E}\{\nu_{k,t}\}$, la predicción de la longitud media de la cola, sin tener en cuenta su capacidad máxima, sobre la ventana de promediado t_c, podrá expresarse como

$$\begin{aligned}\hat{U}_{k,t+1} &= \text{E}_{\nu_{k,t}}\left\{\overline{U_{k,t+1}}\right\} \\ &= \left(1 - \frac{1}{t_c}\right)\ \overline{U_{k,t}} \\ &\quad + \frac{Q_{k,t} - \frac{r_{k,t}\cdot T_0}{N_p} + \text{E}\{\nu_{k,t}\} - \pi_{k,t}}{t_c} \\ &\triangleq \text{L}\left(r_{k,t}\right)\end{aligned} \tag{13}$$

donde $\text{E}_{\nu_{k,t}}\{\cdot\}$ representa el operador esperanza matemática respecto a $\nu_{k,t}$, que puede obtenerse a partir de las características estadísticas del tráfico entrante. Como puede observarse, $\hat{U}_{k,t+1}$ es una función que depende de la tasa de transmisión $r_{k,t}$ que el planificador de paquetes asigna al usuario k. Así pues, a partir de la tasa $r_{k,t}$, la predicción del valor medio de paquetes eliminados por desbordamiento de la cola al final de la trama t será

$$\hat{D}_{k,t+1} = \text{máx}\left\{0, \text{L}\left(r_{k,t}\right) - B\right\} \triangleq \text{F}\left(r_{k,t}\right). \tag{14}$$

Así, pues, si se quiere cumplir con el requisito de QoS μ_k impuesto sobre la probabilidad de pérdida de paquetes, la estimación $\hat{\mu}_{k,t+1}$ del valor medio de la PDP al final de la trama t deberá cumplir

$$\hat{\mu}_{k,t+1} = \frac{\text{F}\left(r_{k,t}\right) + \overline{\pi_{k,t}}}{\text{E}\{\nu_{k,t}\}} \leq \mu_k, \tag{15}$$

donde

$$\overline{\pi_{k,t+1}} = \left(1 - \frac{1}{t_c}\right)\ \overline{\pi_{k,t}} + \frac{1}{t_c}\ \pi_{k,t+1}. \tag{16}$$

Dado que $\text{F}\left(r_{k,t}\right) - \overline{\pi_{k,t}}$ es una función no creciente de $r_{k,t}$, la tasa de transmisión del usuario k deberá cumplir

$$r_{k,t} \geq \text{F}^{-1}\left(\text{E}\{\nu_{k,t}\} \cdot \mu_k - \overline{\pi_{k,t}}\right) \triangleq \alpha_{k,t}, \tag{17}$$

donde $\alpha_{k,t}$ representaría la tasa de transmisión mínima necesaria para cumplir con el requisito de QoS correspondiente a la probabilidad de pérdida de paquetes.

A continuación se realiza un análisis similar para la restricción de QoS asociada al retardo. El retardo medio por paquete en una cola puede expresarse a partir de la fórmula de Little [8] como

$$\hat{d}_{k,t+1} = \frac{\hat{Q}_{k,t+1}}{\text{E}\{\nu_{k,t} - D_{k,t+1}\}} \tag{18}$$

donde $\hat{Q}_{k,t+1}$ es la estimación de la longitud de la cola al final del de la trama t, es decir,

$$\hat{Q}_{k,t+1} = \text{mín}\left\{B, \text{L}\left(r_{k,t}\right)\right\} \triangleq \text{G}\left(r_{k,t}\right) \tag{19}$$

Nuevamente, $\text{G}\left(r_{k,t}\right)$ es una función no creciente de $r_{k,t}$ y, por tanto, para cumplir con el requisito de QoS d_k impuesto sobre el retardo de transmisión medio de un paquete, deberá cumplirse

$$\hat{d}_{k,t+1} = \frac{\text{G}\left(r_{k,t}\right)}{\text{E}\{\nu_{k,t} - D_{k,t+1}\}} \leq d_k \tag{20}$$

o, de forma equivalente,

$$r_{k,t} \geq \text{G}^{-1}(\text{E}\{\nu_{k,t} - D_{k,t+1}\}\ d_k) = \beta_{k,t}, \tag{21}$$

donde $\beta_{k,t}$ representaría la tasa de transmisión mínima necesaria para cumplir con el requisito de QoS referente al retardo de transmisión medio por paquete.

En definitiva, combinando (17) y (21), es decir,

$$r_{k,t} \geq \text{máx}\{\alpha_{k,t}, \beta_{k,t}\} = r_{k,t}^{\min}, \tag{22}$$

se garantiza que el sistema cumple las restricciones de QoS impuestas sobre el servicio ofrecido al usuario k.

En las secciones que se presentan a continuación, se utilizará la notación $\boldsymbol{R}_t^{\min}$ y $\boldsymbol{R}_t^{\max}$ para representar los vectores cuyas componentes k-ésimas son los valores $r_{k,t}^{\min}$ y $r_{k,t}^{\max}$ calculados anteriormente.

III. Variables de optimización

III-A. Asignación de potencias

Dado el vector de potencias del usuario k sobre la subportadora n durante la trama t, definido como

$$\boldsymbol{p}_{n,t} = \left[p_{0,n,t} \cdots p_{K-1,n,t}\right]^T, \tag{23}$$

el algoritmo de asignación de potencias, fijadas las restricciones del sistema, deberá determinar el vector

$$\boldsymbol{p}_t = \left[\left(\boldsymbol{p}_{0,t}\right)^T \cdots \left(\boldsymbol{p}_{N-1,t}\right)^T\right]^T \tag{24}$$

que optimice la función objetivo. Además de asignar potencias, los algoritmos de asignación de recursos también deberán asignar subportadoras y tasas de transmisión. De todas formas, como se verá a continuación, el vector de potencias $\boldsymbol{p}_t$ también puede utilizarse para representar la asignación de los otros recursos del sistema, simplificando la formulación del problema de optimización [9].

III-B. Asignación de subportadoras

Aunque en sistemas OFDMA es posible que una subportadora sea compartida por múltiples usuarios, Jang *et al.* [10] demostraron que la asignación exclusiva de las subportadoras del sistema proporciona mejores prestaciones. En un sistema OFDMA en que las subportadoras se asignan de forma exclusiva a los distintos usuarios del sistema, el vector de potencias puede utilizarse para capturar los efectos de esta asignación si se utiliza la siguiente restricción

$$\begin{aligned}\boldsymbol{p}_{n,t} \in \boldsymbol{\mathcal{P}}_n = \{&\boldsymbol{p}_{n,t} \in \mathbb{R}_+^K \,:\, p_{k,n,t}\; p_{k',n,t} = 0; \\ &\forall\; k \neq k';\; k, k' \in \mathcal{K}\}.\end{aligned} \tag{25}$$

En este caso, el vector de asignación de potencias será

$$\boldsymbol{p}_t \in \boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{P}}_0 \times \cdots \times \boldsymbol{\mathcal{P}}_{N-1} \subset \mathbb{R}_+^{KN}. \tag{26}$$

donde $\boldsymbol{\mathcal{P}}$ representa el espacio de vectores de potencia permisibles para todas las subportadoras del sistema.

III-C. Asignación de tasas de transmisión

El presente estudio, sin perdida de generalidad, únicamente considera tasas de transmisión continuas. La extensión al análisis de sistemas que utilicen tasas de transmisión discretas puede llevarse a cabo de forma relativamente sencilla utilizando la metodología introducida en [11]. La teoría de la información de Shannon nos permite calcular la máxima tasa de transmisión (capacidad del canal), expresada en bits por segundo, para el usuario k sobre la subportadora n y la trama t, a partir de la expresión

$$\begin{aligned}R_{k,n,t}\left(p_{k,n,t}, \delta_{k,n,t}\right) &= \Delta f \log_2\left(1 + \gamma_{k,n,t}\right) \\ &= \Delta f \log_2\left(1 + \frac{p_{k,n,t}\delta_{k,n,t}}{\sigma_\nu^2}\right),\end{aligned} \tag{27}$$

donde Δ_f representa el ancho de banda ocupado por una subportadora. Así, si se dispusiera de sistemas de codificación de canal y modulación digital que permitieran obtener tasas de transmisión continuas idénticas a la capacidad del canal, la potencia de transmisión $p_{k,n,t}$ determinaría de forma unívoca la asignación de la tasa de transmisión del sistema. Nótese que $r_{k,t} = \sum_{n=0}^{N-1} R_{k,n,t}$ es la tasa de transmisión asignada al usuario k en la trama t y que, por tanto, $\boldsymbol{R}_t \triangleq \left[r_{0,t} \cdots r_{K-1,t}\right]^T$ es un vector que agrupa las tasas de transmisión asignadas a todos los usuarios del sistema en el período de trama t.

IV. Formulación del Problema

IV-A. Problema de optimización

Teniendo en cuenta el modelo de colas desarrollado en la sección II-B y suponiendo que al inicio de cada trama OFDMA se dispone de la CSI obtenida en la capa PHY y de la QSI obtenida en la capa DLC, el problema de programación matemática que persigue maximizar la suma total de las tasas de transmisión de los usuarios del sistema (véanse, por ejemplo, las referencias [12], [1], [9]), con restricciones sobre la potencia total transmitida, sobre la probabilidad media de pérdida de paquetes y sobre el retardo de transmisión por paquete, puede formularse como

$$\begin{aligned}&\max_{\boldsymbol{p}_t \in \boldsymbol{\mathcal{P}}} \sum_{k=0}^{K-1}\sum_{n=0}^{N-1} R_{k,n,t}\left(p_{k,n,t}, \delta_{k,n,t}\right) \\ &\text{s.t.} \quad \sum_{k=0}^{K-1}\sum_{n=0}^{N-1} p_{k,n,t} \leq P_T \\ &\qquad r_{k,t} \leq \frac{[Q_{k,t} - \pi_{k,t}]N_p}{T_0} = r_{k,t}^{\max},\ \forall k \in \mathcal{K} \\ &\qquad r_{k,t} \geq \text{máx}\{\alpha_{k,t}, \beta_{k,t}\} = r_{k,t}^{\min},\ \forall k \in \mathcal{K},\end{aligned} \tag{28}$$

donde P_T es la potencia de transmisión máxima disponible en la estación base.

IV-B. Problema dual lagrangiano

Al abordar este problema de optimización utilizando principios de dualidad [4], la función Lagrangiana del problema (28) puede expresarse como

$$\begin{aligned}\mathcal{L}\left(\boldsymbol{p}_t, \lambda, \boldsymbol{\varphi}, \boldsymbol{\phi}\right) = &\sum_{k=0}^{K-1}\sum_{n=0}^{N-1} R_{k,n,t}\left(p_{k,n,t}, \alpha_{k,n,t}\right) \\ &+ \lambda\left(P_T - \sum_{k=0}^{K-1}\sum_{n=0}^{N-1} p_{k,n,t}\right) \\ &+ \sum_{k=0}^{K-1} \varphi_k\left(r_{k,t}^{\max} - r_{k,t}\right) \\ &+ \sum_{k=0}^{K-1} \phi_k\left(r_{k,t} - r_{k,t}^{\min}\right),\end{aligned} \tag{29}$$

$$g(\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}) = \min_{\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}\geq 0}\left\{\max_{\boldsymbol{p}_t\in\boldsymbol{\mathcal{P}}}\mathcal{L}\left(\boldsymbol{p}_t,\lambda\right)\right\} \tag{30a}$$

$$= \min_{\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}\geq 0}\left\{\max_{p_{k,n,t}\geq 0}\left[\sum_{k=0}^{K-1}\sum_{n=0}^{N-1}\left(R_{k,n,t}-\lambda p_{k,n,t}\right)+\lambda P_T+\sum_{k=0}^{K-1}\varphi_k\left(r_{k,t}^{\max}-r_{k,t}\right)+\sum_{k=0}^{K-1}\phi_k\left(r_{k,t}-r_{k,t}^{\min}\right)\right]\right\} \tag{30b}$$

$$= \min_{\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}\geq 0}\left\{\sum_{n=0}^{N-1}\max_{k\in\boldsymbol{\mathcal{K}}}\left\{\max_{p_{k,n,t}\geq 0}\left((1-\varphi_k+\phi_k)R_{k,n,t}-\lambda p_{k,n,t}\right)\right\}+\lambda P_T+\sum_{k=0}^{K-1}\left(\varphi_k r_{k,t}^{\max}-\phi_k r_{k,t}^{\min}\right)\right\} \tag{30c}$$

$$= \min_{\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}\geq 0}\left\{\sum_{n=0}^{N-1}\max_{k\in\boldsymbol{\mathcal{K}}}\left[\max_{p_{k,n,t}\geq 0}\left((1-\varphi_k+\phi_k)R_{k,n,t}\left(\wp_{k,n,t}(\lambda),\delta_{k,n,t}\right)-\lambda\wp_{k,n,t}\right)\right]+\lambda P_T+\sum_{k=0}^{K-1}\left(\varphi_k r_{k,t}^{\max}-\phi_k r_{k,t}^{\min}\right)\right\}. \tag{30d}$$

donde $\lambda\in\mathbb{R}_+$, $\boldsymbol{\varphi}\in\mathbb{R}_+^K$ y $\boldsymbol{\phi}\in\mathbb{R}_+^K$ son los denominados coeficientes de Lagrange o variables duales y, por tanto, el problema de optimización dual puede formularse tal como aparece en (30), al principio de esta página.

El problema de optimización dual (30a) puede simplificarse si se tiene en cuenta la restricción de asignación exclusiva de subportadoras y el hecho de que las variables de potencia son separables entre subportadoras (30c). Nótese que $r_{k,t}=\sum_{n=1}^{N}R_{k,n,t}$ y, por tanto, si se utiliza la definición (27), la maximización del término interior de la expresión (30c) da como resultado una expresión analítica cerrada conocida como *water-filling* multinivel que nos permite expresar la asignación de potencia óptima del usuario k para la subportadora n y la trama t como

$$\wp_{k,n,t}(\lambda,\phi_k,\varphi_k)=\left[\Delta f\frac{1+\phi_k-\varphi_k}{\lambda\ln 2}-\frac{\sigma_\nu^2}{\delta_{k,n,t}}\right]^+, \tag{31}$$

donde $[x]^+=\max(0,x)$. A continuación, sustituyendo (31) en (30c) el problema dual queda simplificado a la expresión (30d). Así, la política óptima consiste en la asignación de la subportadora $n\in\boldsymbol{\mathcal{N}}$ al usuario $k\in\boldsymbol{\mathcal{K}}$ que maximiza el término $(1-\varphi_k+\phi_k)\,R_{k,n,t}\left(\wp_{k,n,t}(\lambda),\delta_{k,n,t}\right)-\lambda\wp_{k,n,t}(\lambda)$.

Utilizando propiedades estándar de la optimización dual (véase [4]) puede demostrarse que la función objetivo para el problema dual es convexa respecto a $\lambda,\boldsymbol{\varphi},\boldsymbol{\phi}$ y, por tanto, pueden utilizarse métodos de búsqueda multidimensional como, por ejemplo, el método del subgradiente, para determinar las variables duales λ^*, $\boldsymbol{\varphi}^*$ y $\boldsymbol{\phi}^*$ que optimizan el *throughput* global del sistema. Una vez hallados los valores óptimos, se usan éstos en las funciones de optimización para obtener las asignaciones de usuario (32) y potencia (33) de cada subportadora del sistema, es decir,

$$k_n^*=\arg\max_{k\in\boldsymbol{\mathcal{K}}}\left\{(1-\varphi_k^*+\phi_k^*)\,R_{k,n,t}\left(\wp_{k,n,t}\right)-\lambda^*\wp_{k,n,t}\right\} \tag{32}$$

$$p_{k,n,t}=\begin{cases}\wp_{k,n,t} & ,\ k=k_n^*\\ 0 & ,\ \text{en caso contrario.}\end{cases} \tag{33}$$

IV-C. Método del subgradiente

Debido a que la función objetivo (29) no es diferenciable en todos sus puntos, no pueden utilizarse algoritmos de búsqueda basados en el gradiente. Así pues, en este trabajo proponemos la utilización del método del subgradiente [5] para solucionar el problema de optimización. Dicho método permite realizar una búsqueda iterativa utilizando los subgradientes como direcciones de búsqueda. A partir de los valores iniciales $\lambda^0,\boldsymbol{\varphi}^0,\boldsymbol{\phi}^0$, se realiza la siguiente actualización en cada iteración

$$\lambda^{i+1}=\left[\lambda^i-s_\lambda^i g_\lambda^i\right]^+,\quad g_\lambda^i=P_T-\sum_k\sum_n p_{k,n,t} \tag{34a}$$

$$\boldsymbol{\varphi}^{i+1}=\left[\boldsymbol{\varphi}^i-s_\varphi^i\boldsymbol{g}_\varphi^i\right]^+,\quad \boldsymbol{g}_\varphi^i=\boldsymbol{R}_t^{\max}-\boldsymbol{R}_t^i \tag{34b}$$

$$\boldsymbol{\phi}^{i+1}=\left[\boldsymbol{\phi}^i-s_\phi^i\boldsymbol{g}_\phi^i\right]^+,\quad \boldsymbol{g}_\phi^i=\boldsymbol{R}_t^i-\boldsymbol{R}_t^{\min}, \tag{34c}$$

donde s_λ^i, s_φ^i y s_ϕ^i son los denominados *step-sizes* o *longitudes de salto* [5].

Cuadro I
PARÁMETROS DE SIMULACIÓN DEL SISTEMA

Parámetro	Valor
Frecuencia (f_0)	5,25 GHz
Ancho de banda (W)	20 MHz
Número subportadoras (N)	256
Período de símbolo OFDM	16 μs
Período de trama OFDMA (T_0)	1,6 ms
Máxima frecuencia Doppler	30 Hz
Potencia disponible (P_{T})	0,1 W
Longitud paquete (N_p)	100 bit/paquete
Longitud cola (B)	200
Ventana promediado (t_c)	$10\cdot T_0$
Modelo de canal	Kermoal *et al.* [13]
SNR media ($\bar{\gamma}$)	0 dB

Cuadro II
REQUISITOS DE QOS PARA LAS FUENTES DE TRÁFICO

Parámetro	Valor
Retardo máximo para tráfico de datos	16 ms
PDP máxima para tráfico de datos	1 %
Retardo máximo para tráfico de voz,	10 ms
PDP máxima para tráfico de voz	1 %

V. RESULTADOS NUMÉRICOS

V-A. Parámetros de simulación

Sin pérdida de generalidad, se ha considerado un sistema MIMO-OFDMA cuyos parámetros de funcionamiento (ver Cuadro I) son similares a los propuestos por Kong *et al.* [2]. Para validar el sistema se ha implementado un simulador MATLAB. El ancho de banda global del sistema es de 20 MHz centrados en una frecuencia portadora $f_0=5{,}25$ GHz. Esta banda frecuencial se subdivide en un total de 256 subportadoras dando lugar a un ancho de banda por subportadora de $\Delta f=78{,}125$ kHz. Así pues, suponiendo un prefijo cíclico (intérvalo de guarda) de 3.2 μs, se obtiene un

período de símbolo OFDM igual a 16 μs. Las tramas OFDMA se construyen a partir de una agrupación de 100 símbolos OFDM y, por tanto, el período de trama resultante es igual a $T_0 = 1{,}6$ ms. Para modelar la respuesta del canal MIMO se ha utilizado la herramienta generadora de canales implementada por Kermoal *et al.* [13], utilizando *arrays* lineales de antenas con una separación entre antenas transmisoras de una longitud de onda y una separación entre antenas receptoras de media longitud de onda. La estación base dispone de colas de usuario con una capacidad máxima de $B = 200$ paquetes/usuario y se suponen paquetes de longitud fija $N_p = 100$ bits/paquete.

Se han considerado diferentes fuentes de tráfico, que incluyen datos y voz, cuyos parámetros aparecen representados en el Cuadro II). El tráfico de datos se modela a través de un proceso de llegadas Markoviano discreto por lotes (DBMAP - *Discrete Batch Markovian Arrival Process*) como el utilizado por Femenias *et al.* en [14] con $\mathcal{A} = 15$ estados y una tasa media de llegada de paquetes $\bar{\lambda} = 12$ paquetes/trama. El tráfico de voz se genera utilizando un modelo ON-OFF de dos estados en que el período ON tiene una duración media de 1 segundo y la del período OFF es igual a 1.35 segundos. Durante el período ON, los paquetes se generan a una tasa de 1 paquete/trama. Los requerimientos de QoS para cada tipo de tráfico aparecen en el Cuadro II.

Utilizaremos este modelo de sistema para comparar las prestaciones obtenidas por el sistema de optimización inter-capas, que utiliza la CSI obtenida por la capa PHY y la QSI aportada por la capa DLC, con las prestaciones obtenidas por el sistema de obtimización que únicamente utiliza CSI. A partir de este momento estos sistemas se etiquetarán como OFDMA-CSI/QSI y OFDMA-CSI, respectivamente. En la implementación del método del subgradiente se ha utilizado un *step-size* de tipo decreciente, es decir,

$$s^i = \frac{a}{b+i}, \quad a, b \in \mathbb{R}_+, \quad \sum_{i=1}^{\infty} (s^i)^2 < \infty, \quad \sum_{i=1}^{\infty} s^i = 0,$$

que garantiza la convergencia del mismo [5]. Debido a la diferencia en los órdenes de magnitud de las diferentes variables de optimización, sus respectivos coeficientes de Lagrange (λ, ϕ, φ), tendrán una parametrización propia de las constantes a y b.

V-B. Sistema con tráfico de datos homogéneo

La Fig. 1 muestra el *throughput* medio global del sistema para los sistemas OFDMA-CSI/QSI y OFDMA-CSI, suponiendo la utilización de sistemas MIMO con $N_T = 2$ y $N_R = 1$. El *throughput* medio del sistema se define como la tasa de información útil transmitida en bits por segundo. Para escenarios en que el número de usuarios es bajo, la capacidad global del canal de transmisión es muy superior a la tasa de información generada por los usuarios y, por tanto, ambos sistemas presentan un *throughput* medio que aumenta linealmente en función de K y no se aprecian diferencias en su comportamiento. Sin embargo, para valores elevados del número de usuarios, la tasa de transmisión global puede superar la capacidad global del sistema y pueden apreciarse diferencias significativas en el comportamiento de los sistemas OFDMA-CSI/QSI y OFDMA-CSI. El sistema OFDMA-CSI, al no utilizar información sobre el estado de las colas y asignar recursos teniendo en cuenta únicamente la CSI, puede estar asignando potencia, ancho de banda y tasa de transmisión muy superiores a la demanda real de los usuarios que están sometidos a condiciones de propagación favorables, en detrimento de usuarios que, disponiendo de una demanda real de recursos, están sometidos a condiciones de propagación poco favorables. A medio/largo plazo y a medida que aumenta el número de usuarios del sistema y se incrementa la tasa de llegada de paquetes a las colas, esta estrategia provoca un aumento del número de paquetes perdidos por desbordamiento de las colas y/o por superar el retardo máximo permitido. El sistema OFDMA-CSI/QSI, en cambio, controla el cumplimiento promedio de los requerimientos de QoS y, por tanto, el número de paquetes perdidos o retardados es menor que en el sistema OFDMA-CSI y en consecuencia el *throughput* es mayor.

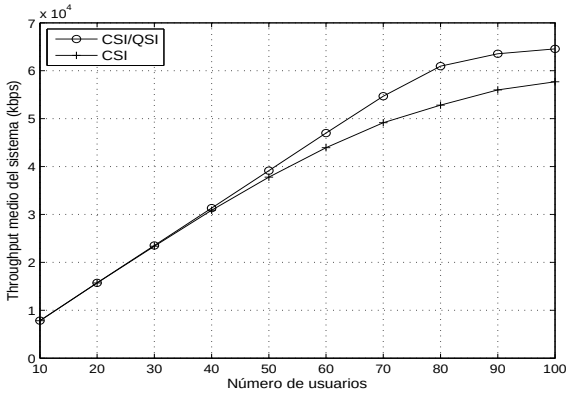


Figura 1. Throughput medio del sistema en función de K.

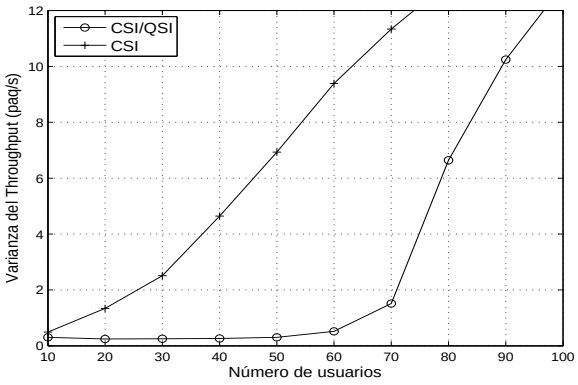


Figura 2. *Fairness* entre los diferentes usuarios del sistema.

Una buena medida del grado de equidad (*fairness*) en la asignación de recursos en un sistema en que todos los usuarios generan la misma clase de tráfico, es la varianza en el *throughput* medio de los usuarios del sistema tal y como muestra la Fig. 2. Las medidas de *throughput* se han tomado sobre una ventana de promediado de 15 tramas. Como puede observarse el sistema OFDMA-CSI que, al no llevar a cabo ningún control sobre la equidad de los algoritmos de asignación, únicamente asigna recursos a aquellos usuarios sometidos a unas condiciones de canal favorables y obvía al resto, presenta una varianza del *throughput* superior a la

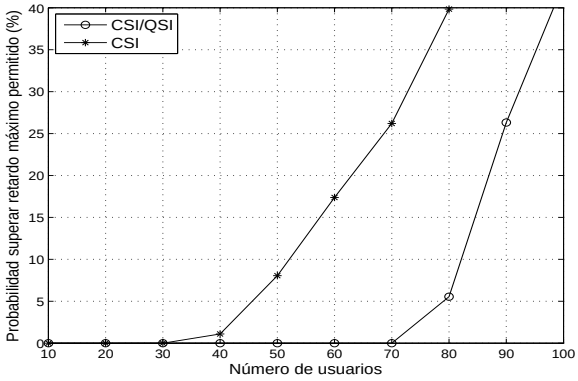


Figura 3. Probabilidad de exceder el retardo medio máximo permitido d_k.

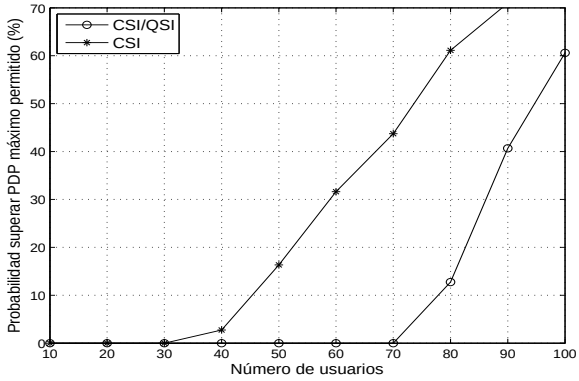


Figura 4. Probabilidad de exceder la PDP media máxima permitida μ_k.

del sistema OFDMA-CSI/QSI. El sistema OFDMA-CSI/QSI controla la equidad y es capaz, para un número de usuarios del sistema $K < 70$, de ceder de forma adaptativa recursos de transmisión de usuarios con un nivel de satisfacción elevado, en términos de QoS, a usuarios con un nivel de satisfacción menor. Para un número de usuarios del sistema $K > 70$, incluso el sistema OFDMA-CSI/QSI empieza a tener dificultades para mantener la equidad entre usuarios.

Las Fig. 3 y 4 muestran las prestaciones del sistema en cuanto a la probabilidad de incumplimiento de los requerimientos de QoS impuestos. Así, la Fig. 3 muestra la probabilidad de violación de la restricción impuesta sobre al retardo máximo, mientras que la Fig. 4 muestra la probabilidad de violación de la restricción sobre la máxima PDP permitida. Cada vez que el retardo medio calculado al finalizar una trama supera el requerimiento especificado (d_k o μ_k) se contabiliza un incumplimiento y las probabilidades de violación se calculan como el cociente entre el número de violaciones de retardo o PDP sobre todas las tramas OFDMA y para todos los usuarios y el número total de ocasiones en que se han calculado el retardo promedio y la PDP para estos usuarios. De nuevo, puede observarse como el sistema propuesto mejora las prestaciones del sistema sin restricciones. De hecho, para este modelo de sistema, el esquema OFDMA-CSI podría proporcionar servicio con ciertas garantías de QoS a un número máximo de usuarios $K \simeq 30$, mientras que el esquema OFDMA-CSI/QSI podría proporcionarlo a un número máximo de usuarios $K \simeq 70$. Óbviamente, ambos esquemas de asignación de recursos deberán actuar conjuntamente con un algoritmo de control de admisión de llamadas, con el fin de garantizar que la llegada de nuevos usuarios no comprometa las garantías de QoS de los usuarios que ya han sido admitidos al sistema.

V-C. Efectos de la configuración MIMO

La máxima tasa de transmisión (capacidad del canal) que garantiza una tranmisión fiable para un usuario k sobre una portadora n y una trama t está determinada por la ecuación (27), que presenta una dependencia directa de la SNR instantánea (7) del esquema MRT con CSI ideal. Esta SNR depende del valor singular máximo de la matriz $\boldsymbol{H}_{k,n,t}$, identificado como $\sigma_{\text{máx}}(\boldsymbol{H}_{k,n,t})$, cuyo valor aumenta (estadísticamente) a medida que se incrementa el número de antenas transmisoras y/o receptoras de la infraestructura MIMO utilizada en la capa PHY. Así pués, al utilizar estructuras MIMO con un mayor número de antenas aumenta la capacidad de transmisión del sistema OFDMA y por tanto, si disponemos de un algoritmo de asignación de recursos capaz de explotar de forma eficiente este incremento de la capacidad, permitirá proporcionar servicio a un mayor número de usuarios con garantías de cumplimiento de las restricciones de QoS. Este fenómeno puede observarse claramente en los resultados presentados en las Figs. 5 y 6, para estructuras MIMO con $N_T = 4$ y $N_R =$1, 2 y 4. A medida que aumenta el número de antenas receptoras[3], el incremento de capacidad de la capa PHY permite obtener incrementos del *throughput* medio global del sistema. El aumento del número de antenas también se traduce en una disminución de las probabilidades de violación de las restricciones de retardo y de PDP, permitiendo que los esquemas OFDMA-CSI y OFDMA-CSI/QSI puedan proporcionar servicio con ciertas garantías de QoS a un número máximo de usuarios K que varía desde 25 a 40 y desde 80 a más de 110, respectivamente, al pasar de una configuración MIMO 4×1 a una configuración 4×4.

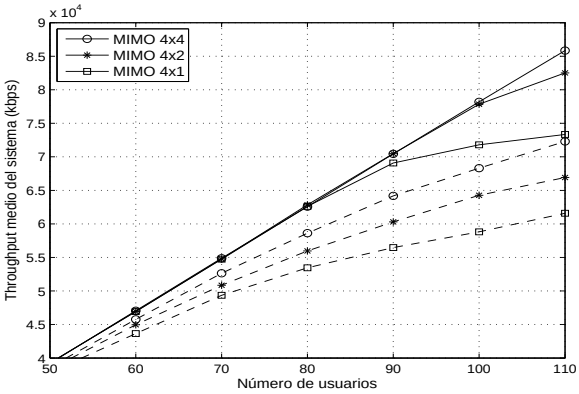


Figura 5. Throughput medio para diferentes configuraciones MIMO.

V-D. Sistema con tráfico heterogéneo

Para mostrar el comportamiento de los esquemas de asignación de recursos OFDMA-CSI y OFDMA-CSI/QSI en

[3]Excepto por los diferentes efectos de la correlación entre antenas en la estación base y las estaciones móviles, se obtienen resultados similares cuando se aumenta el número de antenas transmisoras.

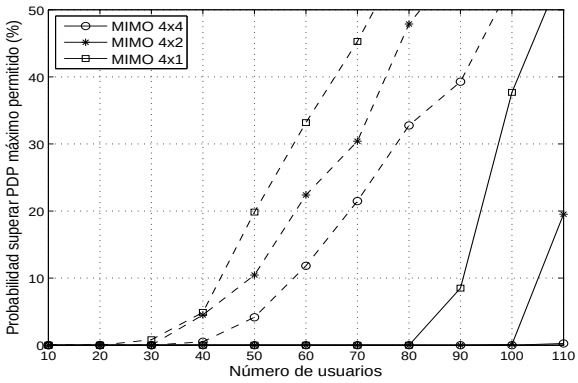


Figura 6. Probabilidad de violación de la PDP.

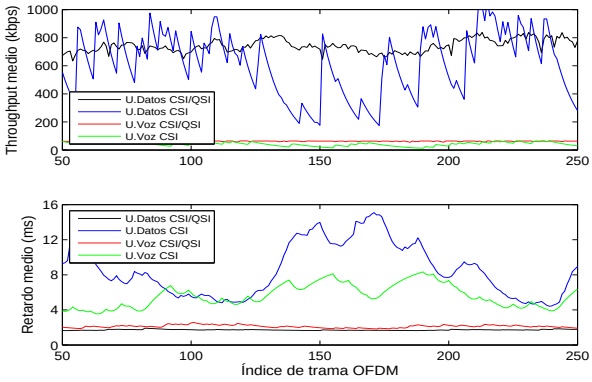


Figura 7. *Throughput* y retardo medio para tráfico heterogéneo.

entornos con tráfico heterogéneo, se ha simulado un sistema en el que se transmiten idéntico número de flujos de tráfico de datos y de voz. En la Fig. 7 se muestra una traza de los resultados obtenidos para dos flujos concretos, uno de datos y el otro de voz, en un sistema con $K = 80$ usuarios y que utiliza una configuración MIMO 2×1. Como puede observarse, dado que el esquema OFDMA-CSI/QSI controla el cumplimiento promedio de los requerimientos de QoS, es capaz de proporcionar, para los flujos de datos y voz, un *throughput* medio (sobre una ventana de promediado de 10 tramas) que se mantiene estable alrededor del valor de la tasa de generación de información de las fuentes de tráfico y un retardo medio por paquete (se obtienen resultados similares para la PDP) muy por debajo del límite impuesto por los requerimientos de QoS. El esquema OFDMA-CSI, en cambio, proporciona un *throughput* medio y un retardo medio por paquete que sufren variaciones importantes. De hecho, puede observarse en la figura que, cuando el usuario dispone de buenas condiciones de propagación el *throughput* (retardo) medio aumenta (disminuye) rápidamente y disminuye (aumenta) también de forma rápida cuando pasa a tener malas condiciones de propagación.

VI. Conclusiones

En este trabajo se han propuesto y analizado algoritmos para la asignación eficiente de recursos en el canal descendente de un sistema MIMO-OFDMA basado en el uso de precodificación lineal óptima en transmisión. A diferencia de la mayoría de propuestas anteriores, se ha analizado el comportamiento de las colas de paquetes en la capa DLC con el fin de llevar a cabo un proceso de asignación de recursos basado en el diseño intercapas modelado como un problema de optimización matemática. El uso conjunto del método de descomposición dual de Lagrange y el método del subgradiente han permitido simplificar el problema de optimización ofreciendo una solución global y eficaz al problema de asignación adaptativa de recursos en sistemas multiportadora. Los resultados han demostrado que el hecho de introducir el control de los requerimientos de QoS en el planteamiento general del problema, permite asignar recursos de manera equitativa y reducir las perdidas de paquetes por desbordamiento de las colas y por exceder el retardo máximo permitido, aumentando en consecuencia el *throughput* y el número total de usuarios que puede soportar el sistema con garantías de QoS.

Agradecimientos

Esta investigación ha sido financiada parcialmente por el MEC y FEDER en el marco del proyecto COSMOS (TEC2008-02422) y la Conselleria d'Innovació, Interior i Justícia del Govern de les Illes Balears en el marco del proyecto PCTIB-2005GC1-09 y una beca predoctoral (FPI07).

Referencias

[1] K. Seong, M. Mohseni, and J. M. Cioffi, "Optimal resource allocation for OFDMA downlink systems," in *Proc. International Symposium on Information Theory (ISIT)*, July 2006, pp. 1394–1398.

[2] Z. Kong, Y.-K. Kwok, and J. Wang, "A low-complexity qos-aware proportional fair multicarrier scheduling algorithm for ofdm systems," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 5, pp. 2225 –2235, jun 2009.

[3] L. M. C. Hoo, B. Halder, J. Tellado, and J. M. Cioffi, "Multiuser transmit optimization for multicarrier broadcast channels: asymptotic FDMA capacity region and algorithms," *IEEE Tran. Commun.*, vol. 52, no. 6, pp. 922–930, June 2004.

[4] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Tran. Commun.*, vol. 54, no. 7, p. 1310, 2006.

[5] S. Boyd, L. Xiao, and A. Mutapcic, "Subgradient methods," *lecture notes of EE392o, Stanford University, Autumn Quarter*, vol. 2004, 2003.

[6] T. Lo, "Maximum ratio transmission," *IEEE Transactions on Communications*, vol. 47, no. 10, pp. 1458–1461, October 1999.

[7] J. G. Proakis, *Digital Communications*, 4th ed. McGraw Hill, 2001.

[8] B. Bunday, *An introduction to queueing theory*. Hodder Arnold, 1996.

[9] I. Wong and B. Evans, *Resource allocation in multiuser multicarrier wireless systems*. Springer, 2008.

[10] J. Jang and K. B. Lee, "Transmit power adaptation for multiuser OFDM systems," *IEEE JSAC*, vol. 21, no. 2, pp. 171–178, February 2003.

[11] B. Dañobeitia, G. Femenias, and F. Riera-Palou, "Resource Allocation in MIMO-OFDMA Wireless Systems Based on Linearly Precoded Orthogonal Space-Time Block Codes," in *Proceedings of the 15th Open European Summer School and IFIP TC6. 6 Workshop on The Internet of the Future*. Springer, 2009, p. 127.

[12] Z. Shen, J. G. Andrews, and B. L. Evans, "Optimal power allocation in multiuser OFDM systems," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, December 2003, pp. 337–341.

[13] J. Kermoal, L. Schumacher, K. Pedersen, P. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE JSAC*, vol. 20, no. 6, pp. 1211–1226, 2002.

[14] G. Femenias, J. Ramis, and L. Carrasco, "Using two-dimensional markov models and the effective-capacity approach for cross-layer design in amc/arq-based wireless networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 8, pp. 4193 –4203, oct. 2009.

Localización en interiores para mejorar el rendimiento del acceso a Internet en redes WiFi con infraestructura

Domingo Marrero, Elsa Mª Macías y Alvaro Suárez
Departamento de Ingeniería Telemática
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira, 35017 Las Palmas de Gran Canaria
{dmarrero,emacias,asuarez}@dit.ulpgc.es

***Resumen*- Uno de los aspectos en los que más esfuerzos se están realizando en las redes inalámbricas IEEE 802.11 es la mejora de las prestaciones de las mismas en cuanto a la Calidad de Servicio (*QoS*, del inglés *Quality of Service*) ofrecida. Estas se materializan en una óptima calidad de la señal, mayor ancho de banda para soportar nuevos servicios, la movilidad sin cortes, etc. Bajo esta premisa y desde hace algún tiempo, hemos desarrollado una aplicación multifuncional para mejorar las prestaciones en redes inalámbricas IEEE 802.11, y sobre ella hemos ido incorporando una serie de funciones en la línea de mejorar la QoS del acceso a Internet. Concretamente esta aplicación sigue el paradigma cliente-servidor, en la que el servidor gestiona múltiples aspectos de la comunicación guiando a los terminales móviles para que éstos obtengan un mejor aprovechamiento del canal y sus limitados recursos. En este artículo presentamos las ideas y los resultados iniciales de la incorporación de la localización de terminales móviles en interiores dentro de un espacio de localización dado por los parámetros *Received Signal Strength Identifier* (*RSSI*) de distintos *Puntos de Acceso* (*PA*) y los terminales móviles, para mejorar la QoS. Los terminales móviles pueden elegir el PA más idóneo para acceder a Internet dentro de una Organización. La solución adoptada se basa en el mecanismo de aprendizaje y creación de *Base de Datos* (*BD*) previa y posterior búsqueda por comparación y aproximación. Los resultados experimentales muestran la complejidad del mecanismo de regulación de la QoS dirigido por localización.**

***Palabras Clave*- IEEE 802.11, mejora de prestaciones, Cliente-Servidor, QoS, canal inalámbrico, localización, servicios multimedia.**

I. INTRODUCCIÓN

Las redes IEEE 802.11 [1] [2] en modo infraestructura requieren un PA para que los terminales móviles conectados a él puedan acceder a la red cableada (Internet). Hoy en día, en interiores, dentro de una organización, suelen encontrarse un conjunto de PA (en algunos casos formando un *Basic Set Service* (*BSS*)) para proporcionar acceso a Internet eficientemente. Es decir, en general, la conectividad física de los terminales móviles a los PA está relativamente bien soportada con este tipo de redes. Con esto se logra que dentro de la Organización exista una cobertura inalámbrica casi completa (con buen nivel en muchos puntos) para el acceso a Internet desde cualquier punto de su interior. Sin embargo, para obtener un nivel aceptable del acceso a servicios multimedia de Internet con QoS, se requiere optimizar varios parámetros simultáneamente. Por ejemplo: el número de terminales móviles comunicando a través del mismo PA (en el mismo canal inalámbrico), el tipo de tráfico que estén comunicando y la calidad de la señal recibida por el terminal móvil, entre otros.

Actualmente ciertos PA [3] balancean la carga generada por diferentes terminales móviles entre ellos dentro de una BSS. Otros permiten especificar parámetros de QoS [4] para lograr que los terminales móviles accedan a Internet distinguiendo el tipo de tráfico soportado. Nosotros hemos desarrollado una aplicación Cliente-Servidor [5] que se instala en un encaminador Linux inalámbrico (*LRW: Linux Router Wireless* de aquí en adelante) capaz de gestionar múltiples aspectos relacionados con el uso del canal en una conexión inalámbrica. Con esta aplicación es posible proporcionar QoS en el acceso simultáneo a Internet de varios terminales inalámbricos tal como hemos demostrado en [6]. Una ventaja de nuestra aplicación frente a las soluciones que se plantean en los PA es que es escalable. Esto es, permite añadir un nuevo servicio para proporcionar controles adicionales de provisión del acceso a Internet con QoS de manera muy sencilla y directa sin necesidad de cambios importantes en el código de la aplicación.

En este trabajo presentamos una ampliación de esta aplicación para mejorar la QoS del acceso de terminales móviles en interiores a servicios de Internet. Para ello hemos estudiado cómo utilizar aspectos de la situación de un terminal móvil en función de su posición dentro de su espacio de localización. Las referencias de niveles de señal que un terminal pueda detectar desde un PA puede ser útil para:

- Informar al terminal móvil para que él tome acciones correctivas (reubicación, reorientación, variaciones físicas, etc.).
- Balancear el acceso a Internet teniendo en cuenta la carga de los PA.
- Planificar el despliegue de los PA a partir de un histórico de localizaciones estables de los terminales.

La localización de terminales es un clásico de las redes móviles [7] y existen muchos métodos de localización ampliamente estudiados [8]. Asimismo, éstos tienen muchas aplicaciones recientes que se usan masivamente [9] [10]. Los métodos de localización suelen ser dependientes de la red, la aplicación y la tecnología inalámbrica utilizada. En el caso de redes WiFi [1] [2] se han desarrollado soluciones propietarias, como por ejemplo la de skyhook [11] basada en Base de

Datos que contienen las localizaciones de los PA en una región amplia (ciudad). Con ello se intenta proveer servicios de localización bajo el abanico de servicios que puede ofrecer un operador de comunicaciones. Igualmente la empresa Ekahau dispone de soluciones especializadas en *Real Time Location System* (*RTLS*) [12]. Cisco también tiene sus propias aplicaciones [13]. Otros trabajos sobre localización en interiores se presentan en [14] basándose en tri-lateralización mediante cálculo de distancias y distribución de probabilidad (histograma). Ninguno de estos métodos se usa para mejorar el acceso a servicios de Internet de la misma forma en que nosotros queremos aplicarla.

Dada la variabilidad física de los niveles de señal radio en redes inalámbricas, la dependencia de un canal compartido por muchos clientes, el uso libre para múltiples aplicaciones y su vulnerabilidad relativa a interferencias externas, las posibilidades de aplicar técnicas de *Time Difference of Arrival* (TDOA), triangulación [15] o marcas de tiempo se limitan bastante. En lugar de aplicar complejos métodos, nosotros usamos el método de determinación de la localización de terminales mediante comparación y aproximación a los valores del mapa de referencia de coberturas (niveles de RSSI [16]). El terminal se localizará en un espacio $\overrightarrow{RSSI}$ de dimensión *n*, siendo *n* el número de PA registrados en una *BD* de coberturas por cada PA. Denotamos $\overrightarrow{RSSI} = \{RSSI1, RSSI2, \ldots . RSSIn\}$.

En este trabajo demostramos que el cálculo eficiente de la localización puede ser aprovechado para definir un parámetro adicional de QoS en el acceso a Internet. Una ventaja adicional es que por su sencillez la obtención de valores de este parámetro se puede llevar a cabo en los PA o en un servidor especializado. Entre los diferentes objetivos que podemos alcanzar que mejoren la QoS, especialmente en situaciones de movilidad o reducido número de PA es:

- Guiar a un terminal hacia la ubicación más adecuada dentro de su espacio de localización.
- Prever zonas con caídas bruscas de conectividad y evitación de las mismas.
- Reubicación de terminales a PA con mejores prestaciones.

Como primera línea de actuación hemos pretendido permitir que el usuario disponga de los mapas de cobertura en su terminal (uno por cada PA próximo a él) para que pueda elegir el PA que le proporcione una conexión más duradera o de mejor calidad con garantías aceptables de acceso a Internet. El usuario haría esta conexión dependiendo de su trayectoria o de forma automática pudiera ser guiado por el sistema. La definición de los mapas de cobertura se puede hacer con una aplicación sencilla, como la que hemos terminado de desarrollar recientemente [17]. La integración de estas dos aplicaciones permitiría que el usuario se subscribiese a este servicio de localización recibiendo los mapas de cobertura que previamente se han definido para una Organización concreta y posteriormente actuar con la información obtenida.

El resto del documento de organiza de la siguiente manera: en el apartado II se realiza una descripción general de la aplicación sobre la que estamos desarrollando múltiples soluciones para mejorar la QoS en redes 802.11. En el apartado III se exponen las ideas básicas sobre la localización como complemento para una mejora en la QoS. En la sección IV, describimos nuestra propuesta de implementación práctica del uso de la localización como parte de nuestra aplicación. En el apartado V se comentan los resultados experimentales y, en la sección VI las conclusiones finales y líneas futuras.

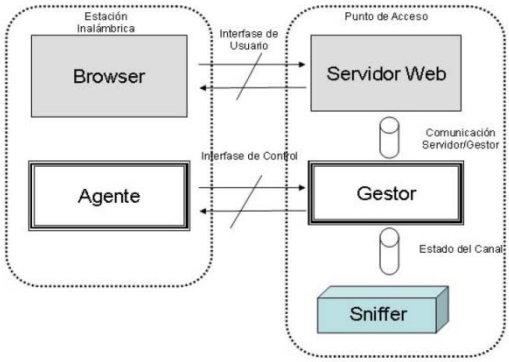


Fig. 1. Módulos que forman parte de la aplicación de pruebas.

II. Descripción General de la Aplicación

Nosotros usamos nuestra aplicación para soportar QoS en el acceso a Internet desde redes IEEE 802.11 con infraestructura en una Organización dada aprovechando información de localización de los terminales móviles. Esta aplicación se basa en el modelo Cliente-Servidor. En la figura 1 se muestran los diferentes módulos que forman parte de esta aplicación.

El servidor es el núcleo central de la aplicación y lo hemos denominado ***gestor*** (que se aloja en el servidor). Está implantado en un LRW [18], aunque podría ser desplegado sobre otras aplicaciones, como hostAP [19] con las correspondientes adaptaciones. El *LRW* está configurado con una interfaz inalámbrica y otra cableada para proporcionar conectividad de acceso a Internet. Puede ser configurado en modo ad-hoc o infraestructura, según se desee. El cliente se aloja en los terminales móviles y lo denominamos ***agente***. Los usuarios establecen sus preferencias o requisitos de acceso a servicios de Internet a través de una interfaz Web soportada por el servidor Web del LRW [5]. Cada usuario se identifica y especifica el servicio a utilizar (opcionalmente, notificaría requisitos de velocidad). A partir de ello, se calcula qué regulación de tráfico (velocidad de transmisión) debería aplicarse al terminal móvil entrante o resto de terminales. El gestor y los agentes intercambian diferentes mensajes de control para variar su comportamiento dependiendo del estado del canal inalámbrico.

Las dos principales funcionalidades de la aplicación, tras sus diferentes mejoras [5] [20] [21] son:

1. Gestión del canal de comunicación inalámbrico mediante distribución del ancho de banda inalámbrico: el gestor y los agentes cooperan para regular el uso del canal en función del tipo de tráfico a comunicar por el canal inalámbrico.

2. Re-asociación (cambio de LRW) de una estación inalámbrica que se encuentre ya asociada a un LRW hacia

otro LRW que ofrezca mejores prestaciones; para ello los LRW se intercambian información de estado.

El gestor determina, regula y lleva a cabo las acciones asociadas en el *LRW* y/o comunica al agente, las que éste debe aplicar en la estación, según cada caso. El gestor y el agente intercambian múltiples mensajes de estado o de control por un canal de transporte no orientado a conexión (*User Datagram Protocol* (*UDP*)), para no sobrecargar el canal con tráfico de control adicional. Los mensajes de control para la primera funcionalidad son los siguientes:

- *Hello* (detección de presencia de agente). El gestor de forma regular, detecta la presencia del agente el cual debe hacer un eco. Si el gestor no lo recibiera, inmediatamente bloquearía la conexión.
- *Update* (aplicación de regulación de tráfico). El gestor notifica periódicamente al agente la velocidad máxima (bps) que le ha asignado. El agente debe confirmarlo.
- *Finish_update* (fin de regulación de tráfico). El gestor notifica al agente el final de la regulación anteriormente establecida.
- *Finish_time* (fin de tiempo de conexión permitida). El gestor notifica al agente el final de la conexión aceptado inicialmente por la finalización del tiempo máximo permitido para la misma.

Para cumplir con la segunda funcionalidad se aplican los siguientes mensajes principales entre gestor y agente:

- *Request_roam_automatic*: el gestor fuerza un traspaso de un terminal móvil (desde el *LRW_inicial* hacia un *LRW_final*). El agente del terminal móvil seleccionado barre el espectro (*scanning*), y si detecta adecuadamente al *LRW_final,* se lo notifica al gestor para terminar el traspaso.
- *Request_roam_manual*: ahora se le notifica al usuario el traspaso para que él lo realice manualmente.
- *Request_end*: el terminal móvil debería estar asociado al *LRW_final* sin la intervención del usuario.

Los mensajes intercambiados entre gestores por la red cableada son:

- *Broad_status*: anuncios broadcast o multicast con información de estado del canal y número de clientes por cada *LRW*.
- *Offer_roam*: ofrecer a otro *LRW* que se encuentre en mejores condiciones.
- *Roam_end*: notificación de traspaso realizado con éxito desde *LRW_final* al *LRW_inicial*.

Con estas dos funcionalidades, hemos demostrado que con la distribución del ancho de banda disponible en función de la demanda y el traspaso de un LRW a otro guiado se consiguen mejorías en la QoS materializado en unas mejores prestaciones del acceso a Internet desde redes IEEE 802.11 [5] [6].

En este trabajo demostramos que también se puede usar la localización de terminales móviles para mejorar el acceso a servicios de Internet de una manera muy sencilla.

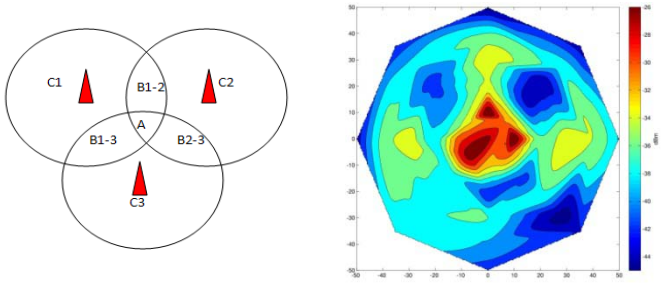


Fig. 2. a) Áreas de solapamiento teórico de cobertura de los PA de una Organización. b) Diagrama de radiación real medido en interiores para WiFi: diagrama de colores (dbm): -26(marrón),-28,-30,…-44(azul), (ejes) niveles teóricos: -50,-40,-30,-20,-10,0,10,20,30,40,50dbm.

III. Consideraciones sobre localización

En este apartado analizamos y describimos cómo añadir información sobre la localización de los terminales móviles (en un espacio de localización de $\overrightarrow{RSSI}$), a nuestra aplicación para mejorar el acceso a servicios de Internet.

La localización a través del método de la RSSI se basa en medir la intensidad de señal recibida desde cada PA y con los cálculos correspondientes por triangulación, y opcionalmente complementado con otras tecnologías, determinar la posición de cada terminal móvil. Normalmente, y de forma deseable, en el interior de una Organización, los PA se disponen de tal manera que se cubra su práctica totalidad. Eso no siempre es posible conseguir tal como demostramos en la práctica. Los PA se suelen disponer de tal manera que se solapen parte de sus áreas de cobertura (a las que denominamos celdas *C1*, *C2* y *C3* en la Fig. 2.a).

Estas representaciones teóricas de celdas tienen distintas derivas, en la práctica:

A. Los diagramas de radiación de las antenas omnidireccionales no son tan perfectos como se indican en la Fig. 2.a. Tal como se aprecia en la Fig.2.b la radiación disminuye con la distancia cuadráticamente; pero no uniformemente. Existen zonas en las que en teoría debería haber un nivel de señal elevado y sin embargo existe un nivel bajo debido a condiciones ambientales particulares de la zona.

B. El canal inalámbrico varía temporal y espacialmente de manera impredecible.

C. Las interferencias entre canales (en IEEE802.11b/g se dispone de tres frecuencias lo suficientemente separadas [1] [2]) no siempre suelen estar bien resueltas y provoca una degradación de la señal.

Estos tres problemas (y otros) hacen que no sea sencillo determinar la localización exacta de un terminal. Por ejemplo, para la Fig. 2.a no siempre podemos asegurar que un terminal se encuentre en la zona *A* si recibiera señal de los tres PA, o que estuviera en las zonas *B1-2*, *B1-3* ó *B2-3* si recibiera señal de dos PA. Por ejemplo, podría estar en la zona B1-3 y

sólo recibir señal de un PA.

Lo que está claro es que el terminal móvil que quiera acceder a un servicio de Internet debe detectar al menos un PA. Para ello puede especificar la frecuencia y/o canal manualmente o, lo más común, hacer un barrido del espectro en la banda de frecuencias de trabajo de WiFi. Detectado uno o varios PA debería asociarse a aquel que le ofrezca mejor calidad de señal. La información que obtengamos de cada PA visible sirve para determinar o estimar la posición del terminal móvil. Esta información, principalmente está relacionada con la intensidad, potencia o nivel de señal recibida, la relación Señal/Ruido (S/N) o el RSSI. Los diferentes drivers de dispositivos WiFi utilizan para realizar la asociación a un PA el nombre del SSID (*Service Set IDentifier*) y, si hay una varios, a aquel con mejor nivel de señal recibida.

Lamentablemente solo utilizar los niveles de señal recibida para determinar la posición es demasiado arriesgado. Si se contase con otros recursos, este problema se podría afrontar con mayores garantías de éxito. Basten dos propuestas:

- Si los PA contasen con información sobre su localización en un espacio o mapa de coberturas dentro de la organización (cargada manualmente por el instalador), y ésta pudiera ser tratada por software, sería el complemento ideal para determinar la localización de cada terminal.
- Los PA podrían contar con un registro de mapas o BD de coberturas con los diferentes niveles de señal que debería haber en cada una de las zonas a las que alcance su señal.

En cualquiera de los casos, la determinación de la localización de un terminal móvil se podría realizar:

a) En el terminal móvil.

b) En el PA.

c) Servidor especializado.

Sería recomendable, para descargar de trabajo a los terminales móviles, que fuesen los PA, los que, ante la petición de determinación de su localización realizada desde un determinado terminal móvil, pudieran barrer el espectro, medir el nivel de señal con los que detecta al terminal móvil y estimar su localización.

Este modelo presenta más ventajas dado que los PA pueden contar con mayor información y recursos que los terminales móviles. Son estáticos y pueden servir de referencia dentro de la zona de la Organización o posición global (coordenadas o posición dentro de la Organización). Además, pueden intercambiar información con otros PA para determinar por triangulación la localización.

Teniendo esto en cuenta, resultaría obvio delegar la localización en el PA que, con mejores prestaciones que los terminales móviles, podrían hacer rápida y eficientemente los cálculos de localización. Además, sería recomendable que la localización se determinara no solo con los datos que tenga el PA de los terminales móviles, sino también con la que le aporten otros PA, e incluso, y primordialmente, con los que los terminales móviles le suministren. Cuánta mayor cantidad información disponga el PA mejor determinará la localización. Nuestra propuesta consiste en que el PA al que está asociado el terminal móvil, sea el que determine su localización. Para ello tendría en cuenta los valores de RSSI de otros PA complementándolos con los datos que le entregue al terminal móvil de los PA a los que se puede asociar.

De esta forma, se añade la información obtenida por el terminal móvil que es bastante importante (se capturan los datos en la posición relativa en un espacio RSSI a determinar). Con ello, no sería muy necesaria la interacción con otros PA; sólo intervendrían el terminal móvil aportando los datos de los PA a los que se puede asociar (niveles de señal o RSSI) y el PA al que esté asociado. Obviamente con las tres fuentes de información sería el caso más completo y óptimo para una estimación óptima.

Teniendo en cuenta las ideas anteriores, la información sobre la localización de los terminales móviles se puede usar para mejorar su acceso a Internet. Los instantes de tiempo en los que es útil esta información sobre localización las resumimos en cuatro casos, si bien destacamos los dos últimos que permitirían mejorar la QoS del acceso a Internet:

- Al inicio de conexiones para selección de servicio (información, perfil, etc.). Esto se realiza en un solo instante de tiempo.
- Durante todo el movimiento del terminal móvil, dada la variación de señal, para evitar la pérdida de conexión. Esto se realiza durante un intervalo de tiempo.
- Durante intervalos de tiempo periódicos como complemento para mejora de la calidad de la comunicación.
- De manera puntual bajo demanda del terminal móvil. Éste solo se especifica cuando requiere este servicio.

IV. Propuesta e Implantación Práctica

Partimos de una BD de valores de RSSI creada previamente y comparando en ella los datos. En cualquiera de los casos, los cambios de intensidad o potencia de señal y la variabilidad de la señal radio hacen complejo el proceso de obtención de resultados con buena exactitud. Sería deseable que el nivel de señal de cada PA fuese estable para conseguir una posición exacta. Este problema se aprecia claramente, como ya se comentó, en la figura 2.b donde los niveles de señal no se distribuyen acordes con la teoría.

Esta *BD* debe contar con los niveles de señal de todo los PAs existentes incluyendo los SSID, frecuencia de trabajo e identificación de PA (por ejemplo número MAC) para las diferentes zonas a controlar. Partiendo de la variabilidad de los niveles de señal, se hace necesario generar la BD haciendo una gran cantidad de muestras, realizadas en diferentes momentos del día y con diferentes estados de carga, para darle un mayor rigor y exactitud a los valores de los diferentes parámetros a utilizar, así como registrar valores mínimos y máximos, cuando éstos sean variables. En cualquier caso, siempre hay un margen de error, debido a la variabilidad de muestras de RSSI. Esta BD se debería actualizar regularmente siempre que haya cambios de *Service Set IDentifier* (SSID) de celdas, frecuencia o cambios de

ubicación. Tanto más fiable sería este modelo, cuanto mayor número de PA estén disponibles.

La creación de esta BD con las zonas de coberturas y niveles de señal disponibles en cada zona por cada PA, constituiría un trabajo de campo previo de las diferentes zonas donde haya PA y se desee ofrecer este servicio de localización para mejorar la QoS. La BD se ubicaría en cada PA o un servidor especializado. Tanto en un caso como en el otro, solo se tendrían que comparar los niveles de RSSI detectados en el terminal móvil para los diferentes PA con los cargados en la BD. Sería necesario aplicar métodos de aproximación pues no siempre serán exactos los datos obtenidos con los incluidos en la BD.

Para la materialización de nuestra implantación vamos a hacer una separación en dos pasos:

- Creación de la BD de coberturas (mapas de coberturas).
- Proceso de determinación de la localización de un terminal móvil.

El primer paso lo llevamos a cabo mediante un proceso de realización de medidas de campo de forma manual seleccionando zonas a controlar. Con un ordenador portátil se registran los niveles de señal y resto de datos de los diferentes PA visibles, y al final, se crea el archivo o BD de coberturas para un espacio de localización RSSI. Paralelamente y como comprobación, hemos utilizado nuestra otra aplicación para *Personal Digital Assistant* (*PDA*) [17], que de forma gráfica muestra los mapas y las ubicaciones.

En la figura 3 se ilustran un par de capturas de la aplicación durante su ejecución en una PDA *HP iPAQ 5555*. Usándola se recorre toda la Organización y elabora un mapa con coordenadas de cada espacio de localización, los PA y niveles de RSSI. Con estos datos, el servidor los registra y los vincula a un plano real de la zona en estudio. Con esta información, posteriormente, se determina la localización de forma eficaz. Otras formas similares de realizar este proceso en interiores y exteriores se plantean en [22].

En cuanto al proceso de determinación de la localización automática sin intervención del usuario, planteamos una forma en la que cada terminal móvil debe barrer el espectro, registrar a todos los PA detectados y esta información deba ser enviada al PA; con ella, el PA o a un servidor especializado, si lo hubiese, determina la posición del terminal móvil solicitante. En la figura 4 se ilustra el proceso incluyendo las diferentes fases o etapas. Una vez se encuentre el terminal móvil asociado a un LRW, en nuestro caso está asociada al *LRW1*, podría solicitar su localización (paso ① en la figura 4). Para ello se haría la solicitud correspondiente. Dado que el *LRW1* solo puede obtener directamente el nivel de RSSI de dicho terminal, y quizás esta información pueda ser insuficiente o no determinante, antes de determinar la localización, podría requerirle información complementaria o más detallada (como el nivel de RSSI e identificaciones de todos los *LRWi* que él detecte) (②).

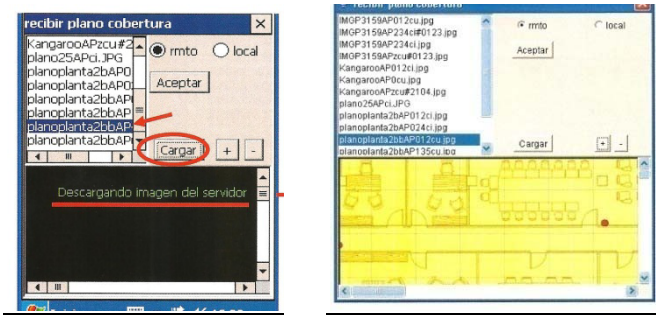


Fig. 3. Aplicación de localización de AP en interiores.

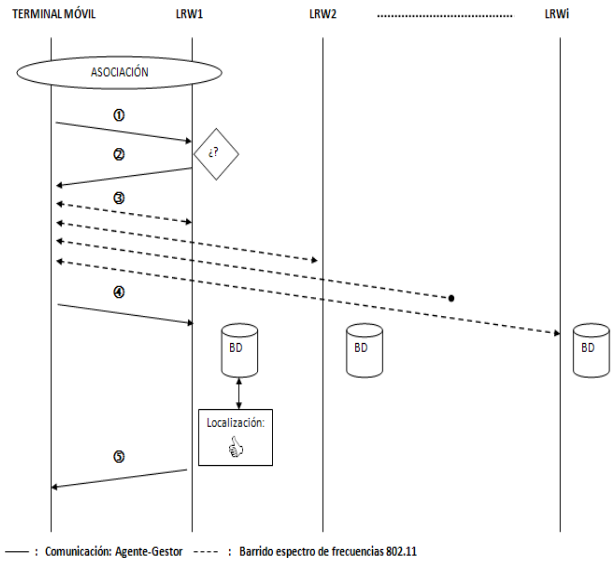


Fig. 4. Modelo de localización basado en BD (mapa).

Después, el terminal móvil realizaría un barrido del espectro (③) y capturaría los diferentes datos de los diferentes PA o *LRW* accesibles. Esta información una vez estructurada de forma correcta, se enviaría al *LRW* (④). Con los mismos, el *LRW* localizaría en la BD, creada y cargada previamente, los datos coincidentes o más próximos con los diferentes rangos, y determinaría la localización. Finalmente se le devolvería al terminal móvil solicitante la posición (⑤), o en su defecto, cualquier incidencia que pudiera haberse producido.

El tratamiento y búsqueda en la BD consiste en ir buscando el mayor número de coincidencias (pudiéndose encontrar múltiples *LRW* que las satisfagan) y pudiéndose dar múltiples casos:

- Se encuentra información de localización inadecuada (un solo *LRW*), o sea, sólo se puede determinar un área de localización del terminal (una esfera teórica) que coincide con el área de cobertura definida por RSSI1. Nuestra aplicación hace que el *LRW*1 controle la QoS asignando velocidades máximas de acceso a Internet entre los terminales móviles.
- Se encuentra información de localización (dos LRW) poco adecuada. En teoría, el terminal móvil se encuentra en el área de cobertura intersección de las definidas por RSSI1 y RSSI2. La aplicación detectaría las fronteras de esa área de cobertura

observando los niveles de RSSI registrados en la BD que coinciden con esa zona. De esta manera la QoS de acceso a Internet mejoraría porque la aplicación aconsejaría al terminal móvil que se moviese hacia una determinada zona cercana donde se obtiene un nivel mejor de RSSI.

- Se encuentra información de localización (tres o más *LRW*) adecuada. En este caso se cuenta con bastante información para localizar las coincidencias o aproximaciones en la BD y, además se pueden sugerir movimientos lineales o puntuales hacia zonas con mejor calidad de señal, cuando se den dichas zonas en la BD de referencia.

Para tratar estos casos introducimos una clasificación, que denominamos *grado de exactitud* de la información de localización. El *LRW*, por medio del gestor indica con un número entre 1 y 5 un baremado de la determinación de la localización. Concretamente, un 1 representa el caso peor, debido probablemente a contar con un sólo *LRW* y, el caso optimo, con un 5, cuando se cuente con tres o más *LRW*. Notar que hemos distinguido 5 casos, pudiendo variarse según se determine.

En base a los resultados de localización, el gestor determina, según la configuración que hayamos hecho de su funcionamiento, bajo qué condiciones de grado de exactitud sugeriría al terminal móvil un cambio de localización o activaría un cambio automático/manual de *LRW* (segunda funcionalidad de la aplicación).

Los mensajes necesarios para esta funcionalidad son:

- *Request_location*: petición de localización realizada desde el agente al gestor.
- *Request_scan*: petición enviada del gestor al agente para que realice el barrido en todos los canales inalámbricos (detección de *LRW* o PAs).
- *Reply_scan*: información de barrido devuelta desde el agente al gestor.
- *Info_location*: información devuelta al agente desde el gestor sobre localización detectada en la BD. Como parte de este mensaje se incluye el grado de exactitud.

Dado que nuestra aplicación, como ya se comentó, se ha implementado en un servidor Linux con la funcionalidad *LRW* y éste cuenta con una más que adecuada capacidad de computación, hemos incorporado la BD y el cálculo de la localización como parte del gestor, si bien podría descargarse de trabajo al gestor implantándolo en una aplicación independiente. Esto formaría parte de una posible evolución futura de la implantación de esta funcionalidad de localización de forma local (proceso interno) o remota (en otro servidor en la red cableada).

Nótese que para el *handoff* de teléfonos móviles en redes celulares se utiliza un sistema similar al nuestro. La diferencia es que en nuestro caso, el proceso sobre IEEE 802.11 es mucho más complejo debido a las condiciones ambientales y las pequeñas distancias de las zonas de cobertura de los PA. Esto lo mostramos a continuación.

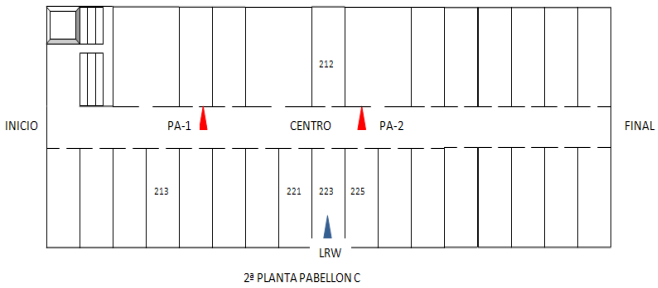


Fig. 5. Esquema interno de distribución de despachos y PA.

V. RESULTADOS EXPERIMENTALES

Una vez implantada esta funcionalidad en nuestra aplicación, se han realizado diferentes pruebas en el contexto de un recinto cerrado, concretamente en las dependencias del Departamento de Ingeniería Telemática en la segunda planta del Pabellón C de los Edificios de Telecomunicación de la Universidad de Las Palmas de Gran Canaria (ULPGC). Se han utilizado como patrones para la BD de coberturas, los PA que dan cobertura inalámbrica a la red universitaria de acceso gratuito con *SSID: ULPGC* y, complementariamente con la red virtual de acceso inter-universitario *SSID: EDUROAM* con acceso restringido. Además, hemos activado uno de los gestores en uno de los equipos actuando como *LRW* actualizado con la funcionalidad de localización. Además se ha adaptado el interfaz web para soportar la petición de localización inicial realizada por el usuario desde el terminal móvil.

Para crear la BD hemos utilizado un ordenador portátil con *Ubuntu 8.10* [23]. Primero se realizó un proceso de captura de datos de PA visibles (barrido de frecuencias) desde cada una de las diferentes dependencias, y con esos datos y su tratamiento posterior (eliminación de datos aislados, erróneos, cálculo de valores medios, búsqueda de mínimos y máximos), se elabora el mapa de coberturas (BD). Para realizar las medidas hemos utilizado las funciones *wireless-tools* de Linux [24].

La zona escogida es el interior de un edificio de paredes antiguas (de gran grosor) cuya distribución está formada por dos filas de despachos en hilera y de fondo aproximadamente unos 65 m con un pasillo central (véase figura 5). Se seleccionaron diferentes despachos y al menos cuatro zonas del pasillo. Únicamente se encontraban activos 2 PA denominados *PA-1* (a aproximadamente 1/4 del pasillo) y *PA-2* (aproximadamente a 3/4 del pasillo) (marcados con triángulos en la figura 5). En estas zonas se han capturado los siguientes datos: *Zona* (cadena de caracteres que identifica posición), *MAC* (cadena formado por los 6 bytes separados por el carácter "**:**" como dirección MAC de cada interface 802.11 de cada PA), *SSID* (cadena de caracteres de identificación del PA), *Frecuencia* (valor de frecuencia, en la forma YYYY), *Canal* (canal de emisión (Z o ZZ)), *Niveles de RSS* (valor mínimo, medio y máximo del valor de RSS y de referencia de señal recibida), *Niveles de Señal* (valor mínimo, medio, máximo del nivel de señal recibida), *Niveles de Ruido* (valor mínimo, medio, y mínimo del nivel de ruido recibido).

ZONA	MAC	SSID	Freq./Canal	RSS Min, med, max	RSS Min, med, max	Señal min-med-max	Ruido min-med-max
.....							
Inicioct	00:12:01:B5:5B:81	ULPGC	2412 1	13 21 33	70 70 70	-62 -73 -82	-95 -95 -95
Inicioct	00:12:01:B5:62:D1	ULPGC	2432 5	21 28 39	70 70 70	-56 -66 -74	-95 -95 -95
Inicioct	00:0F:24:EC:FA:41	ULPGC	2412 1	14 15 16	70 70 70	-79 -79 -81	-95 -95 -95
Inicioct	00:14:A9:75:09:11	ULPGC	2462 1	1 2 9 13	70 70 70	-82 -85 -93	-95 -95 -95
Inicioct	00:12:01:B5:61:F1	ULPGC	2442 7	32 33 36	70 70 70	-59 -61 -63	-95 -95 -95
Inicioct	00:12:01:B5:69:71	ULPGC	2422 3	23 29 38	70 70 70	-57 -65 -72	-95 -95 -95
Inicioct	00:12:01:B5:66:B1	ULPGC	2447 8	21 22 27	70 70 70	-68 -72 -74	-95 -95 -95
Inicioct	00:12:01:B5:65:21	ULPGC	2447 8	17 19 25	70 70 70	-70 -75 -78	-95 -95 -95
Inicioct	00:12:01:B5:5E:71	ULPGC	2452 9	18 21 30	70 70 70	-65 -73 -77	-95 -95 -95
Inicioct	00:12:01:B5:49:A1	ULPGC	2457 10	24 25 27	70 70 70	-68 -69 -71	-95 -95 -95
Inicioct	00:14:A9:75:05:B1	ULPGC	2422 3	9 9 9	70 70 70	-86 -86 -86	-95 -95 -95
Inicioct	00:12:01:B5:61:81	ULPGC	2452 9	6 6 6	70 70 70	-89 -89 -89	-95 -95 -95
Inicioct	00:0F:24:EC:FE:71	ULPGC	2437 6	10 11 1 2	70 70 70	-83 -84 -85	-95 -95 -95
.....							
213	*00:12:01:B5:5B:81*	*ULPGC*	*2412 1*	*18 23 26*	*70 70 70*	*-69 -71 -77*	*-95 -95 -95*
213	*00:12:01:B5:62:D1*	*ULPGC*	*2432 5*	*29 31 35*	*70 70 70*	*-60 -63 -66*	*-95 -95 -95*
213	00:12:01:B5:5B:80	EDUROAM	2412 1	18 23 26	70 70 70	-69 -71 -77	-95 -95 -95
213	00:12:01:B5:62:D0	EDUROAM	2432 5	29 31 34	70 70 70	-61 -63 -66	-95 -95 -95
213	00:12:01:B5:69:71	ULPGC	2422 3	2 2 2	70 70 70	-93 -93 -93	-95 -95 -95
213	00:12:01:B5:69:70	EDUROAM	2422 3	4 4 5	70 70 70	-90 -90 -91	-95 -95 -95
223	*00:12:01:B5:5B:81*	*ULPGC*	*2412 1*	*22 27 29*	*70 70 70*	*-66 -67 -73*	*-95 -95 -95*
223	*00:12:01:B5:62:D1*	*ULPGC*	*2432 5*	*18 20 23*	*70 70 70*	*-72 -74 -77*	*-95 -95 -95*
223	00:12:01:B5:5B:80	EDUROAM	2412 1	23 27 30	70 70 70	-65 -67 -72	-95 -95 -95
223	00:12:01:B5:62:D0	EDUROAM	2432 5	19 20 23	70 70 70	-72 -74 -76	-95 -95 -95
.....							

Fig. 6. Fragmento de BD Real.

El *driver* utilizado para gestionar dispositivos basados en el chip de comunicaciones *Atheros* [25] incorporados en la interfaz wireless del terminal móvil Linux fue *mad-wifi* [26]. En la figura 6 se muestra un fragmento de la BD creada, en la que las diferentes columnas de la BD representan:

- *Zona* de ubicación (pasillo, despacho, escalera, etc.).
- Dirección MAC de cada PA detectado.
- SSID de cada PA.
- Frecuencia de Trabajo y Canal de cada PA.
- Valor más bajo de RSSI obtenido.
- Valor medio de RSSI calculado.
- Valor más alto de RSSI obtenido.
- Los tres siguientes representan: valor más bajo, medio y más alto de RSSI (referencia).
- Los seis últimos representan: valor más bajo, medio y más alto de Nivel de Señal obtenido, Valor más bajo, medio y más alto de Nivel de Ruido obtenido.

En la BD hemos denominado a cada zona de ubicación con las palabras inicioct, 211, 213, 223, etc. Según sea cada caso, los PA detectados pueden diferir, como sucede al principio del pasillo (inicioct) y al final del mismo (extremos del edificio) y, además, estos no son visibles o registran valores no representativos en la parte central e interior de los despachos por la poca penetración de su señal.

Estudiado los datos para los despachos 213 y 223 y reflejados en la figura 7 observamos varios aspectos a destacar:

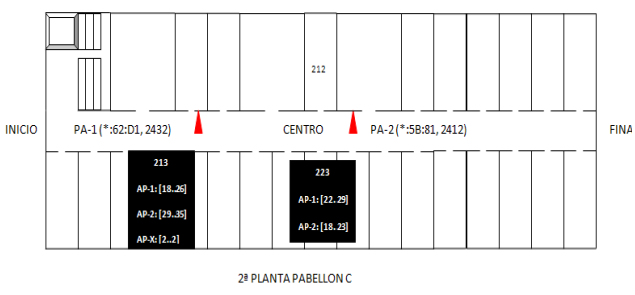


Fig. 7. PA detectados y niveles de RSSI en los despachos 213 y 223.

1º) La variabilidad de valores de RSSI a pesar de la cercanía de los PA a las ubicaciones seleccionadas. Por ejemplo, en el interior del despacho 223, y solamente a unos 4 metros del PA-2 (***00:12:01:B5:5B:81, SSID: ULPGC, FREQ: 2412***), los márgenes de RSS variaron desde 22 a 29 para una captura de unas 200 medidas. Estas medidas fueron realizadas en varias sesiones durante el mismo día y separadas en el tiempo.

2º) En algunos casos, estos márgenes para la ubicación 223 variaron a niveles de 16 a 18, medidos otro día diferente y para otra gran cantidad de muestras. Hecho similar ocurrió para el resto de ubicaciones (primera columna). Si bien esto plantea un serio problema para definir una BD patrón o referencia de medidas, podemos partir del caso más común y evaluar los resultados.

3º) Los rangos RSSI más comunes para el PA-2 no son iguales para las ubicaciones 213 y 223. Esta información puede ser determinante para tener una mejor predicción de la posición.

4º) La cercanía de los PA entre sí, provoca que muchos valores sean iguales en dos ubicaciones distintas. Por ejemplo el rango de valores de RSS entre 22 y 26 se encuentra entre los posibles para el PA-1 y el PA-2 en las ubicaciones 213 y 223. Por tanto, con un valor en este rango, a menos que se complemente con otras medidas, no es útil para discernir en cuál de las dos posiciones se encuentra el terminal.

5º) Se observa que, en ciertas ubicaciones, como por ejemplo la 213, se detecta un PA (***00:12:01:B4:69:71, SSID: ULPGC, FREQ: 2422***) no localizado en la 2ª planta y que probablemente está ubicado en los exteriores del edificio u otras plantas del edificio (muy bajo RSSI y pocas veces detectado). Esta información podría ser relevante (si tuviese valores aceptables) para diferenciar si se está en 223 o 213 ante otras situaciones coincidentes de los dos otros márgenes.

6º) Algunos PA cambian su frecuencia de trabajo. Estos casos han sido eliminados de la BD, dado que esta aleatoriedad es un aspecto que genera distorsiones en el uso de la localización para mejorar la QoS.

Una vez inicializada la BD en el *LRW* y, ubicado a modo de prueba, en la zona 223, realizamos múltiples pruebas de esta funcionalidad. Para ello, simplemente utilizamos un ordenador portátil con el agente instalado y nos ubicamos en diferentes zonas (despachos y pasillos) y procedemos a solicitar el servicio implementado como parte de la aplicación desde dicho ordenador portátil atacando al *LRW*. El gestor procesa la petición y comprobamos que éste, solicita al agente que se realice el barrido de espectro. Una vez finalizado el barrido, se envían los datos capturados (en un formato equivalente al de la base de datos) al gestor. Trascurrido un cierto tiempo (búsqueda en la BD) devuelve el nombre de la ubicación más probable según la estimación realizada por el gestor,

con la indicación numérica del grado de exactitud. En base a éste el usuario y el agente realizan las acciones oportunas según desee, tras su valoración acerca de los resultados obtenidos. El gestor haría lo propio una vez se active el traspaso u otras acciones contempladas.

Tras múltiples ejecuciones de la aplicación, como era de esperar, la gran mayoría de los resultados fueron muy aproximados. En otros casos la variabilidad de los niveles de señal o la reducida información disponible (solo 2 PA disponibles) impidieron obtener la localización con un mayor grado de exactitud. Esto sucedió en múltiples pruebas realizadas, por ejemplo, desde el interior del despacho 223. En varios casos, el agente detectaba al PA-2 con valor 18 (no contemplado como posible en la BD para dicha zona), por lo que el gestor determinaba la ubicación 213 con grado exactitud 2.

VI. Conclusiones y líneas futuras

En este artículo se han presentado las ideas y conceptos vinculados con la localización para mejorar la QoS del acceso a Internet en redes IEEE 802.11 con infraestructura dentro de una Organización (en interiores) y su integración en una aplicación de gestión integral del canal de redes IEEE 802.11. Esta aplicación cuenta con la función de gestión y distribución del uso del ancho de banda del canal y la función de re-distribución de las estaciones al *LRW* más idóneo. Hemos incorporado este sistema de búsqueda de la ubicación en un espacio de búsqueda definido por valores de RSSI de los distintos PA. Estos valores los entregan los terminales móviles a un servidor, y éste hace la estimación y los cálculos para determinar su posición. La implantación se ha materializado en una nueva funcionalidad de nuestra aplicación integrada en el terminal móvil (agente) para hacerse en el proceso inicial de acceso al canal a través del gestor en el *LRW*.

En esta solución se parte del uso de una BD en la que se registra principalmente $\overrightarrow{RSSI}$. Como toda tecnología radio, donde el canal es muy cambiante y alterable, especialmente en el nivel de señal recibida (por múltiples factores, número de clientes, interferencias otros canales, condiciones ambientales, etc.), la estimación de la localización es muy difícil.

Actualmente estamos aprovechando los datos obtenidos de esta funcionalidad para su aplicación y complementación con las otras funcionalidades. Especialmente en la línea de re-orientar a las estaciones hacia los PA más idóneos por calidad de señal, para evitar cortes de conexión, especificar zonas de conectividad segura, etc.

Pretendemos realizar los cálculos de determinación de posición de las estaciones en zonas abiertas donde haya menores problemas de transmisión de la señal debido a condiciones ambientales (por ejemplo reflexión, refracción y difracción). También pretendemos mejorar el esquema y tratamiento de la BD para facilitar su rápido procesado, optimización y filtrado, comparación e iteración en el proceso de búsqueda y toma de decisión final.

Referencias

[1] IEEE 802.11g-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[2] IEEE 802.11b-1999 Supplement to IEEE 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.

[3] DLINK. DWL-1000AP+. DAP2553. URL: www.dlink.com

[4] Linksys WAP2000. WRTG54G. URL: www.linksysbycisco.com

[5] D. Marrero, E. Macías, A. Suárez, "Aplicación multifuncional para gestión del canal en redes IEEE 802.11". VIII Jornadas de Ingeniería Telemática. JITEL2009. Cartagena 15-17 Sept. 2009. ISBN: 978-84-96997-27-1, pp. 16-23.

[6] D. Marrero, E. Macías, A. Suárez, "An Admission Control and Traffic Regulation Mechanism for Infrastructure WiFi networks". IAENG International Journal of Computer Science, 35:1, IJCS_35_1_21. March-2008. ISSN: 1819-656X.

[7] Schiller J. H., "Mobile Communications," Segunda edición, Addison-Wesley, 2003.

[8] Munoz D., Bouchereau F., Vargas C. y Enriquez R., "Position techniques and Applications", Academic Press (Elsevier), 2009.

[9] Meng L., Zipf A. y Winter S. (Eds.), "Map-based Mobile Services Design, Interaction and Usability", Lecture Notes in Geoinformation and Cartography (Springer Verlag), 2008.

[10] Karimi, H. A., "Handbook of research in Geoinformatics", IGIC Global, 2009.

[11] http://www.skyhookwireless.com/howitworks/architecture.php.

[12] Ekahau. RTLS (Real Time Location System) http://www.ekahau.com/products/real-time-location-system/overview.html

[13] http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns788/white_paper_c11-476796.html

[14] M. A. Quintana, D. Sánchez, D. Marrero, Juan L. Navarro, "Localización en WLAN utilizando distribuciones de probabilidad con reducción de cómputo por trilateralización". JITEL2009, Cartagena 15-17 Sept. 2009 ISBN: 978-84-96997-27-. pp. 183-189.

[15] Zhao L., Yao G., Mark J. W., "Mobile positioning based on relaying capability of mobile stations in hybrid wireless networks". IEE Proceedings-communications, 2006, 153(5): 762–770

[16] RSSI (Received Signal Strength Identifier). 802.11k. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4544755&tag=1

[17] Antonio R. Prieto Bernárdez, Alvaro Suárez Sarmiento. "Aplicación Gráfica para la localización de puntos de acceso en interiores de entornos poco cambiantes". Proyecto Fin de Carrera EUITT-ULPGC, Julio 2009.

[18] Netfilter/Iptables Project Homepage. http://www.netfilter.org/. Linux Advanced Routing & Traffic Control, Available: www.lartc.org, URL: http://tcng.sourceforge.net/.

[19] URL: http://hostap.epitest.fi/

[20] D. Marrero, A. Suárez, E. M. Macías, "Dynamic Interconnection of Adhoc Nodes Based on the Type of Service to be Accessed", International Conference on Wireless Networks (ICWN), Junio 2005, pp. 539-545.

[21] D. Marrero, E. M. Macías, A. Suárez, "Dynamic Traffic Regulation for Wifi Networks". World Congress on Engineering 2007 (WCE2007). ICWN'07 Londres 2-4 Julio 2007, ISBN978-988-98671-2-6.

[22] Nobuo Kawaguchi,"WiFi Location Information System for Both Indoors and Outdoors", Springer Berlin / Heidelberg, ISBN 978-3-642-02480-1

[23] Testbed. Interfaces. D-Link Homepage, http://www.dlink.com. S.O. Ubuntu 8.10 Linux y Fedora Core 8. Ordenadores Personales con Linux-router. PCs Portátiles con Linux e interfaces madwifi (chip Atheros).

[24] URL: www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

[25] URL: http://www.atheros.com/

[26] URL: http://www.madwifi.org/

Evaluación de prestaciones de una red híbrida vehicular y de sensores para mejorar la seguridad vial

Carolina Tripp Barba, Karen Ornelas, Guillermo Díaz Delgado, Mónica Aguilar Igartua
Departament d'Enginyeria Telemàtica. Universitat Politècnica de Catalunya (UPC). C/ Jordi Girona 1-3, Mòd. C3, Campus Nord, 08034 Barcelona.
{ctripp, gdiaz, monica.aguilar}@entel.upc.edu, karen.ornelas@gmail.com

***Resumen*- En los últimos años las redes inalámbricas se han convertido en una tecnología de comunicación ampliamente difundida así como en un reto en cuanto a investigación se refiere. Se han presentado muchas contribuciones sobre redes ad hoc, tales como redes inalámbricas de sensores (WSN, *Wireless Sensor Networks*) y redes vehiculares (VANET, *Vehicular Ad hoc Networks*). Recientemente, la cantidad de coches que transitan en nuestras calles, carreteras y autopistas ha ido en aumento, dando pie a un gran interés en las tecnologías de comunicación vehicular. Un nuevo tipo de red ha sido desarrollada, denominada Red Híbrida Vehicular y de Sensores (HSVN, *Hybrid Sensor and Vehicular Network*) en la cual WSNs y VANETs cooperan entre sí con el objetivo común de mejorar la seguridad vial. Existen proyectos recientes, tales como CVIS [8] y COMeSafety [10], que se han enfocado en estos aspectos. Este tipo de propuesta prevendrá al conductor y al copiloto sobre cualquier evento que ocurra en la ruta por la que circulan, tales como accidentes que han sucedido en la carretera, densidad de tráfico, condiciones climatológicas de las rutas, etc. De esta manera el número de accidentes de tráfico podrá decrecer significativamente y se podrán salvar muchísimas vidas. Así mismo, otros servicios de entretenimiento como el acceso a Internet y las descargas multimedia podrán estar disponibles fácil y económicamente con el despliegue de infraestructura a lo largo de las carreteras. Además, el sistema navegador de a bordo podrá elegir la ruta que esté realmente menos congestionada, ayudando así a disminuir la contaminación. Transportarse en coche será más fácil, seguro y más cómodo para los pasajeros. En el presente artículo se presenta una plataforma de HSVN, así como la descripción y evaluación de un protocolo de comunicación entre VANETs y WSNs usando como simulador NCTUns [20] para su evaluación.**

***Palabras clave*- WSN (*Wireless Sensor Networks*), VANET (*Vehicular ad hoc Networks*), HSVN (*Hybrid Sensor and Vehicular Network*).**

I. INTRODUCCIÓN

Las investigaciones en tecnologías de corto alcance han ido en aumento en los últimos años. Así pues, las redes ad hoc han recibido más atención debido al fácil despliegue que suponen. Una red Ad hoc [1, 2] está formada por un grupo de nodos que se comunican entre sí con una interfaz inalámbrica, además de poder trabajar tanto con infraestructura fija como sin ningún tipo de infraestructura. En el entorno en que se plantea este trabajo hay dos tipos de redes ad hoc: las WSNs (*Wireless Sensor Networks*) [3] y las VANETs (*Vehicular Ad hoc Networks*) [2, 4]. Ambas son redes ad hoc capaces de operar sin ninguna infraestructura definida y sin administración centralizada. La organización de esta red está a cargo de los mismos nodos que la conforman. Cada nodo es capaz de trabajar como emisor, destinatario o simple repetidor de la información. Los nodos en una WSN son estáticos, mientras que los nodos en la VANET pueden alcanzar altas velocidades. Los cambios frecuentes que presenta la topología debido a la movilidad de los vehículos en la red VANET exigen el diseño de un protocolo de encaminamiento flexible y que se adapte a estas velocidades de los nodos.

Una WSN consiste en un grupo de pequeños dispositivos inalámbricos capaces de recolectar información de su entorno como temperatura, humedad, movimiento, etc. Este tipo de redes permiten un rápido despliegue de estos dispositivos debido a su pequeño tamaño y peso. Pero presentan algunas restricciones en comparación con otras redes ad hoc que se deben tomar en cuenta al momento de trabajar con ellos, como capacidad limitada de memoria, energía y procesamiento, así como bajo alcance de transmisión.

En una VANET se asume que cada nodo en la red está equipado con alguna tecnología de navegación, como GPS (*Global Positioning System*) [5]. Una VANET se considera como un tipo particular de MANET (*Mobile Ad hoc Network*) [1]. Sin embargo, la principal diferencia está en la velocidad de los nodos que la conforman. Este factor produce cambios rápidos en la topología y eso produce que los enlaces tengan un corto periodo de vida. Por otro lado, los dispositivos en los vehículos no presentan límites de energía, además de poder tener un alto poder de procesamiento. Para finales de 2010, se espera la publicación del estándar IEEE 802.11p [4, 6] el cual será una gran contribución a mejorar la comunicación a través de los vehículos que forman la VANET. El cual maneja rangos de comunicación de hasta 1000 metros, bandas de frecuencia de hasta 5.92 GHz, modulación OFDM (*Orthogonal Frequency Division Multiplexing*), así como soportar alta movilidad de los nodos [6].

Una red híbrida vehicular y de sensores (HSVN, *Hybrid Sensor and Vehicular Networks*) es un nuevo concepto que permite incorporar sensores a lo largo de las carreteras, lo cual puede ser considerado como una arquitectura de red heterogénea de nueva generación. En una perspectiva global, la información sobre las condiciones medioambientales, como

lluvia o hielo, y la densidad de tráfico en trayectos remotos podrá ser monitorizada por los vehículos, que posteriormente será almacenada en la WSN para que pueda ser distribuida a través de otros vehículos que pasen posteriormente por el segmento de carretera determinado por un grupo de sensores. El propósito principal de este tipo de red es que los coches dentro de una VANET puedan compartir información referente a condiciones climáticas, estado de tráfico y seguridad vial, con el fin de reducir el número de accidentes. Gracias al intercambio oportuno de esta información los usuarios podrán viajar más seguros a lo largo de sus trayectos.

II. ESTADO DEL ARTE

Recientemente, en Europa se han creado diferentes consorcios [7, 8, 9, 10, 11, 12] cuyo objetivo es hacer más seguros tanto los vehículos como los trayectos. Estos consorcios están integrados principalmente por fabricantes de coches, investigadores y la Comisión Europea. CAR 2 CAR [7] es un consorcio iniciado por fabricantes Europeos, cuyo objetivo principal es aumentar el tráfico seguro y eficiente haciendo uso de los ITS (*Intelligent Transport Systems*), así como de las comunicaciones vehículo-a-vehículo (V2V, *Vehicle-to-Vehicle*) y vehículo-a-infraestructura (V2I, *Vehicle-to-Infrastructure*).

El proyecto CVIS (*Cooperative Vehicle-Infrastructure Systems*) [8] trabaja con sistemas inteligentes y cooperativos que se basan en comunicaciones de tipo V2V y V2I, con lo que le permite adquirir mejoras tanto en eficiencia en el sistema de transporte, como en la seguridad de los usuarios que estén a lo largo del camino. Los beneficios que se esperan son el poder procesar información disponible del vehículo y de su entorno. Dichos beneficios incluyen mejoras en la capacidad de la red del trayecto, reducción de la congestión de tráfico, reducción de la contaminación, elección de caminos con menor tiempo de trayecto, mejora de la seguridad de tráfico para todos los usuarios, logística más eficiente, aumento del control sobre la red del trayecto (urbano e inter-urbano), aumento en la eficiencia de los sistemas de transporte público y una mejor respuesta de acción ante accidentes e incidentes en carretera.

El proyecto CARLINK [9] busca el desarrollo de un servicio inteligente para coches. La aplicación principal de este proyecto es ofrecer información de clima en tiempo real, reportes del estado del tráfico y otras aplicaciones en *broadcast*. Los vehículos estarán debidamente equipados para hacer posible la comunicación con una estación base y con otros nodos ad hoc que participen en la red. El objetivo del proyecto está orientado a mejorar la industria automotriz, involucrando a los operadores de telecomunicaciones, a los conductores y demás usuarios de las vías. Los nuevos coches está previsto que estén equipados con un nuevo tipo de servicio de telecomunicación relacionado con los ITS que permitiría grandes beneficios a los operadores así como a los usuarios.

El proyecto COMeSafety [10] está respaldado por el foro eSafety [11] respecto a todas las cuestiones relacionadas con las comunicaciones V2V y V2I como base para la cooperación de sistemas inteligentes de transporte por carretera. También proporciona una plataforma abierta de integración de los intereses de todos los participantes públicos y privados representados. Los resultados consolidados se envían a los organismos europeos de normalización y también a todo el resto del mundo.

INFOTRANSIT [12] ha sido desarrollado por la fundación RACC (*Reial Automòbil Club de Catalunya*), la cual provee de información para hacer la conducción más segura. Consiste en un servicio en Internet basado en diferentes fuentes de datos que proveen información actualizada continuamente del tráfico en tiempo real, datos del clima, localización de radares y de accidentes. Utiliza mapas interactivos basados en los mapas de Google [13]. En un futuro no muy lejano, los conductores serán capaces de acceder y actualizar dicha información de tráfico en cualquier momento durante su viaje sin coste adicional alguno. La información será proporcionada por la Dirección General de Tráfico (DGT). Con esto, los conductores podrán fácilmente ver la localización de los radares, podrán obtener videos cortos de las cámaras de tráfico y la localización de cualquier accidente ocurrido en su trayectoria.

Recientemente, ha sido propuesto un nuevo enfoque a partir de la unión de dos tipos de redes ad hoc, WSNs y VANETs. Una HSVN, consiste en hacer que las redes de sensores y vehiculares trabajen juntas para constituir un sistema de comunicación que puede ser utilizado por los vehículos con el objetivo de asistir al conductor con el objetivo principal de reducir los accidentes en las carreteras. Nuevas arquitecturas han sido propuestas para ofrecer un enfoque robusto, flexible y efectivo para las HSVN. Varios trabajos de investigación, como [14] y [15], han sido realizados donde el principal reto ha sido el de diseñar la arquitectura HSVN. Una red HSVN necesita incluir un protocolo de comunicación entre ambas redes que la conforman: la de sensores (WSN) y la vehicular (VANET). El fin es intercambiar datos entre sus respectivos nodos. La mayoría de los estudios hacen algunas suposiciones como que los coches ya cuentan con dispositivos GPS, microprocesadores y sensores, así como el uso de un mismo mapa digital en la red completa. Una de las características más importantes es que en los vehículos no hay límite en cuanto al tiempo de vida de baterías, ni en el tamaño de almacenamiento de datos. Algunos resultados sobre dispositivos de redes y sensores para este tipo de red han sido presentados en [14] donde se describen los sistemas de control de tráfico, protocolos de comunicación y el contenido de la información a compartir que han sido utilizados.

Otro estudio [16] se enfoca en proveer seguridad vial y está dirigido a la comunicación Carretera-Coche (R2C, *Road-to-Car*) mediante la utilización de WSNs. Se basa en la implementación de varios sensores a lo largo de la carretera, la cual está dividida en segmentos. Una red de sensores simple obtendrá información sobre el clima, así como otros datos importantes para los coches. Este estudio está enfocado en ofrecer dos servicios diferentes: prevención de accidentes e investigación post-accidente. Esta información podrá ser

usada tanto para salvar vidas como para que los equipos forenses puedan tener una fuente fiable sobre los hechos.

III. CONCEPTOS BASICOS EN UNA HSVN

La principal característica ofrecida en una red vehicular es la capacidad de distribuir información sobre el tráfico y el estado de las carreteras a través de los demás coches que circulan en la carretera. Los nodos que forman parte de una red vehicular serán capaces de tener acceso a diferente información sobre su entorno. Esta información será de gran ayuda para que el protocolo de encaminamiento presente en la VANET pueda tomar una mejor decisión, por ejemplo el detectar vehículos que tengan destinos similares para elaborar una ruta conjunta de transporte de la información que incremente el tiempo de vida de los enlaces. El mecanismo de inundación no es muy funcional, puesto que una red vehicular puede estar formada por un alto número de nodos; el mecanismo de multisalto es usualmente utilizado, ya que permite el despliegue de la información vehículo a vehículo hasta alcanzar el destino deseado, en caso de que el emisor y el destinatario no estén dentro de un mismo rango de transmisión. El transporte público también puede verse involucrado en la comunicación de estas redes, pues los autobuses pueden operar como nodos fiables de la VANET, además de poder ofrecer una conexión a Internet a los coches que circulen cerca.

En la actualidad, la mayoría de los coches modernos ya cuentan con un dispositivo GPS instalado, por ello las aplicaciones instaladas que asisten a los conductores en la conducción, como Tom-Tom [17] o GARMIN [18], son capaces de conocer la posición geográfica y obtener un mapa digital sobre la misma. Esta información actualizada en tiempo real, servirá de apoyo a las aplicaciones de soporte a la navegación, ya que les harán más fácil la tarea de la toma de decisiones, por ejemplo tomar la ruta más segura y menos congestionada. Para la distribución de la información por la red HSVN se plantea el diseño de un protocolo de encaminamiento basado en técnicas *cross-layer*, de tal manera que las diferentes capas de protocolos podrán colaborar en la mejora de la comunicación. Además, el protocolo de encaminamiento deberá ser capaz de adaptarse y reconfigurarse tomando en cuenta parámetros representativos de cada nivel de protocolos, como la calidad del video que recibe el usuario (nivel de aplicación), pérdidas (nivel de red) y retransmisiones (nivel MAC). Asimismo deberá ser capaz de ofrecer QoS para ofrecer información multimedia (por ejemplo *video-streaming*) sobre accidentes o densidad de tráfico, así como datos propios de información sobre la carretera (clima, rutas óptimas, etc.). Otra característica importante a ser mencionada es que los parámetros del sistema se podrían configurar dinámicamente de acuerdo al estado de la red (tráfico, pérdidas, retardos).

Un simple, rápido y eficiente protocolo de comunicación ha de ser desarrollado para permitir la comunicación entre las VANETs y WSNs. Ambas redes deben compartir información sobre el estado de las carreteras y del tráfico en general. El intercambio de esta información deberá producirse de una manera muy veloz, pues el intervalo en que un coche está dentro del rango de transmisión del nodo sumidero (*gateway*) de la WSN es muy corto (ver Figs. 1 y 2). La cooperación entre las redes de sensores y vehiculares permite ampliar el alcance de transmisión de la información sobre seguridad vial. Los vehículos pueden almacenar datos sobre el estado de los distintos segmentos de la carretera y transmitirlos al sumidero de la WSN por la que pasa. Más tarde, si otro coche pasa por esa misma zona, podrá recuperar dicha información del sumidero de la WSN. En la Fig. 1. puede verse un esquema general del sistema global en que se basa una HSVN como la que consideramos en este estudio.

El contenido de los mensajes que se intercambiarán los nodos de la HSVN referentes a la seguridad vial, deberá ser definido. Estos mensajes deben incluir información sobre los diversos segmentos de la carretera (por ejemplo, condiciones climatológicas, localización de accidentes, posibles trabajos en las calles, etc.). Los mensajes podrán incluir una imagen de baja resolución de las intersecciones próximas; de esta manera el copiloto o el conductor podrán dar un vistazo rápido para tener información fiable sobre los lugares donde pasarán próximamente, por si deciden cambiar de intersección. Después de esto, los datos intercambiados entre el sumidero de la WSN y un vehículo en la VANET, deberán ser almacenados o actualizados en sus respectivas bases de datos. Por otra parte, el protocolo que se diseñe deberá manejar varios tipos de intercambios de información (ver Fig. 1), los cuales se describen a continuación:

- El coche que actúa como líder de grupo (coches A y C en la Fig. 1) almacenará la información de los coches que pertenezcan al grupo.
- La información sobre segmentos de carreteras será intercambiada entre los líderes de grupos que circulen en diferentes direcciones (coches A y C en Fig.1).
- La nueva información que reciba el líder del grupo será transmitida hacia todos los miembros de su grupo.
- Los pasajeros tendrán acceso a Internet, mediante AP (*Access Points*) alojados a lo largo de la carretera o a través del transporte público que tenga conexiones a Internet.

A. Modelos de movilidad en VANETs

En un escenario vehicular, los coches no se mueven libremente a través de todo el área. Éstos deben seguir las vías de una carretera, las calles de una ciudad, respetar señales de tráfico y considerar la presencia de otros vehículos. Además, la distribución de estos nodos no es constante, sino que por el contrario los vehículos tienden a crear grupos. Se debe considerar el tipo de carretera en la cual se circula puesto que la mayoría de estos parámetros (número de carriles, velocidad de los nodos, distancia típica de los trayectos, etc.) cambian de un escenario a otro (rural, urbano o autopista). Para poder lograr resultados realistas, todas estas

características deben ser tomadas en cuenta cuando se diseña una HSVN.

Un modelo de movilidad describe el patrón de movimiento que deben seguir los nodos en un escenario específico. Estos modelos de movilidad deben ser incluidos en las simulaciones que se lleven a cabo con el objetivo de analizar el comportamiento de un protocolo de comunicación diseñado para HSVN. También es necesario disponer de un protocolo para difundir la información a través de los nodos en la VANET. Es fundamental que la elección de los parámetros de simulación y del modelo de movilidad sea adecuada e incluya obstáculos, calles, semáforos y señalizaciones propios de un escenario urbano, por ejemplo. Algunos trabajos de investigación, como por ejemplo [19], demuestran lo importante que es considerar un modelo de movilidad realista para VANET para que los resultados que se obtengan con las simulaciones sean fiables y se acerquen lo más posible a escenarios reales.

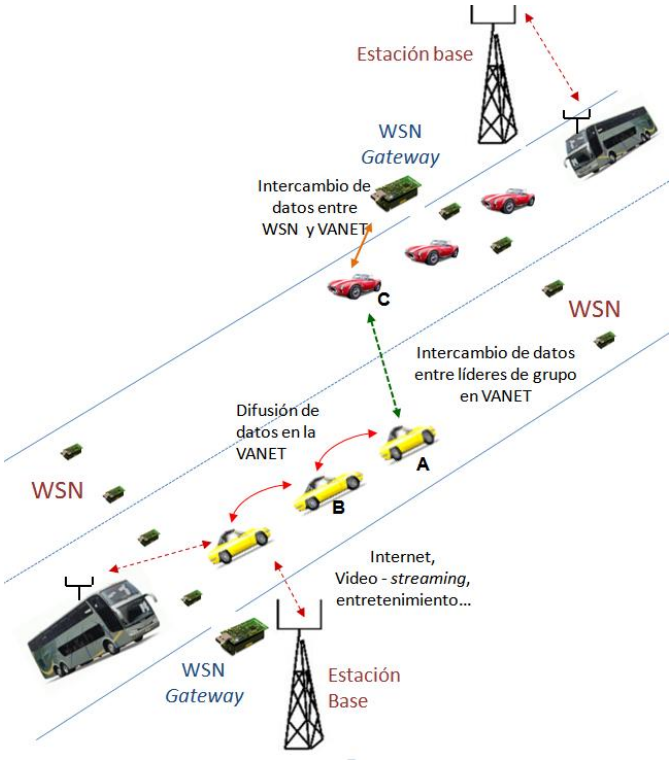


Fig. 1. Escenario general de una HSVN.

B. Propuesta de protocolo de comunicación entre WSNs y VANETs

A continuación se describe el algoritmo de comunicación entre WSNs y VANETs que hemos diseñado. El objetivo principal es cumplir con todos los tipos de comunicación que se puedan producir entre un vehículo y un sensor estático en la carretera. Se presentan tres tipos de comunicación que deben ser considerados entre las WSNs y las VANETs, los cuales se pueden observar en la Fig. 1.

a) Comunicación entre un sensor estático en una WSN y un vehículo en una VANET

WSN → Vehículo:

a.1 El sumidero de la WSN detecta un vehículo dentro de su rango de transmisión.

a.2 El sumidero de la WSN envía una petición de conexión (14 *bytes*) al vehículo que va pasando.

Vehículo → WSN:

a.3 El vehículo envía un ACK (14 *bytes*) al sumidero de la WSN, incluyendo las coordenadas de su destino (20 bits). De esta manera el vehículo establece cuál es la información de su interés. También incluye el identificador ID (20 bits) del grupo al que pertenece el vehículo, si lo hubiere.

WSN → Vehículo:

a.4 Se transmite un paquete que contiene información sobre el estado de la carretera de todos aquellos segmentos que conoce y que están dentro de la ruta del vehículo hasta su destino. Se asume que todos los nodos (coches y sumidero) tienen un navegador consistente (es decir, mismo mapa, mismos segmentos). Asimismo, se incluye información de la carretera de todos los segmentos a otros destinos distintos del destino del propio vehículo, pues esta información puede interesar a otros vehículos. El contenido del paquete contiene la siguiente información:

a.4.1 Por cada segmento de carretera hay un campo de la cabecera (2 bits) que incluye información acerca del estado de la *densidad de tráfico* de dicho segmento. La codificación de datos es: 0=segmento libre, 1=segmento semicongestionado, 2=segmento muy congestionado, 3=n/i (no se tiene información).

a.4.2 Por cada segmento de la carretera hay un campo de la cabecera (2 bits) que incluye información acerca del *estado de la carretera* en dicho segmento. La codificación de datos es: 0=buenas condiciones, 1=hielo, 2=lluvia, 3=accidente.

a.5 Se transmite un paquete que contiene una imagen a baja resolución (50 *kbytes* aproximadamente) del próximo cruce que haya dentro de su trayectoria.

Vehículo → WSN:

a.6 El vehículo envía al sumidero de la WSN información (datos e imágenes) que recolectó previamente de otros vehículos o de otras WSN remotas. En caso de que exista nueva información relacionada al estado de la carretera, el WSN se encarga de actualizar dicha información en su base de datos, esta información es la descrita en a.4.

Vehículo → WSN:

a.7 El vehículo abandona el rango de transmisión del sumidero de la WSN y la conexión termina.

b) Comunicación Vehículo a Vehículo. Vehículos que se mueven en la misma dirección.

Vehículo A → Vehículo B:

b.1 El vehículo B es detectado por el vehículo A dentro de su rango de transmisión. El vehículo B está detrás del vehículo A, misma dirección (ver Fig. 1).

b.2 Una petición de conexión (14 *bytes*) se envía del vehículo A al vehículo B.

Vehículo B →Vehículo A:

b.3 Un ACK (14 *bytes*) es enviado como respuesta del vehículo B al vehículo A. Esto incluye el ID del grupo (identificación, 20 bits). Además de las coordenadas de su destino.

Vehículo A → Vehículo B:

b.4 Se transmite información de la carretera relativa a todos aquellos segmentos que están dentro de la ruta del vehículo B hasta su destino y también información de la carretera relativa a los caminos que tengan otras rutas. El contenido del paquete contiene la siguiente información:

b.4.1 Ver a.4.1.

b.4.2 Ver a.4.2.

b.5 Se transmite un paquete que contiene una imagen a baja resolución (50 *kbytes* aproximadamente) del próximo cruce que haya dentro de su trayectoria.

Vehículo A → Vehículo B:

b.6 Vehículo A sale del límite de cobertura del vehículo B y la comunicación termina.

c) Comunicación Vehículo a Vehículo. Vehículos que se mueven en direcciones opuestas.

Vehículo A en una dirección → Vehículo C en la dirección opuesta (ver Fig. 1).

c.1 En el caso de detectar un vehículo en la dirección opuesta, la conexión se establece solo por los primeros vehículos de cada grupo (líder de grupo). La comunicación entre el vehículo A y el vehículo C será como se describe en b); desde b.1 a b.6

c.2 Cada líder de grupo difunde la nueva información de la ruta dentro de su grupo.

Hemos hecho algunas consideraciones relacionadas con la cantidad de información necesaria para poder comunicar el estado del camino para todos los segmentos que pertenecen al trayecto de un mismo destino. Básicamente, el número de segmentos sobre los cuales hay que enviar información depende del tipo de escenario (urbano, rural, autopista) y de la distancia que exista hasta el destino. Por ejemplo, en el caso de una *autopista* cuya distancia hasta un destino típicamente sea de 500 km y los segmentos del camino (localizados en las salidas de la autopista) tengan una distancia de unos 10 km, en promedio existirán 50 segmentos por destino. En caso de que el escenario sea una *carretera*, con una distancia hasta el destino de unos 50 km y los segmentos de unos 5 km de longitud, serán entonces 10 segmentos por destino. Finalmente, en los escenarios de *ciudad* donde las distancias promedios de los viajes son de 5 km, los segmentos serán de 200 m y el total de segmentos serían 25 por trayecto medio. En resumen el número de segmentos dependiendo el tipo de escenario queda de la siguiente manera:

- Autopista, 500 km trayecto total, 50 segmentos.
- Carretera, 50 km trayecto total, 10 segmentos.
- Ciudad, 5 km trayecto total, 25 segmentos.

A continuación presentamos unos cálculos sobre la cantidad de información que intercambian los nodos ad hoc de una HSVN y el tiempo disponible que tienen vehículos y nodos sensores para proceder con dicho intercambio. Nos centraremos primero, a modo de ejemplo, en el escenario *carretera*, siendo los cálculos similares para los escenarios *autopista* y *ciudad*. En un sólo paquete de 1000 octetos (tamaño de los paquetes transmitidos que hemos utilizado) es posible codificar hasta 1995 segmentos (1995 = (1000*8-20bits_ID) / 4bits_cabecera). Para un desplazamiento en carretera, un intercambio típico entre el sumidero de una WSN y un coche perteneciente a la VANET incluirá información acerca de 10 segmentos correspondientes a la información del destino de interés de ese vehículo. Cabe mencionar que existe espacio disponible dentro de un mismo paquete para incluir información acerca de 198 destinos más en *carretera*, donde 198=[(1995-10)/10]. En una *autopista*, un paquete puede llevar información acerca de 40 destinos (1995/50) y en un entorno de *ciudad* aproximadamente acerca de 80 destinos (1995/25).

- Autopista, información de 40 destinos por paquete.
- Carretera, información de 198 destinos por paquete.
- Ciudad, información de 80 destinos por paquete.

Cada vehículo transmite una señal guía (*beacon*) cada 10 mseg con el fin de que los demás nodos dentro de la red ad hoc estén percatados de ellos. Cuando un vehículo se encuentra fuera del rango del nodo sumidero de la WSN no recibirá las señales guía, por lo que el nodo sumidero dejará de enviarle información. El MAC IEEE 802.11b posee un enlace del ancho de banda de carácter nominal de 11Mbps, y un *throughput* aproximado de *th*=7Mbps (para tráfico tipo UDP).

Estos valores corresponden al MAC IEEE 802.11.b, ya que es el utilizado en las simulaciones de este trabajo al ser el MAC implementado actualmente en el simulador elegido para probar nuestra primera propuesta en un escenario general. En un futuro se pretende trabajar con el MAC 802.11.p, más específico para entornos vehiculares. De todos modos, el protocolo de comunicaciones diseñado en este trabajo funciona independientemente del MAC, sea IEEE802.11b o IEEE802.11p.

Hemos considerado una velocidad máxima de v (km/h) y un rango de transmisión del nodo sumidero de r (m). El tiempo disponible para el intercambio de información entre vehículo y nodos sumidero de la WSN es por tanto de $T_{disponible}=2r/v$ (seg.). Para los tres escenarios considerados, y un radio de cobertura del nodo sumidero de r =80m, esto nos da unos tiempos disponibles para la transacción de la información de:

- Autopista, v=120 km/h, $T_{disponible}=2r/v$=4,8 seg.
- Carretera, v=80 km/h, $T_{disponible}=2r/v$=7,2 seg.
- Ciudad, v=50 km/h, $T_{disponible}=2r/v$=11,52 seg.

Durante este tiempo la comunicación se establece y la transmisión de todos los paquetes deberá tener lugar, de acuerdo al intercambio de mensajes descrito en el punto *a* del protocolo de comunicación. Se enviará la información relacionada a los segmentos del trayecto en un simple paquete de tamaño p=1000 *bytes*, el cual tarda $T_{segmentos\_camino}=p/th$=1,14 ms en enviarse. Son necesarios 50

paquetes para enviar una imagen de 50 *kbytes*, que tarda en enviarse T_{imagen}=0,057 seg. (50 *kbytes*/7Mbps). Entonces, el tiempo total necesario para enviar dicha información es $T_{requerido}=T_{segmentos\ camino}+T_{imagen}$=0,058 sec. Todo intercambio de información (datos e imágenes) entre el coche y el sensor sumidero de la WSN ha de producirse tal que $T_{requerido}<T_{disponible.}$ De los números anteriores, vemos que sí es posible. La ilustración de estos intervalos se halla en la Fig. 2. Además, se podrán enviar más imágenes de otras intersecciones posteriormente, puesto que todavía hay tiempo hasta final de cobertura.

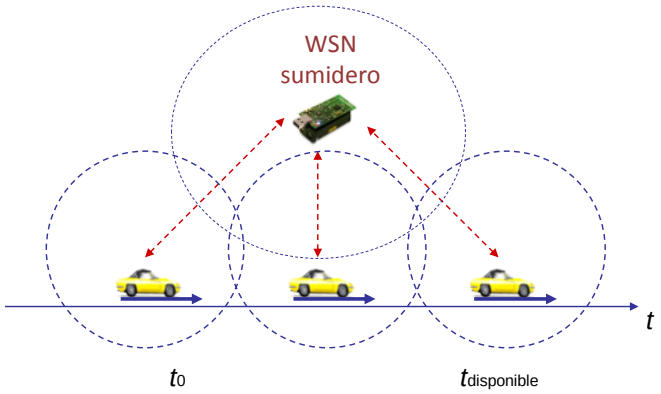


Fig. 2. Intercambio temporal disponible para intercambiar mensajes.

IV. SIMULACION Y RESULTADOS

Para validar el protocolo de comunicación propuesto entre WSNs y VANETs, se han realizado varias simulaciones de la transmisión de datos entre diferentes nodos en una HSVN. Se ha utilizado el Simulador libre NCTUns en su versión 6.0 (*National Chiao Tung University Network Simulator*) [20].

Se ha trabajado con un escenario simple (un nodo sumidero y un grupo de cuatro coches), el cual asume que el sumidero ya cuenta con la información que han monitorizado los diferentes sensores que pertenecen a la WSN. En las simulaciones el sumidero envía paquetes de datos del segmento al último coche del grupo. Para ello, los otros coches del grupo funcionan como ruta de transmisión del protocolo de encaminamiento. Los coches están separados entre sí por una distancia de 130 metros.

Los nodos móviles cuentan con el programa *CarAgent*, presente en el simulador, el cual permite que los nodos sigan la carretera diseñada. Se han modificado las velocidades de los coches, los tamaños de los paquetes y el protocolo de encaminamiento para poder observar el comportamiento de la red. Se ha analizado la pérdida de paquetes bajo dos protocolos de encaminamiento y con diferentes parámetros antes mencionados. Estos parámetros se listan en la Tabla 1.

En las simulaciones comparamos el comportamiento del protocolo AODV [21] con respecto al DSR [22] en términos de paquetes perdidos. Los protocolos utilizados son DSR y AODV, los dos son protocolos reactivos, pero que difieren en el hecho de que DSR incluye en la cabecera del paquete la lista de todos los nodos por los que debe pasar para llegar a su destino. En AODV el paquete solo incluye la dirección destino y la dirección del próximo salto a seguir, además de utilizar una pequeña tabla de encaminamiento de nodos vecinos. Hemos utilizado estos protocolos por ser los que están implementados en el simulador, NCTuns. Como fruto de la evaluación de prestaciones con cada uno de ellos bajo diferentes condiciones y escenarios, podremos comprobar cuál de ellos es más adecuado para posteriormente ser modificado y adaptado a VANETs en un trabajo futuro.

Además presentamos un intervalo de confianza del 80% para los valores obtenidos, donde se realizaron 5 simulaciones por escenario. En la Fig. 3 se puede ver la evolución de la pérdida de los paquetes usando el protocolo AODV. En la Fig. 4 se observan la pérdida de paquetes con el protocolo DSR. De acuerdo con los resultados puede observarse que AODV tiene un buen comportamiento en el caso de velocidades bajas (menores a 80km /h), por lo cual sería un protocolo ideal en caso de ser usado en escenarios de ciudad donde las velocidades suelen ser moderadas. En el caso del protocolo DSR, presenta una baja tasa de pérdidas en comparación con AODV en el caso de utilizar altas velocidades. Esto usando paquetes de 1000 octetos que producen menos pérdidas.

Tabla 1. Parámetros de simulación

Velocidad de los nodos	40 a 80 km/h
Número de carriles en la vía	4 (dos en cada dirección)
Tamaño de la carretera	2 km
Número de nodos móviles en la VANET	4
Número de nodos en la WSN	1 nodo sumidero
Rangos de transmisión	200 m
Protocolo de encaminamiento en la HSVN	AODV y DSR
Tamaño de paquetes	500, 1000 y 1500 octetos
Tiempo de simulación	80 segundos
Transmisión de datos	1Mbps
MAC	IEEE 802.11b
Capacidad nominal	11 Mbps

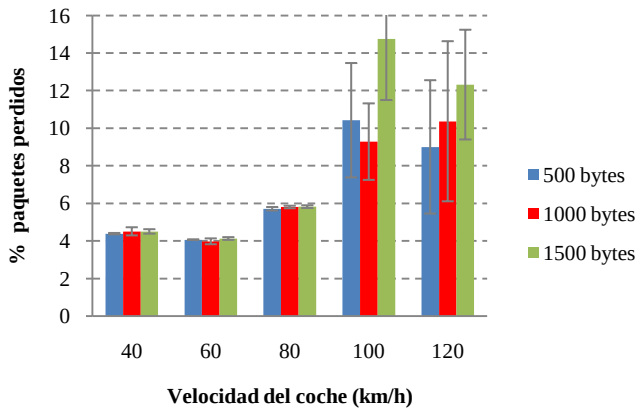


Fig. 3. Evolución de pérdida de paquetes para AODV.

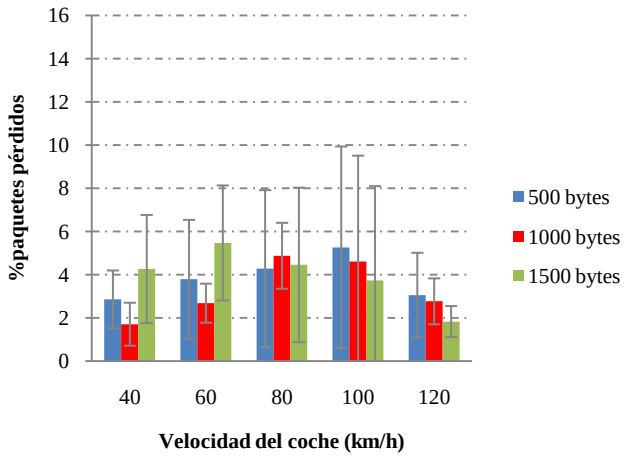


Fig. 4. Evolución de pérdida de paquetes para DSR.

V. CONCLUSIONES Y TRABAJO FUTURO

En este artículo se ha mostrado el comportamiento en cuanto a la pérdida de paquetes de los protocolos AODV y DSR en una HSVN que incluye la propuesta del protocolo de comunicación entre WSN y VANET. El resultado de la simulación muestra la eficacia de AODV para escenarios de bajas velocidad (ciudad) y DSR en escenario de altas velocidades (autopista).

Como trabajo inmediato se realizará el análisis de este mismo escenario pero bajo otros protocolos de encaminamiento GSR (*Geographic Source Routing*) [23], SAR (Spatial Aware Routing) [24], VADD (*Vehicular Assisted Data Delivery*) [25]. También procederemos a evaluar el comportamiento de la VANET usando el estándar MAC IEEE 802.11p específico para este tipo de redes. Además de enfocarnos en el desarrollo de un protocolo de encaminamiento propio *cross-layer* que ofrezca QoS, y poder comparar sus prestaciones con los resultados anteriores.

AGRADECIMIENTOS

Éste trabajo ha tenido el apoyo del Ministerio Español de Ciencia y Educación bajo los proyectos ITACA (TSI2007-65393-C02-02) y CICYT CONSEQUENCE (TEC2010-20572-C02-02). C. Tripp Barba contó con el apoyo de la Comisión para las Universidades e Investigación del DIUE de la Generalitat de Catalunya y del Fondo Social Europeo con la beca FI-Agaur y del programa Doctores Jóvenes en Áreas Estratégicas de la UAS (Universidad Autónoma de Sinaloa, México). Asimismo, G. Díaz-Delgado ha contado con el apoyo de becas de CONACYT, PROMEP UAQ, México y Fundación Carolina, España. Finalmente los autores desean agradecer a los revisores sus comentarios que fueron un gran aporte.

REFERENCIAS

[1] C. Siva Ram Murthy, B.S. Manoj. “Ad Hoc Wireless Networks: Architectures and Protocols”. June 3, 2004 ISBN: 978-0131470231.

[2] H. Hartenstein, K. Laberteaux. “VANET Vehicular Applications and Inter-Networking Technologies (Intelligent Transport Systems)”. Wiley, March 2010. ISBN: 978-0470740569

[3] K. Sohraby, D. Minoli, T. Znati. “Wireless Sensor Networks: Technology, protocols and applications”. Wiley Interscience, 2007. ISBN: 978-0-471-74300-2.

[4] S. Olariu, M. Weigle. “Vehicular Networks from Theory to Practice”. Norfolk Virginia, USA. Chapman and Hall, 2009. ISBN: 978-1420085884.

[5] B. Hofman-Wellenhof, H. Lichtenegger, J. Collins. “Global Positioning System: Theory and Practice”. Springer, 2001. 5th Ed. ISBN: 3211835342.

[6] D. Jiang, L. Delgrossi. “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environment”. 67th IEEE Vehicular Technology Conference VTC. Singapore, 2008.

[7] C2C. Car-To-Car Communication Consortium. http://car-to-car.org/.

[8] CVIS. Cooperative Vehicle-Infrastrucure Systems http://www.cvisproject.org/

[9] CARLINK. Wireless Traffic Service Platform for Linking Cars. http://carlink.lcc.uma.es/.

[10] COME. Co-operative Intelligent Road Transport Systems: Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications. http://www.comesafety.org/.

11] eSafety Forum. [Online] http://www.esafetysupport.org/

[12] INFOTRANSIT. Reial Automòbil Club de Catalunya (RACC). http://infotransit.es.

[13] Google Maps. http://maps.google.com/.

[14] F. Kong, J. Tan. “A Collaboration-based Hybrid Vehicular Sensor Network Architecture”. IEEE International Conference on Information and Automation. Zhangjiajie, China, 2008.

[15] E. Weingärtner, F. Kargl. “A Prototype Study on Hybrid Sensor Vehicular Networks”. 6 KuVS Fachgespräch Sensornetzwerke, RWTH-Aachen Technical Report, no. AIB 2007-1, Aachen, Germany. 2007.

[16] J. Bohli, O. Ugus, D. Westhoff. “A Secure and Resilient WSN Roadside Architecture for Intelligent Transport System”. ACM Workshop on Wireless Security. Alexandria, Virginia, USA, 2008.

[17] TomTom. http://www.tomtom.com/.

[18] GARMIN. http://www.garmin.com/garmin/cms/site/es.

[19] D. Djenouri, E. Nekka, W. Soualhi. “Simulation of Mobility Models in Vehicular Ad hoc Networks”. 1st ICST Int. Conf. On Ambient Media and Systems (Ambi-sys). Quebec, Canada, 2008. ISBN: 978-9639799165.

[20] NCTUns 6.0 (Network Simulator and Emulator). 2010. http://nsl.csie.nctu.edu.tw/nctuns.html.

[21] Ad hoc On-Demand Distance Vector (AODV) Routing. http://www.ietf.org/rfc/rfc3561.txt

[22] The Dynamic Source Routing Protocol (DSR. http://www.rfc-editor.org/rfc/rfc4728.txt

[23] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Hermann, M. Mauve. "A Routing Strategy for Vehicular Ad Hoc Networks in City". IEEE Intelligent Vehicles Symposium '03, pp. 156-161. 2003.

[24] J. Tian, L. Han,K. Rothermel. "Spatially Aware Packet Routing for Mobile Ad Hoc Inter-Vehicle Radio Networks". IEEE Intelligent Transportation Systems, Shanghai, pp. 1546-1551. China, 2003.

[25] J. Zhao, J. Cao. "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks". 25th IEEE International Conference on Computer Communications, pp.1-12. INFOCOM 2006.

MEJORAS DEL RENDIMIENTO CON EL DISEÑO CROSS-LAYER PARA LOS SERVICIOS DE SEGURIDAD.

Antonio Urbano Fullana[1], Josep Lluís Ferrer Gomila[2] y Magdalena Payeras Capellà[3]
Universitat Illes Balears,
Dept. Matemáticas e Informática,
Ctra. Valldemossa, Km 7,5. 07120, Palma
e-mail antonio.urbano@uib.es[1] jlferrer@uib.es[2] mpayeras@uib.es[3]

***Resumen*—Los servicios tradicionales sobre redes cableadas deben ser capaces de operar, en la actualidad, sobre redes inalámbricas. A los mecanismos de seguridad existentes en las capas del modelo TCP/IP, se añaden los mecanismos de seguridad de capa MAC y por tanto se generan duplicidades e incluso multiplicidades en el cifrado de la información.**

La aplicación de mecanismos de cifrado en redes inalámbricas consume recursos de los dispositivos en los que se implementan como son, memoria, CPU y energía de la batería. Los recursos disponibles en un terminal inalámbrico son limitados y la utilización de mecanismos de cifrado eficientes pueden mejorar el rendimiento global del dispositivo. Las redes de área local 802.11, son un ejemplo donde dispositivos inalámbricos utilizan sus recursos para acceso a redes y servicios y en particular a Internet. En estas redes, en modo infraestructura, es el punto de acceso (AP) el elemento que concentra el tráfico de los dispositivos de una determinada área. La carga en tareas de cifrado y descifrado en el punto de acceso repercute en los tiempos de proceso disminuyendo el rendimiento en términos de capacidad de transmisión por usuario. Este hecho se agrava al aumentar los usuarios a los que da cobertura el AP.

En [1] se analizan los servicios de seguridad en la arquitectura TCP/IP sobre redes IEEE 802.11, se describe la incidencia de los mecanismos de cifrado sobre la cantidad total de octetos cifrados y finalmente se propone una solución que elimina la redundancia en el cifrado de determinados octetos. En el artículo que aquí se presenta se propone un algoritmo basado en el diseño Cross-Layer que implemenmta la solución propuesta en [1] para eliminar la redundancia en el cifrado de la información en las diferentes capas. También analizamos el rendimiento en términos de energía consumida y ancho de banda global realizando una comparativa entre los resultados obtenidos al aplicar la solución Cross-Layer y los resultados obtenidos cuando no la aplicamos.

Keywords: Wireless Security, Security Protocols, Cross-Layer, WEP, IPSEC, 802.11.

I. INTRODUCTION.

Las operaciones de cifrado y descifrado consumen tiempo de procesador y recursos de memoria en los equipos en los que se ejecutan. Existe una relación entre el número de octetos cifrados y el rendimiento en términos de energía consumida y la capacidad de transmisión por cliente. Al disminuir el número de octetos que deben ser cifrados, un cliente inalámbrico disminuye el consumo de energía. Si reducimos los datos cifrados en el AP, éste disminuye el tiempo de proceso por lo que aumenta el rendimiento global. La propuesta presentada en [1] para reducir el número de octetos cifrados consiste en que las capas inferiores no cifrarán aquellos octetos que lo han sido en capas superiores. Esto implica que las capas inferiores deben conocer que octetos han sido cifrados y por tanto deben conocer los mecanismos de seguridad implementados en capas superiores, sobre qué parte de la información se realiza y en base a estos datos pueden decidir cómo implementar el cifrado local de capa. El diseño Cross-Layer (CL) propone una estructura en la que las distintas capas pueden intercambiar información, por lo que su utilización soluciona el problema del intercambio de información de seguridad entre estas capas.

Este artículo se organiza como sigue. En la sección II describimos el análisis de los servicios de seguridad realizado en [1] y en particular la redundancia producida en el cifrado de la información. La seccion III introduce el diseño Cross-Layer, basado en la comunicación entre capas. En la seccion IV se resumen aspectos del consumo de energía en terminales inalámbricos y del rendimiento en los puntos de acceso. El análisis, en términos de energía consumida e impacto sobre el rendimiento, comparando los costes de cifrado original con los costes del cifrado aplicando nuestra propuesta se realiza en V. En las secciones VI y VII presentamos un algoritmo basado en el diseño Cross-Layer para gestionar el cifrado de capa y que considera los mecanismos de cifrado de capas superiores. Las conclusiones y el trabajo futuro se presentan en la seccion VIII.

II. TRABAJO PREVIO.

En esta sección describimos el análisis de los servicios de seguridad realizado en [1] así como la propuesta para eliminar la multiplicidad en el cifrado de los datos.

En [1] se demuestra que al aplicar mecanismos de seguridad en diferentes capas se produce una redundancia en el cifrado de determinados octetos. Para ello se estudia un escenario donde un usuario A, que pertenece a una red inalámbrica que implementa el mecanismo de cifrado WEP, desea acceder a un servidor S a través del protocolo HTTPS.

En este escenario el servidor S pertenece a una empresa que requiere conexiones VPN. Por tanto los mecanismos de seguridad que implementa el terminal inalámbrico son SSL a nivel de tranporte, IPSEC, en su formato ESP en modo túnel, a nivel IP y WEP a nivel MAC. La red 802.11 del escenario es una red en modo infraestructura gestionada por un punto de acceso (AP) que también implementa WEP a nivel MAC.

En el trabajo anteriormente mencionado se analiza el encapsulado de los datos de aplicación hasta formar la trama 802.11 incluyendo los servicios de seguridad de capa (SSL, IPSEC y WEP) y los protocolos HTTP, TCP e IP. También se presentan datos de la redundancia producida por el cifrado de la información en cada uno de los mecanismos de seguridad de capa y se propone un esquema para modificar los octetos cifrados en función del parámetro Profundidad de Cifrado (PC), definido como el número de veces que se cifra un octeto. Los algoritmos de cifrado estudiados en [1] son RC4 para los protocolos SSL y WEP, y 3DES para el cifrado en el protocolo ESP en modo túnel (IPSEC). De los resultados indicados en [1] se extrae que para una longitud de datos L, la arquitectura TCP/IP tradicional cifrará (NxL)+K octetos y como alternativa a esta duplicidad de cifrado, se presenta una solución que reduce el número de octetos cifrados a L+K', siendo N el número de mecanismos de cifrado aplicados, L la longitud de datos y, finalmente, K y K', variables que dependen de la sobrecarga de los mecanismos de cifrado utilizados en el cifrado original, K, y al aplicar la solución presentada, K'. La tabla I resume los valores de N, K y K' en función de los mecanismos de cifrado utilizados y la figura 1 representa las rectas que se obtienen al variar el valor de L. En las gráficas se indican los resultados correspondientes al cifrado sin aplicar la solución propuesta sin referencia y referenciados como "CL" los resultados obtenidos al aplicar la solución propuesta.

Longitudes de cifrado					
Cifrado	N	K	K'	(NxL)+K	L+K'
SSL+IPSEC+WEP	3	206	125	3L+206	L+125
IPSEC+WEP	2	148	104	2L+148	L+104
SSL+WEP	2	89	73	2L+89	L+73

Tabla I
VALORES DE N, K Y K'.

III. EL DISEÑO CROSS-LAYER.

El diseño Cross-Layer se fundamenta en la posibilidad de que las diferentes capas del modelo OSI intercambien información. Este diseño tiene especial interés en redes inalámbricas donde la comunicación entre capas aporta beneficios frente a una estructura en capas tradicional. Diversos autores analizan y presentan soluciones basadas en el diseño Cross-Layer [10], [21], [19]. En [4] se define el plano de seguridad, como plano de coordinación Cross-Layer, indicando las desventajas del cifrado en diferentes capas. La aplicación de Cross-Layer en la seguridad de los datos se analiza en [22] y [23] centrando su análisis en la detección de intrusos y en la detección de

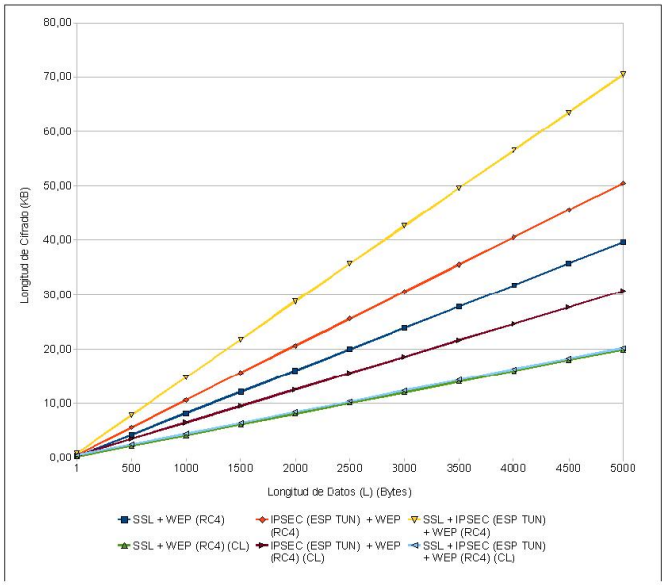


Figura 1. Longitud de Cifrado

ataques de jamming en redes ad-hoc, respectivamente. Según nuestro conocimiento, ningún autor ha estudiado el problema aquí planteado.

IV. ENERGÍA Y RENDIMIENTO.

La aplicación de mecanismos de cifrado aumenta el coste computacional y por tanto aumenta el tiempo de proceso y el consumo de energía en los terminales inalámbricos. El consumo de energía del algoritmo de cifrado RC4 se estudia en [14], de donde se extrae (ver figura 5 de [14]) que el consumo por octeto para cifrar y descifrar mediante el algoritmo RC4 y referenciado a una PDA iPAQ H3670, equivale a 3.93 uJ/octeto. En [15] se cuantifica el consumo de energía producido por el cifrado de datos mediante el algoritmo RC4 y referenciado a un procesador INTEL Pentium 700 Mhz. El consumo debido al cifrado en IPSEC se analiza en [6] y [14], donde, referenciado a una PDA iPAQ H3670, el consumo debido al cifrado 3DES es de 6,04 uJ/octeto (ver figura 5 de [14]). La tabla II resume los consumos de energía por octeto de información cifrada indicados anteriormente.

El efecto producido por los mismos mecanismos de cifrado en un punto de acceso que concentra a varios terminales, repercute sobre el rendimiento del conjunto. A medida que aumenta el número de terminales inalámbricos, el punto de acceso aumenta las operaciones de cifrado y descifrado, aumentando el retardo de proceso y disminuyendo el rendimiento por usuario. El análisis del rendimiento de los protocolos y mecanismos de seguridad que operan sobre redes 802.11 se analiza en [2], [3], [24] y [8] y el análisis teniendo en cuenta el sistema operativo se estudia en [12]. En [5], [13], [9] y [17], se analiza el rendimiento y coste de implementar IPSEC. En [11] se analiza el rendimiento de implementar DES y 3DES tomando como métrica la longitud de los datos de entrada (ver tablas 1 a 4 de [11]). Aplicando el algoritmo 3DES en modo cifrado de bloques y sobre una máquina Pentium IV 2.4 Ghz, la velocidad media para

Energía consumida por RC4.		
Arquitectura	Cifrado	Energía
iPAQ H3670	IPSEC (3DES)	6,04 uJ/octeto
iPAQ H3670	WEP (RC4)	3,93 uJ/octeto
INTEL PENTIUM 700 Mhz PAYLOAD: 10000 B	WEP (RC4)	0,005 uJ/octeto
INTEL PENTIUM 700 Mhz PAYLOAD: 1400 B	WEP (RC4)	0,005 uJ/octeto
INTEL PENTIUM 700 Mhz PAYLOAD: 1000 B	WEP (RC4)	0,005 uJ/octeto
INTEL PENTIUM 700 Mhz PAYLOAD: 100 B	WEP (RC4)	0,015 uJ/octeto
INTEL PENTIUM 700 Mhz PAYLOAD: 50 B	WEP (RC4)	0,055 uJ/octeto

Tabla II
DETALLE DE ENERGÍA CONSUMIDA POR 3DES, RC4 EN IPAQ H3670 E INTEL PENTIUM 700 MHZ

operaciones de cifrado y descifrado es de 2663 octetos/seg (ver tabla 2 [11]).

En [24], [13] y [20] se analizan, entre otros, el rendimiento y coste de implementar WEP en redes 802.11. En [16] se analiza el *throughput* en Mbps para cifrar datos mediante el algoritmo RC4 en función de la frecuencia de la CPU. El coste de cifrado RC4 en la arquitectura INTEL Pentium es de 7 ciclos de CPU por octeto [18]. En [24] observamos la influencia del número de nodos en los tiempos de cifrado WEP. La dependencia de la distancia entre nodos, la ubicación de los mismos y de sus características se analiza en [7]. La tabla III resume los valores, indicados anteriormente, de retardo y throughput producidos por el cifrado.

V. ANÁLISIS GLOBAL.

Las modificaciones propuestas en [1] reducen significativamente el número de octetos que deben cifrarse. Podemos evaluar teóricamente las mejoras que se producen desde el punto de vista de rendimiento y coste de implementación. El análisis del rendimiento debe realizarse en el nodo móvil y en el punto de acceso (AP). Desde el punto de vista del terminal inalámbrico, cualquier reducción de la longitud de datos a cifrar implica un menor consumo de recursos que equivale a un menor consumo de energía y por tanto a un mayor tiempo de duración de la batería. Desde el punto de vista del punto de acceso, la disminución de la carga de cifrado, equivale a un descenso del número de operaciones que realiza en un intervalo de tiempo y por tanto a un aumento del rendimiento del conjunto.

La propuesta de [1], considerando SSL, IPSEC y WEP, modifica la longitud de cifrado de ((3xL)+206) a (L+125) octetos, siendo L la longitud de los datos en capa de aplicación. Con este resultado y basándonos en los artículos y resultados indicados en la sección IV, podemos calcular los costes en energía y rendimiento para una PDA iPAQ H3670 y una arquitectura basada en el procesador INTEL Pentium 2,4 Ghz.

En este artículo definimos el parámetro tamaño de fichero que corresponde a la longitud de los datos de usuario. Este valor difiere del parámetro L, que en [1] se define con un valor menor que el tamaño máximo de segmento a nivel TCP. Los datos de usuario definidos por el tamaño máximo de fichero se dividen en bloques de longitud L para ser tratados en capas inferiores.

V-A. Análisis del consumo de energía.

Los datos presentados en el apartado IV referencian el consumo de energía del algoritmo RC4 y los algoritmos 3DES/SHA1 implementados en una PDA iPAQ H3670. El consumo por octeto del cifrado mediante RC4 y 3DES es de 3,93 uJ/octeto y 6,04 uJ/octeto respectivamente. Estos datos nos permiten evaluar el coste, en términos de energía, de los mecanismos de cifrado actuales así como del ahorro que supone la solución presentada en [1].

La figura 2 representa el consumo de energía en la implementación de los algoritmos 3DES y RC4 en una PDA iPAQ H3670, a partir de los datos presentados en [14] y en función de los datos de aplicación (L).

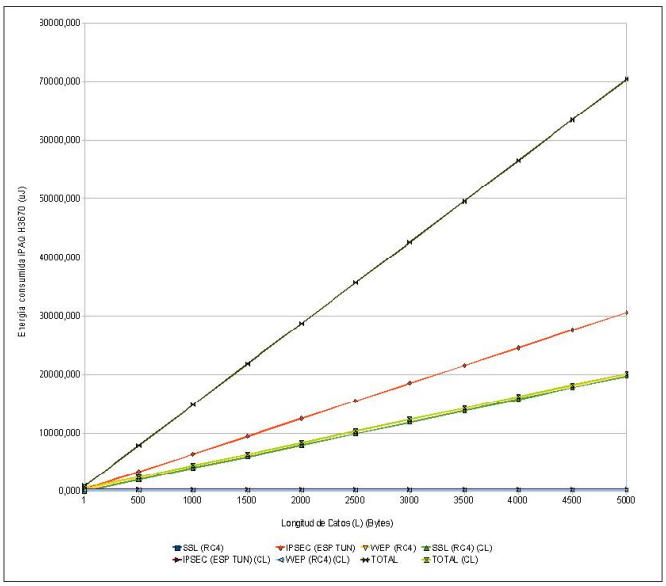


Figura 2. Consumo de energía por algoritmo.

De los datos técnicos de la PDA iPAQ H3670 obtenemos que la batería que incorpora tiene una capacidad de 950 mAh y suministra una tensión de 3.7 V. La figura 3 representa el consumo en mAs de los algoritmos de cifrado utilizados en función del tamaño de archivo a transmitir, comparando el consumo original con el resultante de aplicar la solución Cross-Layer presentada.

Rendimiento de RC4.					
Arquitectura	Cifrado	Capacidad de cifrado	Tiempo 100 octetos	Tiempo 700 octetos	Tiempo 1400 octetos
INTEL Pentium IV 2,4 Ghz	3DES	2663 Bps	0,0375s	0.263s	0,526s
INTEL Pentium	RC4	7 ciclos/Octeto			
INTEL Pentium IV 2,4 Ghz	RC4		29,17 ms	2,04 ms	4,08 ms

Tabla III
DETALLE DE RENDIMIENTO DE RC4 Y 3DES EN ARQUITECTURA INTEL.

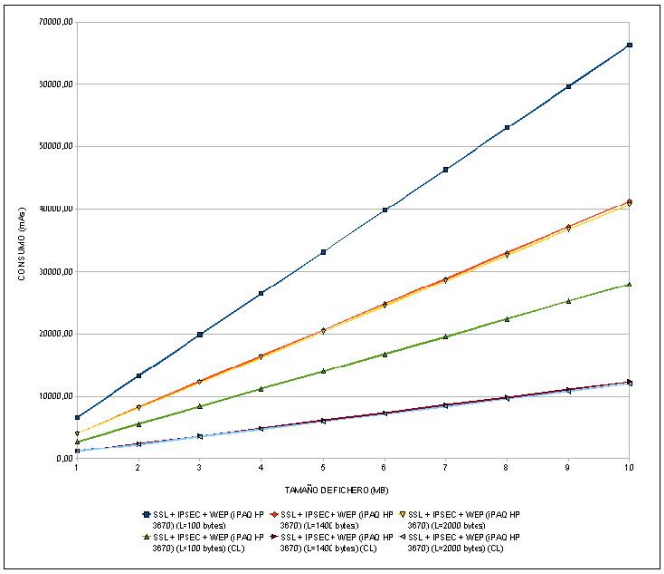


Figura 3. Consumo de energía total en mAs.

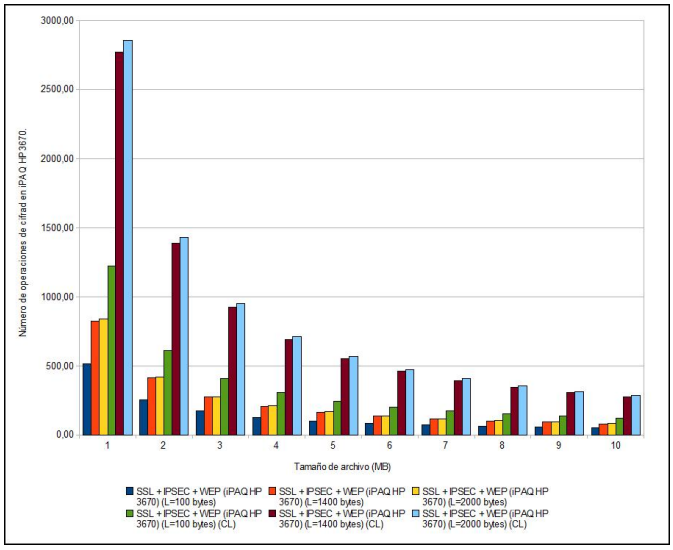


Figura 4. Número de operaciones de cifrado.

La figura 4 representa el número de operaciones de cifrado, en función del tamaño de fichero, que se puede realizar con una PDA iPAQ H3670 con una batería de 950 mAh y las compara con las que se pueden realizar al aplicar la propuesta Cross-Layer. La solución presentada permite que la PDA, al aplicar el diseño Cross-Layer, incremente el número de operaciones que puede realizar o que la batería tenga una tiempo de vida mayor, con valores de 237 % para L=100 octetos, 335 % para L=1400 octetos y 340 % para L=2000 octetos.

Si consideramos el consumo de energía de un terminal inalámbrico debido exclusivamente a las operaciones de cifrado de datos, podemos realizar una estimación del tiempo de vida de la batería. En este caso, si la batería tiene una capacidad de 3420000 mAs (950 mAh), el consumo total en función de la capacidad de transmisión de datos de un terminal, se representa en la figura 3 y el tiempo de vida estimado de la batería en función de la capacidad de transmisión se representa en la figura 5.

De los datos presentados, comprobamos que el consumo de energía de la solución Cross-Layer propuesta es el 42 % del consumo necesario al no aplicarla, si L=100 octetos. Para L=1400 y L=2000 octetos, el consumo de energía se reduce a un 30 % y 29 % respectivamente. Para una transmisión de datos constante de 1 MBps y considerando L=1400 octetos, se necesitan 4130,89 mAs de energía y la duración de la batería considerada (3420000 mAs) es de 0,23 horas. Si aplicamos la solución Cross-Layer presentada, la energía necesaria es de 1234,13 mAs y la duración de la misma batería es de 0,77 horas.

V-B. Análisis del rendimiento.

El nodo que concentra el tráfico de la red inalámbrica es el punto de acceso, que implementa seguridad en la capa MAC y por tanto sólo verá afectado su rendimiento por la aplicación de mecanismos de cifrado a nivel MAC (en nuestro escenario RC4). Por otra parte el terminal inalámbrico implementa seguridad en las capas de transporte, IP y MAC, y, por tanto, su rendimiento se verá afectado por los mecanismos de cifrado de dichas capas. En el apartado IV hemos presentado datos y artículos que analizan el rendimiento de los mecanismos de cifrado, tomando como métrica el tamaño de fichero que debe cifrarse. Al aplicar

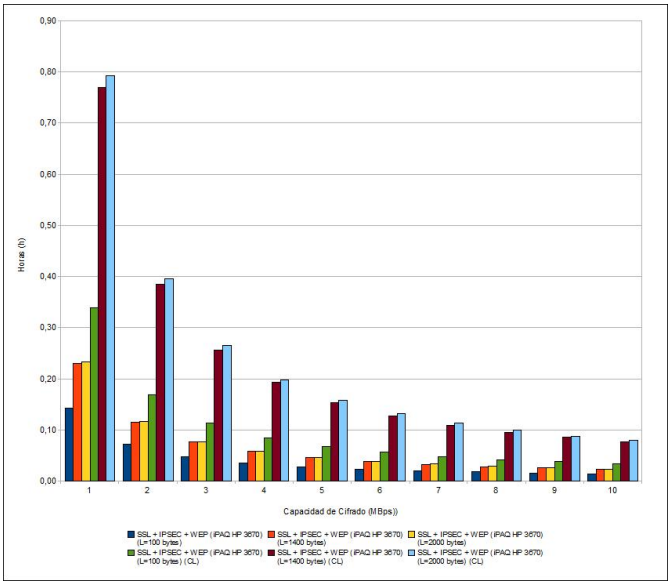


Figura 5. Duración de la batería para diferentes tamaños de archivo.

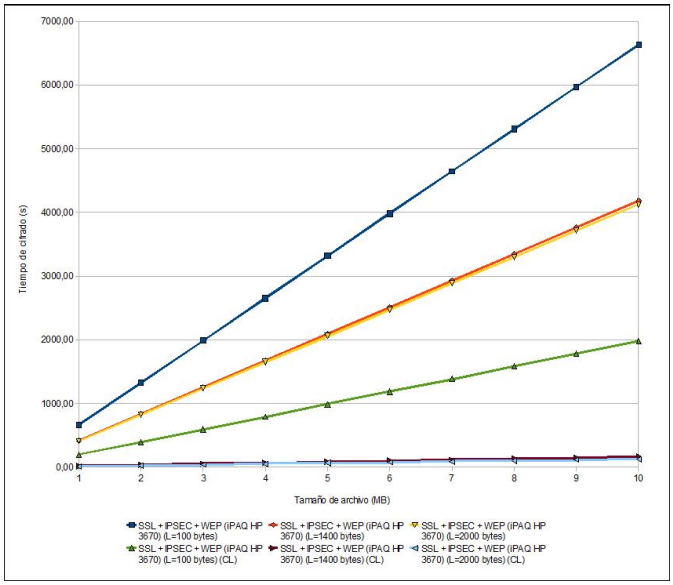


Figura 7. Tiempos de cifrado en los terminales inalámbricos.

estos datos obtenemos la figura 6 que representa el tiempo de cifrado de los algoritmos considerados en [1] y que son RC4 (utilizado en WEP y SSL) y 3DES (utilizado en IPSEC) en función de la longitud de datos (L).

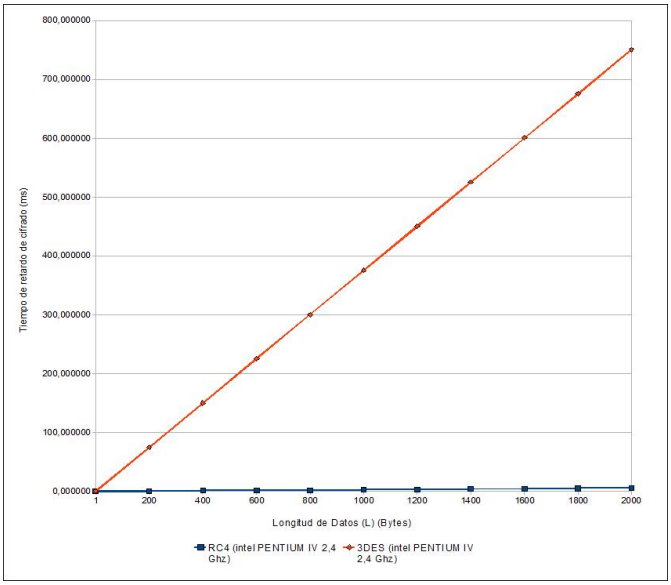


Figura 6. Tiempos de cifrado de los algoritmos 3DES y RC4.

Si aplicamos los datos a los terminales inalámbricos obtenemos la figura 7 que representa el tiempo de cifrado cuando un terminal ímplementa SSL, IPSEC y WEP antes y después de aplicar la solución Cross-Layer propuesta. La reducción de tiempo de cifrado total es de un factor 2.37 para un valor de L igual a 100 octetos, 3.35 si L es 1400 octetos y 3.4 si el valr de L es 2000 octetos.

Si aplicamos los datos al punto de acceso y analizamos el rendimiento a nivel MAC del algoritmo RC4 cuando se aplican mecanismos de cifrado en capas superiores, obtenemos la figura 8 que representa el tiempo de cifrado del algoritmo RC4 en el punto de acceso antes y después de aplicar la solución Cross-Layer propuesta. La tabla IV resume los valores y reducción del tiempo de cifrado necesario en el punto de acceso a nivel MAC, cuando el valor de L es 2000 octetos,

Tiempo de cifrado de RC4 en punto de acceso			
Algoritmos de cifrado	Tiempo original (ms)	Tiempo Cross-Layer (ms)	Reducción tiempo de cifrado
SSL y WEP	5,581	0,153	36,37
IPSEC y WEP	5,665	0,162	35,07
SSL, IPSEC y WEP	5,721	0,162	35,42

Tabla IV
TIEMPOS DE CIFRADO DEL ALGORITMO RC4 EN PUNTO DE ACCESO PARA L=2000 OCTETOS.

V-C. Efectos del número de clientes sobre el tiempo de cifrado del algoritmo RC4.

En el apartado IV hemos analizado el rendimiento de los mecanismos de cifrado en un cliente inalámbrico. El AP da servicio a todos los terminales de su área de cobertura por lo que en este apartado introducimos el análisis del rendimiento en el AP desde el punto de vista del número de terminales a los que da servicio cuando aplica cifrado WEP (algoritmo RC4). Una primera estimación del efecto del incremento de terminales inalámbricos lo realizamos a partir del análisis de [20], donde se estudia dicho aspecto. De este artículo se extrae la tabla V que proporciona el throughput teórico y empírico, considerando un payload de 1500 octetos, para 1 y 4 (media del throughput) clientes, en los casos de aplicar

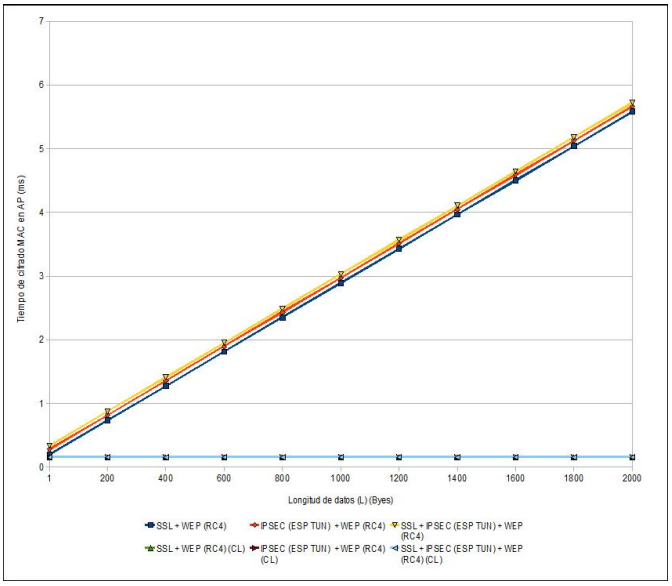


Figura 8. Comparativa de Tiempos de cifrado original y aplicando la propuesta Cross-Layer en el AP.

y no aplicar cifrado WEP-128.

Throughput (Mbps)				
Cifrado	Teórico 1 cliente	Analítico 1 cliente	Teórico 4 clientes	Analítico 4 clientes
None	22,7	22,72	21	20,55
WEP-128	22,7	22,67	21	20,37

Tabla V
THROUGHPUT WEP-128.

Aplicando estos datos a los tiempos de cifrado del algoritmo RC4 indicados en [1], obtenemos los valores de tiempo de cifrado indicados en la tabla VI donde se indica, que el aumento del tiempo de proceso para cada cliente, que supone incrementar el número de clientes del AP de 1 a 4, es del 11,29 %.

Rendimiento de RC4 para 1500 octetos.		
Núm. clientes	Tiempo teórico	Tiempo analítico
1	0,00698 ms	0,007 ms
4	0,00772 ms	0,00779 ms

Tabla VI
DETALLE DE RENDIMIENTO DE RC4 ARQUITECTURA INTEL PARA 1 Y 4 CLIENTES.

VI. ANÁLISIS DE LA ARQUITECTURA CROSS-LAYER.

La solución presentada en este artículo requiere que cada capa tenga información de los servicios de seguridad implementados en el resto de capas y especificamente de los mecanismos de cifrado aplicados. En [21] se proponen tres esquemas de arquitectura para soluciones que requieran una interacción entre capas:

1. Comunicación directa entre capas.
2. Base de datos compartida.
3. Nuevas capas de abstracción.

La información de aplicación que desciende por las capas hasta el nivel MAC corresponde a una conexión entre el cliente inalámbrico y un servidor. Los protocolos de capa generan a partir de dicha información las PDU (Protocol Data Unit) que tienen sus campos cifrados si los servicios de seguridad de capa lo requieren, pero no lo están si la aplicación no lo requiere o, incluso puede suceder, que los mecanismos de cifrado cambien en el transcurso de la comunicación. La información de cifrado intercambiada entre capas debe ser específica para una conexión entre el cliente y un servidor y afectará a la información transmitida en esa conexión. Para otra conexión con otro servidor la información de seguridad puede variar, porque se aplican mecanismos de cifrado diferentes o porque no se requiere ningún servicio de seguridad. Con estas variaciones la arquitectura Cross-Layer debe proporcionar información del cifrado realizado sobre los datos que va a procesar y esta información debe estar actualizada.

Al analizar las arquitecturas propuestas en [21] y considerando las características descritas anteriormente, descartamos la arquitectura basada en nuevas capas de abstracción porque la estructura de protocolos actuales no necesita ser modificada. También descartamos la creación de una base de datos debido a que debería contener información independiente por cada segmento generado en la capa TCP. Proponemos una arquitectura Cross-Layer basada en la comunicación directa entre capas basada en la activación de flags en el segmento y paquete que informen de los mecanismos de cifrado que incorpora.

VII. PROPUESTA DE ARQUITECTURA CROSS-LAYER.

En este apartado y considerando la solución propuesta en [1] proponemos un algoritmo basado en el diseño Cross-Layer para la interacción entre capas. Este algoritmo es particular para el escenario presentado en este artículo pero permite variaciones en cuanto a protocolos, mecanismos de cifrado y servicios de seguridad que puedan producirse en escenarios diferentes. La figura 9 presenta el algoritmo Cross-Layer que se describe a continuación.

En primer lugar definimos el registro de seguridad de capa n (RS_n) formado por 3 bits (a_{n2}, a_{n1}, a_{n0}) que indica si la capa n aplica mecanismos de cifrado y determina que mecanismo es utilizado. Para indicar que la capa n no aplica mecanismos de cifrado el registro RS_n tendrá el valor RS_n=(0,0,0). En nuestro escenario tan solo utilizamos un bit de este registro pero al definirlo con tres bits nos permite considerar futuras ampliaciones en cuanto a los mecanismos de cifrado incluidos. Definimos el valor de estos registros para los mecanismos de seguridad de nuestro escenario como:

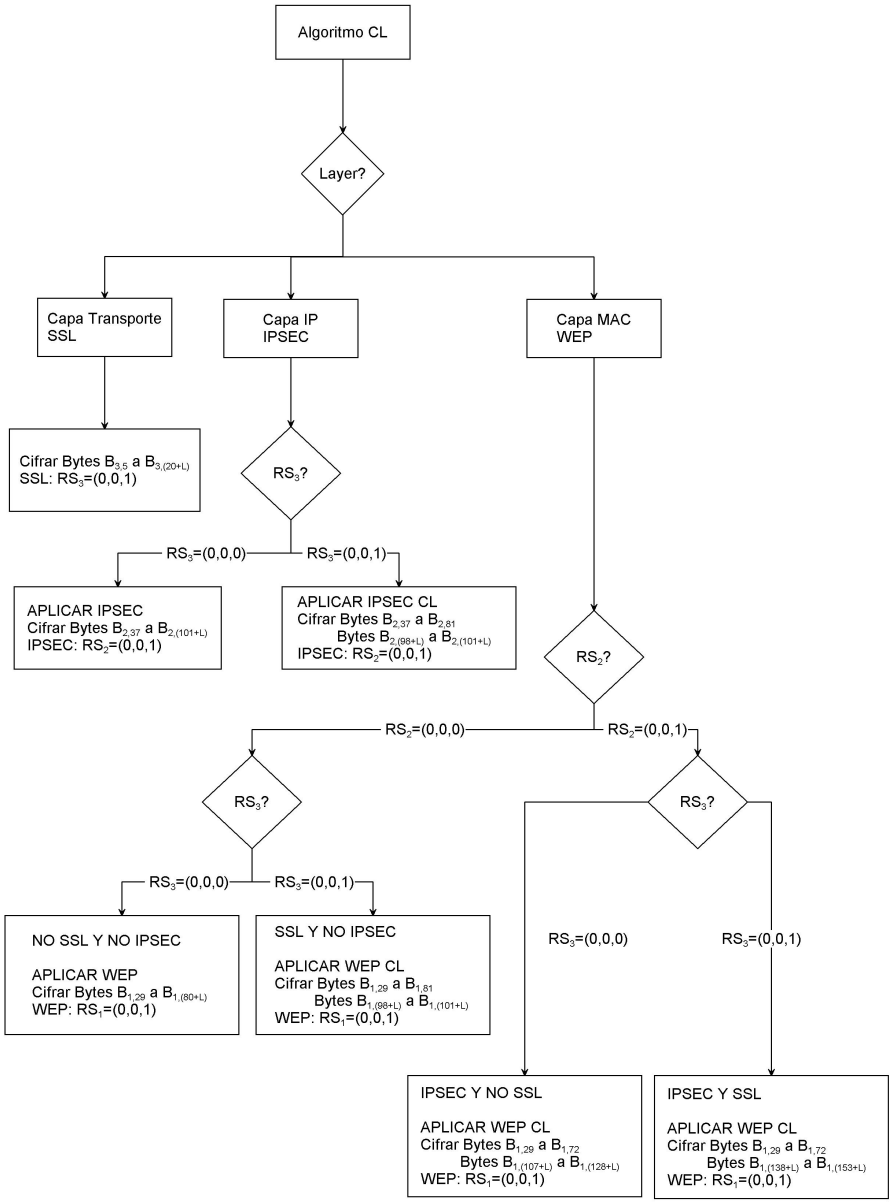


Figura 9. Algoritmo Cross-Layer de cifrado de datos .

1. SSL: n=3, (a_{32}, a_{31}, a_{30})=(0,0,1).
2. IPSEC con protocolo ESP en modo túnel: n=2, (a_{22}, a_{21}, a_{20})=(0,0,1).
3. WEP: n=1, (a_{12}, a_{11}, a_{10})=(0,0,1).

A partir de la solución propuesta en [1] diseñamos el algoritmo de capa de la arquitectura Cross-Layer, que decidirá si una capa aplica mecanismos de cifrado y qué octetos debe cifrar. Para referenciar los octetos sobre los que actuarán estos mecanismos, definimos $B_{i,j}$ como el octeto de información i de la capa j, siendo $i, j \geq 0$.

1. Algoritmo en capa Transporte. SSL cifrará la información según se describe en [1]. El valor de RS_3 será igual a (0,0,1).
2. Algoritmo en capa IP. El algoritmo evalúa en primer lugar el valor de RS_3. Si éste es igual a (0,0,0) aplicará el cifrado IPSEC en todos los campos por defecto, referenciados por los octetos $B_{2,37}$ a $B_{2,(101+L)}$. En el caso en que RS_3=(0,0,1) IPSEC aplicará cifrado a los octetos con PC=0 en capa IP, octetos $B_{2,37}$ a $B_{2,81}$ y octetos $B_{2,(98+L)}$ a $B_{2,(101+L)}$). Al aplicar cifrado modificará el valor de RS_2=(0,0,1).
3. Algoritmo en capa MAC. El algoritmo Cross-Layer de capa evalúa en primer lugar el valor de RS_2 y a continuación se evalúa el valor de RS_3. El valor de estos registros ofrecen cuatro posibilidades a partir de las que se decide sobre qué octetos a nivel MAC se aplicará cifrado. La tabla VII resume las opciones de los registros RS_2 y RS_3 y el resultado del algoritmo Cross-Layer a nivel MAC.

Opciones registros de seguridad de capa n				
RS_3	RS_2	Mecanismos Cifrado utilizado	Cifrado WEP	octetos a cifrar
(0,0,0)	(0,0,0)	Ninguno	Aplicar WEP	$B_{1,29}$ a $B_{1,80+L}$
(0,0,0)	(0,0,1)	IPSEC	Aplicar WEP CL	$B_{1,29}$ a $B_{1,72}$ y $B_{1,107+L}$ a $B_{1,128+L}$
(0,0,1)	(0,0,0)	SSL	Aplicar WEP CL	$B_{1,29}$ a $B_{1,81}$ y $B_{1,98+L}$ a $B_{1,101+L}$
(0,0,1)	(0,0,1)	SSL + IPSEC	Aplicar WEP CL	$B_{1,29}$ a $B_{1,72}$ y $B_{1,138+L}$ a $B_{1,153+L}$

Tabla VII
ALGORITMO CL EN CAPA MAC

La aplicación de la propuesta Cross-Layer presentada requiere la señalización entre todos los nodos que participan en el cifrado de la información. Debido a las restricciones de espacio dejamos para futuros trabajos la presentación de dichos mecanismos de señalización.

VIII. CONCLUSIONES Y TRABAJO FUTURO.

En este artículo hemos diseñado un algoritmo Cross-Layer para implemtar la solución presentada en [1] para reducir la redundancia en el cifrado de los octetos de los diferentes protocolos de capa. Hemos cuantificado que el ahorro de energía y duración de la batería para una PDA iPAQ H3670 es de 58 % si L=100 octetos, cuando se implementa el dideño Cross-Layer. Para L=1400 y L=2000 octetos, el ahorro de energía es de un 70 % y de un 71 % respectivamente. La reducción del tiempo de cifrado del algoritmo RC4 en un procesador INTEL Pentium 4 2.4 Ghz que implementa el diseño Cross-Layer propuesto, es de un factor 2,37 si L=100 octetos, 3,35 si L=1400 octetos y 3,4 si L=2000 octetos. También hemos cuantificado el incremento de tiempo de cifrado al aumentar el número de clientes de 1 a 4, siendo este incremento del 11,29 %.

El trabajo a realizar a partir de este artículo consiste en considerar otros servicios de seguridad y mecanismos de cifrado de capa con el objeto de cuantificar el coste de energía en los terminales inalámbricos y el rendimiento en el AP. En este artículo hemos introducido los efectos del incremento de clientes inalámbricos y en particular sobre el algoritmo de cifrado RC4 al pasar de 1 a 4 clientes. El trabajo futuro debe incluir el análisis del coste en energía y rendimiento en función del número de clientes inalámbricos y de la longitud de los datos en los servicios de seguridad considerados.

IX. AGRADECIMIENTOS.

Este trabajo ha sido parcialmente financiado por el MEC y FEDER bajo los proyectos: "Seguridad en la Contratación Electrónica basada en Servicios Web"(CICYT TSI2007-62986) y ARES "Grupo de Investigación Avanzada en Seguridad y Privacidad de la Información"(Consolider - Ingenio CSD2007-004).

REFERENCIAS

[1] A. Urbano, J.L. Ferrer and M. Payeras. Análisis de la arquitectura de seguridad en los protocolos TCP/IP y 802.11. *Internal Report N1032010.*, 2010. http://secom.uib.es/papers/201003_INTERNAL_REPORT_N1.pdf.

[2] Baghaei N. and Hunt R. Security performance of loaded IEEE 802.11b Wireless Networks. *Computer Communications, Elsevier, U.K.*, 27(17):1746–1756, 2004.

[3] Barka E. and Boulmalf M. Impact of encryption on the Throughput of Infrastructure WLAN IEEE 802.11g. *IEEE Wireless Communications and Networking Conference.*, March 2007.

[4] Carneiro G., Ruela J. and Ricardo M. Cross-Layer Design in 4G Wireless Terminal. *IEEE Wireless Communications*, 11(2):7–13, April 2004.

[5] Craig A. Shue, Minaxi Gupta, Steven A. Myers. IPSec: Performance Analysis and Enhancements. *IEEE International Comference on Communications*, June 2007.

[6] Da Costa Junior F., Gaspary L., Barbosa J., Cavalheiro G., Pfitscher1 L., and Ramos J.D.G. Evaluating the Impact on Data Reception and Energy Consumption of Mobile Devices using IPSec to securely access WiFi Networks. *Paper presented at the Wireless Communications and Networking Conference (WCNC2005). News Orleans. LA, USA*, March 2005.

[7] Dawoud D.S., Bigondo A. and Dawoud P. A study of the energy consumption of security Encryption Policies in wireless devices. *Paper presented at Southern Africa Telecommunication Networks and Application Conference (SATNAC2008)*, September 2008.

[8] Gin A. and Hunt R. Performance Analysis of Envolving Wireless IEEE 802.11 Security Architectures. *International Conference on Mobile Technology, Applications and Systems*, 2008.

[9] Jin-Cherng L., Ching-Tien C. and Wei-Tao C. Design, Implementation and Performance Evaluation of IP-VPN. *in Proceedings of the 17 th International Conference on Advanced Information Networking and Applications (AINA'03)*, pages 206–209, March 2003.

[10] Kawadia V. and Kumar P.R. A cautionary perspective on cross-layer design. *IEEE Wireless Communications*, 12(1):3–11, 2005.

[11] Nadeem A. and Younus Javed M. A Performance Comparison of Data Encryption Algorithms. *Paper presented at the Proceedings of the 1st International Conference on Information and Communication Technologies (ICICT 2005), Karachi, Pakistan.*, August 2005.

[12] Narayan S., Kolahi S.S., Sunarto Y., Nguyen D.D.T., Mani P. The influence of Wireless 802.11g LAN encryption Methods on Throughput and Round Trip Time for Various Windows Operating Systems. *Proceedings of 6th IEEE Conference on Communication Networks and Services Research Conference (CNSR). Halifax*, pages 171–175, May 2008.

[13] Niedermayer H., Klenk A. and Carle G. The Networking Perspective of Security Performance - A Measurement Study. *in Proc. 13th GI/ITG Conf. Measurement, Modeling, and Evaluation of Computer and Communication Systems (MMB), Nürnberg, Germany*, March 2006.

[14] Potlapally N. R., Ravi S., Raghunathan A. and Jha N.K. A study of the energy consumption Characteristics of Cryptographic Algorithms and Security Protocols. *IEEE Transactions on Mobile Computing.*, 5(2):128–143, February 2003.

[15] Prasithsangaree P. and Krishnamurthy P. Analysis of Energy consumption of RC4 and AES Algorithm in Wireless LAN. *IEEE GLOBECOM 2003*, pages 1445–1449.

[16] Rapuano S. and Zimeo E. Measurement of performance impact of SSL on IP data transmissions. *ScienceDirect Measurement.*, 41:481–490, 2008.

[17] Ronan J., Malone P. and Foglhú M. Ó. Overhead Issues for Local Access Points in IPSec enabled VPNs. *IPS Workshop, Salzburg*, February 2003.

[18] Schneier B. and Whiting D. Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processos. *Lecture Notes in Computer Science. In Eli Biham, editor, Fast Software Encryption '97*, 1267:242–259, 1997.

[19] Shakkottai S., Rappaport T.S. and Karlsson P.C. Cross layer design for Wireless Networks. *IEEE Communications Magazine*, 41(10):74–80, October 2003.

[20] Siwamogsatham S., Hiranpruek K., Luangigkasut C. and Srilasak S. Revisiting the Impact of Encryption on Performance of IEEE 802.11 WLAN. *Proceedings of ECTI-CON*, 1:381–384, May 2008.

[21] Srivastana V. and Montani M. Cross-Layer Design: a survey and the road ahead. *IEEE Communications Magazine*, 43:112–119, December 2005.

[22] Thamilarasu G. and Sridhar R. Exploring Cross-Layer techniques for Security: Challenges and Opportunities in Wireless Networks. *Military Communications Conference. (MILCOM2007)*, pages 1–6, October 2007.

[23] Thamilarasu G., Mishra S. and Sridhar R. A cross-layer approach to detect jamming attacks in wireless ad hoc networks. *Military Communications Conference. (MILCOM2006)*, pages 1–6, October 2006.

[24] Zeynep Gurkas G., Halim Zaim A., Ali Aydin M. Security Mechanisms and Their Performance Impacts on Wireless Local Area Networks. *Procedings of the Seventh IEEE International Symposium on Computer Networks (ISCN'06)*, June 2006.

Evaluación de un Nuevo Mecanismo de Transmisión Multicast en Redes HomePlug AV

P.J. Piñero Escuer, J. Malgosa Sanahuja, P. Manzanares Lopez, J.P. Muñoz Gea
Departamento de Tecnologías de la Información y Comunicaciones
Universidad Politécnica de Cartagena
Antiguo Cuartel de Antigones (Campus muralla de mar), 30202 Cartagena.
Email: {pedrop.escuer, josem.malgosa, pilar.manzanares, juanp.gea}@upct.es

***Resumen*—La aparición de las redes *peer-to-peer* y el rápido avance de las tecnologías utilizadas para el despliegue de redes *in-home* suponen la apertura de una gran cantidad de posibilidades tanto para los usuarios particulares como para las PYMES, y lleva a pensar que este tipo de redes tendrán un papel muy importante en un futuro próximo. De entre las diferentes tecnologías adecuadas para entornos *in-home*, una de las de mayor índice de penetración son las comunicaciones a través de la infraestructura de cableado eléctrico. Actualmente, el estándar más importante dentro de este tipo de comunicaciones, Homeplug AV, presenta un mecanismo ineficiente para la realización de transmisiones *multicast*, muy presentes en entornos *in-home*. Para solventar esta limitación, este trabajo propone un nuevo mecanismo para realizar transmisiones *multicast* en redes HomePlug AV que mejora notablemente el método utilizado actualmente en este tipo de redes.**

***Palabras Clave*—Redes *in-home*, Homeplug AV, *Multicast*.**

I. Introducción

Se denominan redes *in-home* a aquellas redes que tienen como objetivo principal la comunicación entre los diferentes dispositivos eléctricos y electrónicos presentes en una vivienda: desde televisores y aparatos de radio hasta ordenadores o vídeo-consolas. Actualmente, la aparición de las redes *peer-to-peer* y el rápido avance de las tecnologías utilizadas para el despliegue de redes *in-home* estan haciendo que este tipo de redes se empiecen a ver como parte de la propia Internet, y no únicamente como redes de acceso a la misma. En la Internet del futuro [1], las redes *in-home* (y su extensión natural, las redes *in-building*) permitirán que los dispositivos que las forman, además de poder descargar contenidos de la red, puedan actuar como servidores de contenidos. Esto abre una gran cantidad de posibilidades tanto para usuarios particulares como para pequeñas y medianas empresas (PYMES) y lleva a pensar que este tipo de redes tendran un papel muy importante en la Internet del Futuro y de la denominada Sociedad de la Información.

En la actualidad existen varias alternativas que se podrían utilizar para desplegar una red *in-home*. Estas tecnologías se pueden dividir en tres categorías [2]:

- *Inalámbricas*. Su principal ventaja es que el receptor tiene libertad para moverse manteniendo la conectividad siempre y cuando no se aleje excesivamente de los puntos de acceso que le dan servicio. Las tecnologías inalámbricas más interesantes son las de la familia 802.11. Dentro de ella tenemos 802.11b, que opera a 2.4Ghz y proporciona una tasa de transmisión de 11Mbps, 802.11a que proporciona 54Mbps a 5Ghz y 802.11g que opera a 2.4GHz y proporciona 54Mbps. Por último, recientemente ha aparecido el estándar 802.11n que trabaja tanto en la banda de 2.4Ghz como en la de 5Ghz y que puede proporcionar tasas de transmisión de hasta 300Mbps.
- *cableadas*. Este tipo de redes presentan el inconveniente de que requieren el despliegue de una infraestructura de cableado estructurado para dar servicio de voz y datos (fundamentalmente *fast-ethernet*) que puede llegar a ser muy costoso.
- *No-new-wires*. Se denominan así las tecnologías que son capaces de aprovechar las infraestructuras de cableado ya existentes en el edificio para el despliegue de la red. Dentro de esta categoría tenemos las tecnologías que utilizan la línea telefónica, el cable coaxial del operador de CATV o la red eléctrica para el intercambio de datos. Esta última es la que más interés está despertando actualmente entre la industria y la comunidad científica, ya que las otras dos presentan el inconveniente de que, al menos la mayoría de países Europeos, el número de puntos de conexión con la línea telefónica o con la red de cable es muy limitado

Las dos tecnologías con mayor índice de penetración tanto en el hogar como en la PYME, (es decir, en entornos *in-home*) son las redes inalámbricas y comunicaciones a través de la red eléctrica (*PLC, Power Line Communications*). Las redes PLC son muy sencillas de instalar y de ampliar y además, al utilizar los cables de baja tensión instalados en el edificio, su coste de instalación y ampliación es extremadamente bajo. Existen diferentes estándares para la tecnología PLC. Sin embargo, el HomePlug AV (HomePlug Audio y Video, o símplemente HPAV) es el más popular. Este estándar, presentado por la Homeplug Powerline Alliance [3] en 2005, puede proporcionar tasas de transmisión de hasta 200 Mbps sobre los cables de baja tensión de cualquier edificio [4]. Prueba del auge de esta tecnología es que actualmente existen en el mercado más de 70 productos certificados Homeplug [5], incluyendo productos que extienden esta tecnología, llegando a tasas de transmisión de hasta 1Gbps [6].

Entre las muchas aplicaciones que pueden utilizarse en las redes *in-home*, los juegos en red o las transmisiones de contenidos multimedia entre varios usuarios son algunas de las más comunes y frecuentes. En estos casos la utilización de la tecnología IP *multicast* pueden ser de gran utilidad, ya que esta tecnología optimiza el uso de los recursos de la

red[1]. Sin embargo, con el estándar actual, las comunicaciones IP *multicast* no son posibles en las redes HPAV. Esto es debido a que, a pesar de que el canal PLC es *broadcast*, la naturaleza de la modulación OFDM (*Orthogonal Frequency-Division Multiplexing*) [7] que se utiliza a nivel físico es punto a punto. La técnica que se utiliza para realizar transmisiones a un grupo de receptores en las redes HPAV consiste en la transmisión de cada paquete a los distintos miembros del grupo de manera consecutiva utilizando transmisiones punto a punto. En este trabajo se propone un nuevo método para realizar comunicaciones *multicast* sobre redes HPAV, el cuál consigue tasas de transmisión elevadas incluso cuando el número de miembros del grupo *multicast* es muy alto.

El resto del artículo se estructura de la siguiente manera: en la sección II se describen las características principales de la tecnología HomePlugAV. La sección III presenta la caracterización del canal de comunicaciones PLC utilizada para implementar nuestra técnica de transmisión *multicast*. La sección IV muestra los resultados de simulación. Finalmente la sección V resume las conclusiones más destacadas de este trabajo.

II. Tecnología HomePlug AV

A. Características principales

Homeplug AV es un estándar para la transmisión de datos en redes PLC de bajo voltaje (220v) auspiciado por la Homeplug Alliance. Es la evolución natural de la version anterior, denominada Homeplug 1.0, y su principal objetivo es proporcionar suficiente capacidad para soportar un acceso a Internet de banda ancha y, a la vez, permitir la distribución de contenidos de audio y vídeo. Esta tecnología es capaz de transmitir datos a una capacidad de hasta 200 Mbps, aunque el uso de Turbo Códigos Convolucionales para la detección y recuperación automática de errores reduce la tasa real de bits de información a aproximadamente 150 Mbps.

A nivel físico, la modulación utilizada para la transmisión de bits es OFDM. Esta modulación se basa en la transmisión simultánea de un gran número de portadoras ortogonales entre si y con un ancho de banda muy reducido. Concretamente, en HPAV se utilizan 1155 portadoras en la banda de 1.8Mhz a 30Mhz, por lo que la separación entre portadoras es de aproximadamente 24.4KHz. Sin embargo algunas de estas portadoras coinciden con las bandas de emisión de los radioaficionados y no pueden ser utilizadas, lo que provoca que el total de portadoras útiles se reduzca a 917. La figura 1 muestra la máscara de atenuación que se debe aplicar a las transmisiones HPAV para eliminar las frecuencias no disponibles en el rango 1.8-30 Mhz. También se puede observar que la potencia de transmisión de las portadoras que pueden utilizarse está limitada a -50dBm/Hz.

En función de las características del canal que detecte el transmisor, éste eliminará aquellas portadoras con una relación señal a ruido (SNR) más pobre, y además seleccionará la modulación y codificación adecuada para cada una de las portadoras restantes. Esta modulación puede ser desde una simple BPSK (1 bit de información por portadora) cuando la SNR es baja, hasta 1024 QAM (10 bits de información por portadora) cuando la SNR es muy alta. La elección de la modulación será distinta en función de la probabilidad de error de bit deseada. La tabla I muestra la modulación utilizada en función de la SNR observada para cada portadora, para una BER de 10^{-8}. Estas asignaciones serán las utilizadas en los experimentos realizados en este trabajo. Es importante destacar también que una portadora cualquiera se elimina si su SNR está por debajo del mínimo exigido por la modulación BPSK.

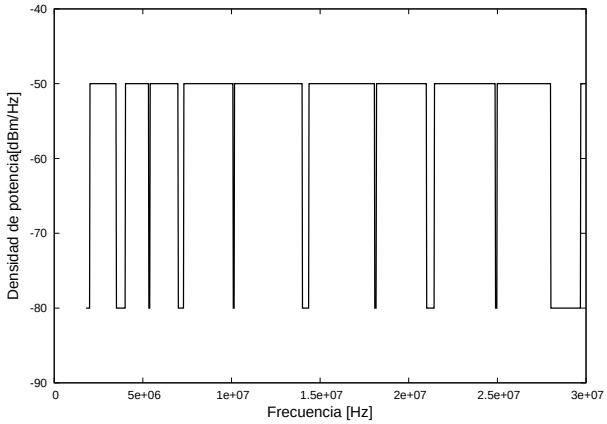


Fig. 1. Máscara de transmisión para HomePlug AV

Tabla I
Modulación en función de la SNR para una BER de 10^{-8}

Modulación	Rango de SNR (dB)
BPSK	12 - 15
4-QAM	15 - 20
8-PSK	20 - 22
16-QAM	22 - 29
64-QAM	29 - 35
256-QAM	35 - 40
1024-QAM	$>$ 40

Los diversos dispositivos electrónicos conectados a la red eléctrica utilizarán la red *in-home* mediante el uso de modems HPAV. Cada uno de los modems conectados a la red dispone de un mapa de tonos (*TM, Tone Map*) para comunicarse con cada uno de los restantes modems. Este mapa de tonos indica el tipo de modulación a utilizar para cada portadora. Conocido el número de bits por portadora, la capacidad de nivel físico del enlace puede ser calculada mediante un cociente entre el número de bits por símbolo y el perido de cada símbolo OFDM. El valor del periodo de símbolo en HPAV (considerando los intervalos de guarda) es de 46.52μs.

Por su parte, el nivel MAC de HPAV está diseñado para ser altamente eficiente, proporcionando dos modos de transferencia distintos:

- Transferencias orientadas a la conexión con requerimientos de QoS (ancho de banda garantizado, limitación del jitter y latencia máxima). Este servicio se proporciona utilizando un sistema de acceso al medio TDMA (*Time Division Multiple Access*).
- Transferencias no orientadas a la conexión (*conection-*

[1]Recordemos que la idea principal de la tecnología IP *multicast* es minimizar el número de flujos idénticos de información que deben generarse para alcanzar todos los miembros que forman parte del grupo *multicast*. En un medio broadcast se reduciría a un único flujo

less) que comparten un mismo canal de comunicaciones (*contention*). Este modo de transferencia es utilizado tanto por servicios asíncronos pero con requerimiento de QoS como por servicios *best-effort* y se proporciona mediante un esquema de acceso al medio CSMA/CA basado en prioridades.

A pesar de que el canal de comunicaciones PLC de HPAV es *broadcast*, la modulación OFDM hace que las comunicaciones sean siempre punto a punto. En efecto, cuando dos modems se comuniquen entre sí, los demás modems conectados a la red también recibirán dicha información (por ser transmitida a un medio compartido), pero no serán capaces de decodificarla ya que desconocen el mapa de tonos empleado por la pareja emisor-receptor.

Complementando la modulación OFDM, el estandar HPAV emplea un tipo de modulación especial, denominada modulación ROBO (*ROBust Ofdm*) que permite la transmisión *broadcast*. Este modo de transmisión se emplea siempre que es necesario transmitir paquetes de control (o cualquier otro tipo de paquetes *broadcast*) que deba ser necesariamente recibido por todos los miembros de la red HPAV. El modo ROBO emplea una modulación y una codificación robustas frente al ruido con el fin de asegurar la correcta recepción y decodificación de la información en todos los receptores. Podría pensarse en utilizar este modo de transmisión para servicios *multicast*. Sin embargo, la tasa de transmisión del modo ROBO está limitada a unos 5-10 Mbps a nivel físico, lo que es cláramente insuficiente para la mayoría de las aplicaciones que utilizan transmisiones *multicast*.

B. Comunicaciones multicast en HomePlug AV

Por las características descritas anteriormente, la implementación de transmisiones *multicast* en redes HPAV presenta serios problemas. La utilización de la tecnología IP *multicast* en redes HPAV se traduce automáticamente en una serie consecutiva de transmisiones punto a punto a cada uno de los miembros del grupo *multicast* (ello se hace de manera totalmente transparente para el usuario). De esta forma, la capacidad efectiva de transmisión *multicast* se puede obtener mediante la ecuación 1 donde se puede observar que la capacidad efectiva disminuye de manera exponencial a medida que aumenta el número de receptores.

$$\frac{1}{C_{total}} = \sum_{i=1}^{N} \frac{1}{C_i} \tag{1}$$

El trabajo presentado en este artículo propone una solución alternativa para la implementación de las comunicaciones *multicast*. El modo de transmision *multicast* propuesto consiste en la elección y utilización de un mapa de tonos común para todos los miembros del grupo *multicast*. En este mapa de tonos común se asignará a cada portadora la modulación que corresponda al miembro del grupo que presenta la peor SNR para esa frecuencia. De esta forma se consigue que todos los miembros del grupo *multicast* sean capaces de decodificar correctamente la información, con una tasa de error baja. La modulación escogida para cada portadora tendrá una cantidad de bits de información igual o menor a la que se le asignaría para una transmisión punto a punto. Con este modo de transmisión se consiguen dos importantes ventajas con respecto al sistema *multicast* tradicional de HPAV:

- El número de miembros del grupo *multicast* no tiene porqué afectar significativamente a la capacidad efectiva de la transmisión *multicast*.
- El número de accesos del transmisor al canal es menor, ya que solo debe acceder una vez por cada grupo *multicast* al que desee transmitir información. Esto hace que el retardo introducido por el protocolo de control de acceso al medio (CSMA/CA) sea mucho menor que si se realizaran las múltiples transmisiones en modo punto a punto.

III. Caracterización del canal PLC

A. Modelo del canal PLC

Para estudiar el correcto funcionamiento del modo de transmisión *multicast* propuesto y cuantificar sus beneficios se ha empleado un simulador de la respuesta en frecuencia del canal de comunicaciones PLC. El simulador empleado en este trabajo está basado en el modelo propuesto en [8][9]. Este modelo se basa en la caracterización del canal de comunicaciones PLC como un sistema lineal e invariante con el tiempo y con un ruido estacionario aditivo. Además, supone que las características de los dispositivos no se ven influidas por el valor de la señal de distribución de energía electrica. Esta suposición no es completamente cierta, pero el error que se comete no afecta sustancialmente a los resultados objeto de este estudio.

El modelo asume que la red de cableado eléctico consiste en un conjunto de líneas de transmision de tipo bifilar conectadas entre sí construyendo una topología con forma de árbol. En las terminaciones de estas líneas puede haber un circuito abierto o un dispositivo. Los dispositivos se caracterizan como bipolos con una carga lineal y una fuente de ruido. Finalmente, los dispositivos transmisor y receptor estarán también compuestos por una carga lineal y por un generador de señal en el caso del transmisor. Por tanto, para poder simular el comportamiento de un dispositivo conectado a un enchufe necesitamos conocer su impedancia característica en función de la frecuencia y la densidad espectral de potencia (DEP) de ruido que genera. En este trabajo hemos caracterizado algunos de los dispositivos más comunes en una vivienda y el módem HPAV modelo PLE-200 de Linksys. En la figura 2 se observa la parte real e imaginaria de la impedancia de entrada de dicho módem.

La respuesta del canal entre dos puntos cualesquiera de la red estará condicionada, además de por la distancia entre ellos, por la impedancia de las distintas ramificaciones de la red eléctrica que no pertenecen al camino principal entre los dos puntos considerados. La medida en que estas impedancias afectan al camino principal se puede calcular aplicando las propiedades de desplazamiento de impedancias propias de las líneas de transmisión.

Por último, el ruido presente en el receptor puede tener dos origenes posibles: ruido externo a la red o ruido generado por los dispositivos. En el segundo caso, la contribución de un dispositivo al ruido total vendrá determinada por la respuesta del canal desde el dispositivo hasta el receptor. Finalmente, el ruido total se calculará mediante el principio de superposición.

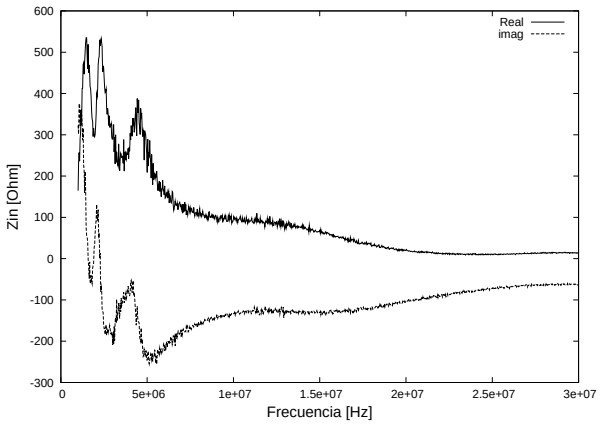


Fig. 2. Impedancia de entrada de un módem HPAV Linksys PLE200.

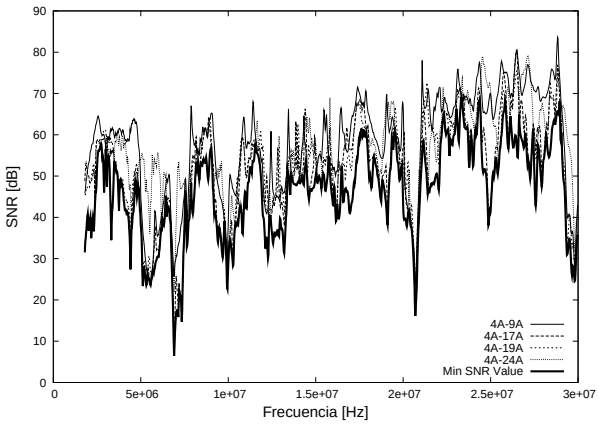


Fig. 4. SNR para las transmisiones del escenario I.

B. Estructura del simulador

El simulador utilizado en este trabajo está basado en el modelo anterior y tendrá como parámetro de entrada una topología red HPAV a la que se conectarán diferentes dispositivos, proporcionando como resultado final la capacidad (en bps) del enlace entre dos puntos cualesquiera de la red.

Los datos de la topología de red que se desea estudiar se introducirán mediante un fichero XML. A partir de estos datos se generará el árbol de la red a simular. Este árbol será el argumento de entrada del módulo encargado de obtener la respuesta del canal HPAV utilizando el modelo descrito anteriormente. Este módulo calculará la atenuación que produce el canal y la potencia de ruido a la salida para cada una de las frecuencias de las portadoras del estándar HPAV. Con estos datos y sabiendo que la potencia de las portadoras HPAV es de -50 dBm/Hz, se puede calcular para cada una de ellas la relacion señal a ruido.

A partir de los valores de relación señal a ruido, y teniendo en cuenta que el esquema de modulación que utiliza HPAV asigna a cada portadora una cantidad de bits de información en función de dicha relacion (ver tabla I), el simulador es capaz de calcular la velocidad del enlace entre dos puntos cualesquiera de la red.

IV. Resultados

Para comprobar el funcionamiento y cuantificar los beneficios del modo de transmisión *multicast* propuesto se estudiaron dos posibles escenarios: una transmisión *multicast* dentro de una vivienda (escenario *in-home*) y una transmisión *multicast* a equipos ubicados en dos viviendas pero que comparten una misma fase eléctrica (escenario *in-building*).

Las viviendas utilizadas en la simulación responden al plano mostrado en la figura 3. En él todos los enchufes disponibles en cada vivienda están numerados del 1 al 26. La tabla II muestra los dispositivos conectados a cada uno de los enchufes. Además los puntos de iluminación están indicados por un círculo bicolor.

A. Escenario I

En este primer escenario obtendremos el resultado correspondiente a la transmisión desde un equipo situado en el enchufe 4 de una vivienda (Vivienda A) hasta otros cuatro equipos situados en los enchufes 9, 17, 19 y 24 de la misma vivienda.

Tabla III
Resumen resultados escenario I

Enlace	C (Mbps)
4A - 9A	192.132
4A - 17A	186.092
4A - 19A	187.382
4A - 24A	188.414
Multicast punto-punto	47.120
Multicast	180.911

La figura 4 muestra la SNR del canal entre cada pareja emisor-receptor. Además, en la misma figura se muestra el mínimo valor de la SNR para cada una de las portadoras. A partir de estos valores, y utilizando el esquema de modulación OFDM empleado por HPAV, se obtienen las capacidades de canal de nivel físico para cada pareja emisor-receptor. Una vez obtenidas dichas capacidades punto a punto entre los diferentes equipos, la capacidad de la transmisión *multicast* mediante transmisiones punto a punto se obtiene aplicando la ecuación 1.

En el mismo escenario, y para los resultados de SNR obtenidos, la capacidad de transmisión *multicast* del método propuesto en este trabajo se obtiene aplicando el mismo esquema de modulación al valor mínimo de relación señal a ruido en cada portadora (también mostrado en la gráfica, con un trazado más grueso). Los resultados obtenidos se detallan en la tabla III. Las cuatro primeras filas corresponden a los valores de capacidad de enlace obtenidos si sólo se realizara la transmisión entre el emisor y un receptor en particular. El siguiente valor, 47.120 Mbps, corresponde a la capacidad obtenida en la transmisión *multicast* que emplea transmisiones punto a punto. Por último, el valor de 180.911 Mbps corresponde a la capacidad de transmisión *multicast* con el modo de transmisión propuesto. Comparando los resultados se puede comprobar como la velocidad de transmisión obtenida mediante el método propuesto es mucho mayor (aproximadamente 4 veces mayor) a la que se consigue con el método utilizado actuálmente en los equipos HPAV.

Es interesante destacar también que los resultados serían incluso mejores que los mostrados en la tabla, ya que el

Tabla II
DISPOSITIVOS CONECTADOS A LOS DIFERENTES ENCHUFES DE LA VIVIENDA

Enchufe	Dispositivo		Enchufe	Dispositivo	
	Vivienda A	Vivienda B		Vivienda A	Vivienda B
1	Cto. abierto	Aspiradora	14	Cto. abierto	Máquina de afeitar
2	Cto. abierto	Cargador tlf. móvil	15	Cto. abierto	Cto. abierto
3	Lampara	Módem HPAV	16	Lámpara	Cto. abierto
4	Módem HPAV	Cto. abierto	17	Módem HPAV	Lámpara
5	Cto. abierto	Cto. abierto	18	Cto. abierto	Módem HPAV
6	Cto. abierto	Cto. abierto	19	Módem HPAV	Módem HPAV
7	Cto. abierto	Cto. abierto	20	Cto. abierto	Cto.abierto
8	Máquina de afeitar	Lámpara	21	Cto. abierto	Módem HPAV
9	Módem HPAV	Cargador tlf. móvil	22	Cto. abierto	Cto. abierto
10	Lámpara	Cto. abierto	23	Lámpara	Cargador tlf. móvil
11	Cargador tlf. móvil	Módem HPAV	24	Módem HPAV	Cto. abierto
12	Aspiradora	Cto. abierto	25	Batidora	Cto. abierto
13	Cto. abierto	Lámpara	26	Cto. abierto	Batidora

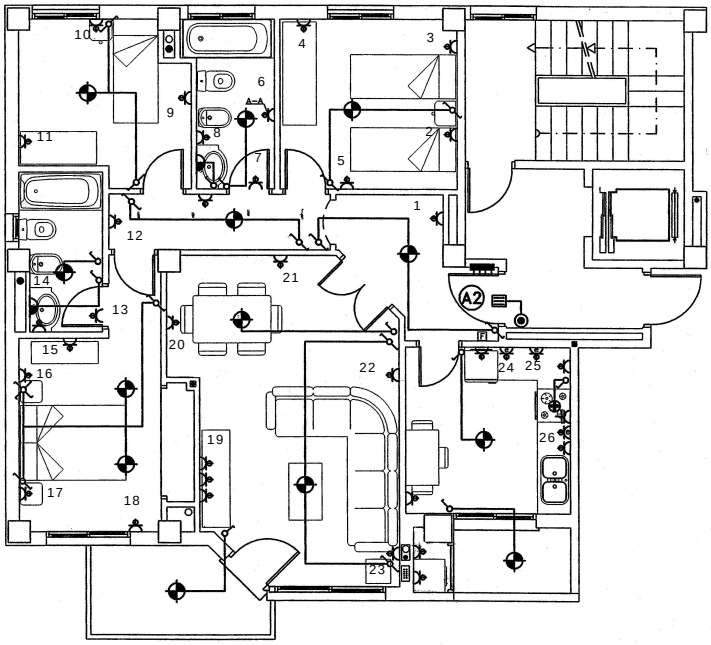


Fig. 3. Plano de las viviendas utilizadas en la simulación.

transmisor debería acceder al canal cuatro veces para el caso punto a punto mientras que solo debería acceder una vez en el metodo *multicast* propuesto. Teniendo en cuenta que el protocolo de acceso al medio introduce un retardo cada vez que se quiere acceder al canal (mayor cuanto mayor sea el tráfico remanente de la red), la diferencia de capacidades real sería incluso mayor que la que se muestra en la tabla.

B. Escenario II

El segundo escenario consiste en una transmisión a varios equipos situados en las dos viviendas (Viviendas A y B). Como en el primer escenario, el transmisor está situado en el enchufe 4A (es decir, el enchufe 4 de la vivienda A) y los restantes miembros del grupo *multicast* se sitúan en los enchufes 9A, 17A, 19A, 24A, 3B, 11B, 18B, 19B y 21B. En este caso cabe esperar que, debido a que la distancia entre la fuente de información y los equipos receptores de la otra vivienda será grande, el valor mínimo de la relación señal a ruido obtenido para cada portadora sea más bajo que en el escenario anterior.

La figura 5 muestra la SNR del canal entre cada pareja emisor-receptor. Además se muestra el mínimo valor de la SNR para cada frecuencia. Se puede observar como, para el caso de transmisiones entre diferentes viviendas, se obtienen incluso relaciones señal a ruido negativas para algunas portadoras. La tabla IV muestra la capacidad obtenida al realizar una transmisión entre cada pareja emisor-receptor, la capacidad obtenida en la comunicación *multicast* empleando transmisiones punto a punto y finalmente la capacidad obtenida mediante el modo de transmisión *multicast* propuesto.

De los resultados obtenidos se puede observar como, aunque el valor obtenido es menor que en el primer escenario, la capacidad *multicast* resultado del método propuesto sigue

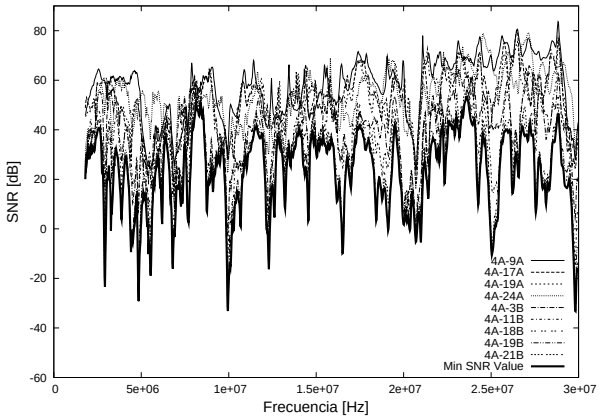


Fig. 5. SNR para las transmisiones del escenario II

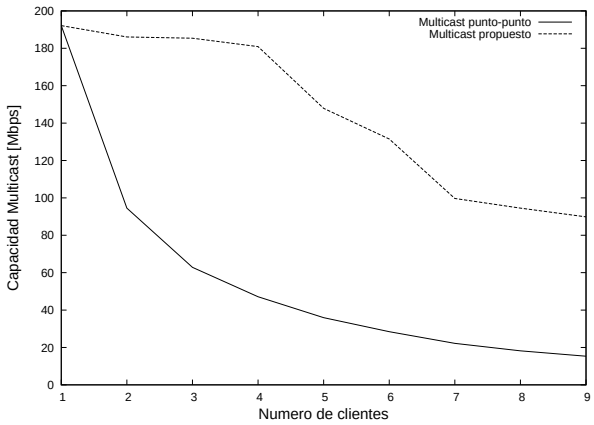


Fig. 6. Evolución de la capacidad de transmisión *multicast* en función del número de clientes para los dos métodos de transmisión *multicast* bajo estudio

Tabla IV
RESUMEN RESULTADOS ESCENARIO II

Enlace	C (Mbps)
4A - 9A	192.132
4A - 17A	186.092
4A - 19A	187.382
4A - 24A	188.414
4A - 3B	151.419
4A - 11B	136.071
4A - 18B	100.752
4A - 19B	101.096
4A - 21B	97.214
Multicast punto-punto	15.319
Multicast	89.853

siendo mayor que la obtenida mediante el método *multicast* punto a punto.

Debido a que el número de miembros del grupo *multicast* en este escenario es elevado, se puede estudiar como evoluciona la capacidad *multicast* a medida que se suscriben al grupo los diferentes usuarios. En la figura 6 se muestra la evolución de la capacidad *multicast* mediante el método propuesto y mediante transmisiones punto a punto. Los clientes se han ido añadiendo por número creciente de enchufe, y añadiendo en primer lugar los clientes conectados en la vivienda A y posteriormente los clientes de la vivienda B. Se observa que en el caso del método propuesto la capacidad apenas disminuye cuando se conectan los cuatro equipos de la primera vivienda. Sin embargo, cuando se comienzan a conectar los equipos de la segunda vivienda se produce una bajada apreciable de la capacidad de transmisión debido a que la relación señal a ruido de la comunicación con estos clientes es considerablemente inferior. También podemos apreciar que la capacidad obtenida con el método propuesto es mayor a la obtenida por el método de transmisiones punto a punto independientemente del número de clientes.

Por último, destacar que los valores de las gráficas dependerán del orden en el que se conecten los clientes, pero que el método propuesto estará en todos los casos por encima del método de transmisiones punto a punto. Esto se puede afirmar porque el método propuesto siempre proporciona una capacidad *multicast* que es ligeramente inferior a la capacidad de transmisión punto a punto del equipo más lento, mientras que en el caso del *multicast* mediante transmisiones punto a punto, como se aplica la ecuación 1, el valor de capacidad suele ser mucho menor.

V. CONCLUSIONES

La utilización de la tecnología PLC para el despliege de redes *in-home*, y en concreto la utilización del estándar HPAV (el más importante de esta tecnología) ofrece importantes limitaciones cuando se desean realizar transmisiones *multicast*. Esto es debido a que el método utilizado actualmente por la tecnología HPAV para la realización de comunicaciones *multicast* consiste en transmitir consecutivamente paquetes punto a punto a los diferentes miembros del grupo *multicast*

Las comunicaciones *multicast* son de gran utilidad en aplicaciones tales como los juegos en red y la distribución de contenidos multimedia, aplicaciones de éxito en redes *in-home* e *in-building*. Tenemos por tanto que es nesesario algún método que mejore su funcionamiento en redes HPAV.

En este trabajo se ha propuesto un nuevo método para la realización de transmisiones *multicast* en redes HPAV. Para comprobar su funcionamiento se ha desarrollado un simulador de canal PLC y se han realizado varias simulaciones de una topología compuesta por dos viviendas. Los resultados muestran que el método propuesto presenta unas caracteristicas muy superiores al método de transmisiones basado en transmisiones punto a punto, consiguiendo unas capacidad de transmisión de nivel físico que en algunos escenarios es varias veces superior a la obtenida con transmisiones punto a punto.

Además, con el método propuesto se obtienen otras ventajas añadidas como son que la capacidad de transmisión *multicast* no disminuye de manera importante a medida que aumenta el número de clientes del grupo *multicast*, y que el número de accesos del servidor al canal se reduce de manera importante, consiguiendo reducir los retardos provocados por el protocolo de acceso al medio.

AGRADECIMIENTOS

Este proyecto de investigación ha sido apoyado por la subvención de proyecto TEC2007-67966-C03-01/TCM (CONPARTE-1) y también ha sido desarrollada en el marco del “Programa de Ayudas a Grupos de Excelencia de la Region

de Murcia, de la Fundacion Seneca, Agencia de Ciencia y Tecnologia de la RM (Plan Regional de Ciencia y Tecnologia 2007/2010)". Pedro José Piñero Escuer también agradece a la Fundación Séneca la concesión de una beca predoctoral FPI (Exp. 13251/FPI/09).

REFERENCIAS

[1] M. Botterman. *Internet of Things: an early reality of the Future Internet. Workshop report*. 2009

[2] Y. J. Lin, H. A. Latchman, R. E. Newman and S. Katar. *A comparative performance study of wireless and power line networks*. IEEE Communications Magazine, 41(4):54-63, 2003.

[3] Homeplug Powerline Alliance. *http://www.homeplug.org*.

[4] HomePlug AV white paper. HomePlug Powerline Alliance. *http://www.homeplug.org/*. 2005

[5] Homeplug certified products. *http://www.homeplug.org/kshowcase/view*, 2009.

[6] Gigle semiconductors, *http://gigle.biz/*, 2009.

[7] Bahai, A. R. S., Saltzberg, B. R., Ergen, M., *Multi Carrier Digital Communications: Theory and Applications of OFDM*, Springer, 2004.

[8] Sancha, S.; Canete, F. J.; Diez, L.; Entrambasaguas, J. T., *A Channel Simulator for Indoor Power-line Communications*, Power Line Communications and Its Applications, 2007. ISPLC '07. IEEE International Symposium on, pp.104-109, 26-28 March 2007.

[9] F. J. Cañete, J. A. Cortés, L. Díez, and J. T. Entrambasaguas, *Modeling and evaluation of the indoor power line transmission medium*, IEEE Communications Magazine, 41(4):41-47, 2003.

Análisis multiresolución espacio-temporal de matrices de tráfico

David Rincón, Isaac Balasch
Departamento de Ingeniería Telemática (ENTEL), Escola Politècnica Superior de Castelldefels (EPSC)
Universitat Politècnica de Catalunya (UPC)
C/ Esteve Terrades, 7 08860 Castelldefels (Barcelona)
drincon@entel.upc.edu, isaacbalasch@gmail.com

Resumen- Las matrices de tráfico (*Traffic Matrices*, TM), definidas como la demanda de volumen de tráfico transportado entre dos nodos, son uno de los parámetros más importantes en las fases de diseño, despliegue y operación de una red de telecomunicaciones. Nuestro objetivo es modelar estas matrices de demanda, con el objetivo a largo plazo de proveer predicciones fiables de tráfico, y aplicar dicha predicción a planificación y provisión de servicio, ingeniería de tráfico, síntesis (para simulaciones), y detección de anomalías. Nuestra hipótesis es que dicho modelo debe ser disperso (en el sentido de tener pocos parámetros) y basado en análisis multiresolución (MRA). En el presente artículo se presenta un análisis espacio-temporal de matrices de tráfico de redes reales, mediante el uso de la transformada *Diffusion Wavelet*, que permite realizar el análisis multiresolución sobre estructuras topológicas complejas como por ejemplo, un grafo. La principal novedad respecto a trabajos anteriores es la introducción de un parámetro de correlación temporal que permite mejorar la compresibilidad de la señal y por tanto, avanzar en el desarrollo del modelo disperso. Los algoritmos han sido evaluados con datos provenientes de medidas de redes operativas, obteniendo resultados que mejoran los trabajos previos.

***Palabras Clave*- Caracterización de Tráfico, Matrices de Tráfico, Diffusion Wavelets, Análisis Multi-Resolución (MRA).**

I. INTRODUCCIÓN

La matriz de tráfico (*traffic matrix*, TM) o de demanda de una red se define como el volumen de tráfico enviado desde uno de los nodos a cualquiera de los otros durante un cierto intervalo temporal (típicamente del orden de algunos minutos u horas) [1, 2, 3]. Dada una red con N nodos, la TM se compone de N^2 entradas. La Fig. 1 muestra la topología de la red norteamericana Abilene y un ejemplo de matriz de tráfico de la misma, correspondiente a un intervalo de 5 minutos.

Las matrices de tráfico se pueden estudiar a diferentes escalas de agregación espacial del tráfico; por ejemplo, a nivel de usuarios individuales, redes locales, routers, puntos de presencia (PoPs, *Points of Presence*), o sistemas autónomos, por poner algunos ejemplos desde el caso con más granularidad hasta el de menos detalle. La propia estructura jerárquica de Internet permite definir un análisis multiescala de manera natural, agregando los flujos de tráfico correspondientes a cada nivel para obtener el nivel superior [2]. En el caso de la Figura 1 la TM se ha medido al nivel de PoP, con N=12 PoPs y se compone de N^2=144 elementos. Nótese que la cantidad de enlaces entre los 12 nodos es de K=30 (15 enlaces bidireccionales).

Dada su importancia en las tareas de ingeniería de red (monitorización de carga, detección de anomalías, predicción de saturación de los enlaces y provisión de red), el estudio de

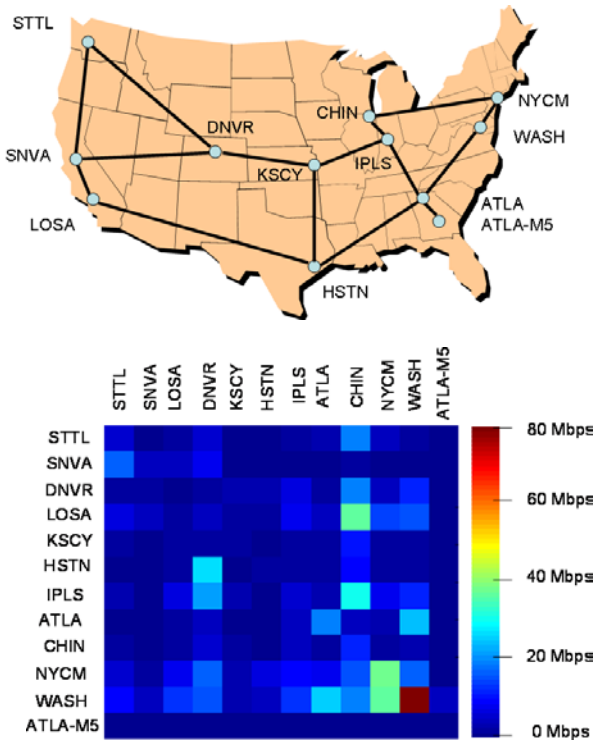


Fig. 1: Arriba: topología de los PoPs de Abilene en 2004. Abajo: matriz de tráfico de Abilene del día 3 de marzo de 2004 de 12:00 a 12:05.

las TM es de gran interés para los operadores [2, 3, 4, 5].

Nuestro objetivo a largo plazo es el desarrollo de modelos de TM y aplicarlos a predicción e ingeniería de tráfico. Partimos de la hipótesis, justificada en la Sección II, de que un modelo disperso (con pocos parámetros) es adecuado, y que éste puede ser obtenido mediante el analisis multiresolución (MRA, *MutiResolution Analysis*). Nuestro objetivo en el presente artículo es extender el análisis MRA estático que realizamos con la transformada Diffusion Wavelet en trabajos anteriores [1, 9] a una tercera dimensión que incluye el tiempo; es decir, queremos aprovechar la correlación temporal para comprimir más la señal (a más compresión, menos parámetros). Para ello procederemos a la estimación de la correlación existente en una serie de medidas de TM sobre las redes Abilene y Géant, construiremos un operador de difusión que integre esta correlación sobre el operador de gravedad, y analizaremos la compresibilidad de las matrices.

El resto del artículo se organiza como sigue. La sección II presenta con más detalle la motivación de nuestro trabajo, así

como conceptos y trabajos anteriores que son la base de nuestra contribución. La tercera sección describe el análisis multiresolución con la transformada Diffusion Wavelet. A continuación, la sección IV presenta los datos de Abilene y Géant, y el estudio del valor de autocorrelación de las matrices de tráfico. La quinta sección describe el método empleados para explotar el valor de autocorrelación en las matrices de tráfico conjuntamente con el modelo de gravedad. La sección VI muestra los resultados de los métodos descritos. El artículo finaliza con las conclusiones y líneas futuras de desarrollo.

II. MOTIVACIÓN Y CONCEPTOS PREVIOS

A. Medida e inferencia de las matrices de tráfico

Aunque existen herramientas de monitorización de flujos como Cisco Netflow o similares, las TM son difíciles de medir directamente, ya que las herramientas mencionadas presentan diversos problemas [7]: sobrecarga de la CPU de los routers, imprecisión en el muestreo (que es la solución a la sobrecarga), o la dificultad de sincronizar las medidas efectuadas en diferentes puntos de la red, entre otros retos.

Debido a estas dificultades, lo que tradicionalmente han hecho los operadores es o bien limitarse a monitorizar la carga de cada enlace (lo que limita enormemente la predicción de tráfico y las operaciones de ingeniería de tráfico), o bien hacer una estimación indirecta de las matrices de demanda a partir de medidas mucho más fáciles de obtener, que son los contadores SNMP de las interfaces de los routers (bytes enviados en los últimos 5 minutos). Existe una relación entre la carga de los enlaces (que podemos expresar como vector **y**, de longitud K, donde K es el número de enlaces unidireccionales) y la matriz de tráfico (expresada como vector **x,** de longitud N^2), a través de la matriz de encaminamiento **A** (de dimensiones K x N^2, cuyas entradas A_{ij} son 1 o 0 en función de que el enlace i pertenezca o no al conjunto de enlaces seguido por la ruta j)[1]. Bajo estas definiciones,

$$y = Ax \tag{1}$$

Sin embargo, estas medidas no nos dan suficiente información para recrear la TM original mediante

$$x = A^{-1}y \tag{2}$$

debido a la dimensionalidad del problema (N^2 incógnitas a partir de K datos, donde K es del orden de N y típicamente mucho más pequeño que N^2 – véase el ejemplo de la Fig. 1-) por lo que se necesitan datos adicionales para poder solucionar la ecuación (2), en forma de modelos *a priori* de la matriz de tráfico [4-7].

B. Modelos matemáticos para las TM

Tanto para solucionar el problema de inferencia descrito anteriormente, como para disponer de mecanismos de predicción de tráfico, de importancia capital para los operadores de telecomunicaciones, es necesario disponer de buenos modelos estadísticos. Sin embargo, pocos estudios han abordado las propiedades de las TMs, y un aspecto que no facilita en absoluto esta tarea de investigación es la dificultad de conseguir datos reales por parte de los operadores (al fin y al cabo, publicar los datos de tráfico podría convertirse en una ventaja comercial para sus competidores), lo que dificulta tanto el desarrollo de modelos de TM como su validación. Las redes financiadas con fondos públicos (GÉANT, Abilene, RedIris) ofrecen algo más de colaboración y en ocasiones han publicado sus TMs, ya sea con toda la información o parcialmente anonimizadas (véase [8], [17])

En nuestra opinión, una de las cualidades que debe cumplir un buen modelo es que sea disperso (*sparse*), en el sentido de tener un número de parámetros o coeficientes, M, mucho menor que el número de elementos de la matriz, es decir $M<<N^2$. Los argumentos a favor de un modelo de este tipo son, entre otros [9]:

- Si el modelo dispone de pocos parámetros será mucho más fácil asignarles sentido físico, y el modelo tendrá bases más razonables.
- Generalmente existe un compromiso entre la capacidad predictiva de un modelo, su fidelidad, y la cantidad de parámetros involucrados. Si se tienen muchos parámetros se puede obtener un modelo muy fiable para un cierto conjunto de datos, pero dará peores resultados como modelo predictivo porque será demasiado específico y difícilmente aplicable a otras situaciones.
- Si el modelo disperso tiene $M \leq K$ parámetros, quizá sea posible obtener una solución unívoca al problema de inferencia, o al menos una buena aproximación.

C. El modelo de gravedad

Existen algunos modelos dispersos en la literatura, como el modelo de gravedad (*Gravity Model*) [4, 7], que tiene tan sólo 2N parámetros ($2N << N^2$). El modelo de gravedad se basa en una suposición razonable, y que se cumple fielmente en el caso de la telefonía: el tráfico intercambiado entre dos nodos (centrales telefónicas) es proporcional al producto de las poblaciones de usuarios a las que dan servicio.

En el caso de las redes de datos no es tan fácil establecer una relación directa entre población y tráfico, pero sí se cumple con bastante fidelidad que se puede aproximar el factor de población por la medida del tráfico total saliente o entrante, de manera que el tráfico que viaja del nodo A al B es proporcional al producto del tráfico total que sale de A y el tráfico total que entra a B. Matemáticamente, obtenemos el modelo de gravedad a partir del tráfico total T_{total} (que corresponde a la suma de todos los valores de la TM) y los vectores de probabilidades p_{in} y p_{out} de longitud N (cada una de cuyas entradas corresponde a la fracción del tráfico total que entra o sale de cada uno de los nodos, respectivamente):

$$TM_{grav} = T_{total} \times p_{in} \times p_{out}^{\ T} \tag{3}$$

donde p^T indica vector traspuesto.

De la ecuación (3) se deduce rápidamente que el modelo de gravedad tiene rango 1, ya que por construcción TM_{grav} sólo tiene una fila y una columna linealmente independientes. Por tanto, el modelo de gravedad puede interpretarse como una aproximación de dimensionalidad

[1] En el caso, cada vez más habitual en las redes IP, en que se use encaminamiento ECMP (*Equal Cost MultiPath*), la matriz A podría tener entradas fraccionales (A_{ij} = 0.5 significaría que el enlace entre los nodos i y j sólo transporta el 50% del tráfico entre el nodo origen y el destino, y el resto se encamina por una ruta alternativa compuesta por otros enlaces).

mínima de la TM original (véase la Fig. 2). Finalmente, nótese que los parámetros del modelo son fácilmente medibles mediante los contadores SNMP de carga de los enlaces, ya que sólo hay que calcular la fracción del tráfico total que sale o en cada uno de los enlaces (es decir, normalizar los contadores respecto a la suma de todos ellos).

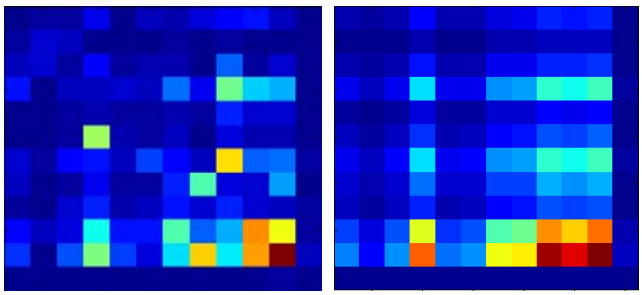


Fig. 2: Izquierda: Matriz de tráfico de Abilene. Derecha: modelo de gravedad obtenido a partir de la matriz de tráfico.

El modelo de gravedad se ha utilizado con un éxito razonable en el problema de inferencia [4, 7, 10], obteniendo buenas aproximaciones de la solución a las TM originales. Sin embargo, este modelo no es necesariamente una buena representación de la TM, sino que más bien es un modelo *a priori*, un punto inicial que luego es corregido mediante la proyección hacia la solución más cercana de las que pertenecen al espacio de soluciones posibles de la TM, es decir, el espacio de aquellas $\mathbf{x}$ que son soluciones de (2). A este proceso se le llama "tomogravedad" (Fig. 3), por analogía con los procesos tomográficos usados en equipos médicos.

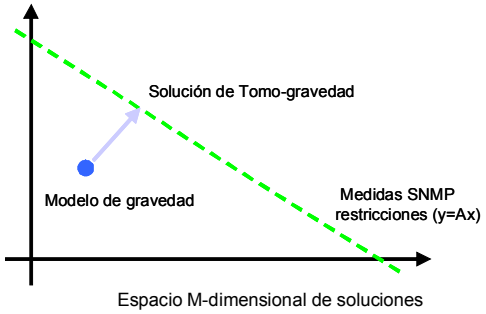


Fig. 3: Ilustración del proceso de tomogravedad (figura de M. Roughan).

D. *Trabajos anteriores*

En estudios anteriores [1, 9] hemos aplicado la técnica de Análisis Multiresolución (*Multi-resolution Analysis*, MRA) al estudio de las TM, con la esperanza de obtener una representación compacta, comprimida en pocos coeficientes. Intuitivamente, podemos considerar el MRA como un *zoom* a diferentes resoluciones o escalas: si miramos de cerca, vemos muchos detalles (alta frecuencia), pero si nos alejamos, obtenemos una visión global con pocos detalles (bajas frecuencias). Normalmente el MRA se realiza mediante la transformada wavelet, y se aplica a la compresión mediante la eliminación de las altas frecuencias [11]. En general MRA se puede entender como un decorrelador, en el sentido de reducir la representación de la señal a unos pocos parámetros en el dominio transformado, obteniendo así una señal transformada dispersa. Un punto importante de las transformadas wavelet es la existencia de algoritmos rápidos para su cálculo, habitualmente en forma de banco de filtros.

Sin embargo, no podemos llevar a cabo un análisis MRA estándar en TMs. Al contrario que en una imagen, donde podemos interpretar, intuitivamente, que se utiliza la información de los puntos adyacentes para aproximar el valor de un cierto pixel, la relación espacial entre los nodos de una red es mucho más compleja y depende de su topología. Por eso debemos utilizar técnicas específicamente diseñadas para MRA sobre grafos.

Una primera aproximación al MRA sobre grafos es [13], donde las *Graph Wavelets* (GW) se introdujeron como una extensión a la transformada wavelet 2D. Sin embargo, no dispone de un algoritmo computacional rápido, y la transformada no es ortonormal. Finalmente, la transformada Graph Wavelets no representa el tráfico de manera dispersa, sino que resulta en una descomposición redundante muy similar a la que obtenemos con la transformada wavelet continua (*Continuous Wavelet Transform*) [11].

Una herramienta más adecuada es la transformada *Diffusion Wavelet* (DW) [12], que permite no sólo el MRA de grafos (la topología de la red, en nuestro caso) sino también de funciones definidas sobre dichos grafos (la TM, por ejemplo). Los grafos representan la distribución de los nodos en la red subyacente y reflejan la relación espacial natural en la TM. Por ejemplo: dos nodos cercanos en la red es probable que tengan patrones de comportamiento semejantes, como por ejemplo la distribución de su actividad diurna, y es probable que ante alguna anomalía también se vean afectados simultáneamente, ya sea de manera similar u opuesta. La DW es matemáticamente sólida, dispone de algoritmos rápidos de cálculo, y es ortogonal [12].

En [1] se generaliza la DW a dos dimensiones, para estudiar TMs (que son función del nodo origen y el destino) y se estudia su aplicación al modelado de matrices de tráfico. Se observa, a partir de datos correspondientes a redes reales, que las matrices de tráfico en el dominio de las DW son dispersas y (relativamente) estables en tiempo, siendo la falta de esa estabilidad un síntoma de anomalías en la TM. En [9] se experimenta con diferentes operadores de difusión, entre ellos un operador basado en el modelo de gravedad, que permitió conseguir factores de compresión bastante elevados (del orden del 95% de la energía de la matriz original concentrada en sólo el 10% de coeficientes). En la Sección III se presentan detalles de estos análisis.

Los estudios anteriores se centraron en análisis estáticos, sobre matrices de tráfico aisladas, y aunque se realizaron sobre series largas de matrices, no aprovechaban en ningún caso la correlación inherente a las series de tráfico. Algunos estudios sobre el modelado de TMs han usado PCA (*Principal Component Analysis*) sobre las TMs como series temporales, y se centran en la correlación de los elementos de las TMs para separar los componentes periódicos del tráfico de las fluctuaciones aleatorias y otras anomalías [14]. Sin embargo, no queda claro cómo las estructuras descritas en llevarían a un modelo simple para usar en la síntesis de matrices de tráfico.

Finalmente, otro estudio a tener en cuenta es [15, 16], aunque se centra en otra aplicación de MRA, denominada *compressed sensing*, que consiste en el uso de pocas medidas para estimar correctamente un valor desconocido, determinando qué subconjunto de sensores son los más representativos. Zhang *et al*. [15] se centran en la inferencia de TMs, mientras que en una de las primeras aplicaciones de

la DW a redes de ordenadores, Coates *et al* [16] abordan el problema de encontrar el mínimo número de medidas necesarias para monitorizar extremo a extremo ciertas métricas de una ruta (por ejemplo el retardo en la capa IP o la tasa de error de bit en la capa física de una red óptica), mediante la transformada DW. La principal contribución del artículo es el uso de algoritmos de *compressed sensing*, pero es de especial interés en nuestro contexto porque los autores introducen el uso de series temporales en combinación con la DW, y concluyen que buena parte de la mejora de los resultados proviene de la correlación de las series de medidas. En dicho artículo se asume, sin justificación, que la similitud entre medidas consecutivas tiene un valor 0.5, y se construye un operador de difusión (el papel del cual se aclara en la Sección III) como el de la Fig. 4, en el que además de la relación espacial entre nodos (en este caso, la topología) se incluye la correlación temporal en un grafo tridimensional.

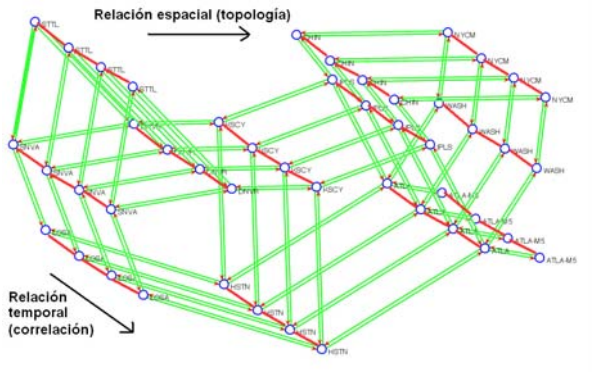


Fig. 4: Introducción de la correlación temporal al estilo [15]. Figura de [19].

III. Análisis Multiresolución de Matrices de Tráfico

A continuación se describirán los algoritmos de MRA sin entrar en detalles formales, que pueden consultarse en [9, 12].

A. MRA con Diffusion Wavelets

Dado un grafo $G\{V, A\}$ (donde V son los vértices y A las aristas), queremos aplicar MRA tanto al grafo como a cualquier función definida en los vértices. La técnica DW consiste en crear un *operador de difusión* que sea análogo a la función de escalado de la Transformada Wavelet "clásica" [11]. El operador de difusión se representa con la transformada lineal Tf, donde T se expresa como una matriz aplicada a la función (vector sobre el grafo) f. Aplicar este operador "difumina" la función a estudiar, f, sobre el grafo subyacente. Los valores de la función sobre nodos cercanos (cercanos en la topología del grafo) se mezclarán rápidamente, mientras que los lejanos se mantendrán separados. La DW se adapta intrínsecamente a la topología del operador sobre el que se definen las funciones anteriores.

En general podemos utilizar cualquier operador T que tenga un autoespectro (espectro de autovalores) decreciente y que esté normalizado de manera que el autovalor más grande sea 1. Una vez definido T, lo *dilatamos* tomando sus potencias. Intuitivamente, lo que hacemos es avanzar la difusión en una unidad de tiempo cada vez que multiplicamos T por sí misma; por tanto, tras n instantes temporales, se aplica la transformada lineal n veces, es decir $T^n f$. Esto da como resultado un difuminado espectral de la función.

En grafos, el equivalente natural de descomposición espectral resultante de la DWT es la teoría espectral de grafos: esto es, el estudio de los autovalores y autofunciones de operadores lineales. El Teorema Espectral permite la siguiente representación del operador lineal T,

$$T = \sum_{i=1} \lambda_i v_i^T v_i \qquad (3)$$

donde λ_i son los autovalores de T, y v_i son sus autovectores.

Tras el cálculo de cada potencia de T, ignoraremos los autovalores inferiores a un cierto nivel $|\lambda_i| \le \varepsilon$, donde ε es un parámetro configurable con un valor pequeño (entre 10^{-3} y 10^{-15} en nuestros experimentos). Unos pocos autovalores (en el caso que quedaran por debajo de ε) se descartan en el primer paso, y el proceso se itera al considerar las potencias de T. La aplicación sucesiva del operador de difusión divide el espectro original del grafo en subbandas, y podemos definir el MRA de la siguiente manera: para una escala dada j, los autovectores asociados con $|\lambda_i^{2^j}| \ge \varepsilon$ expanden el subespacio V_j de la aproximación de baja frecuencia, mientras los autovectores asociados con los autovalores descartados en el paso j-ésimo (aquellos que $|\lambda_i^{2^j}| < \varepsilon$ y $|\lambda_i^{2^{j-1}}| \ge \varepsilon$ expanden el subespacio de alta frecuencia o de detalle W_j. La Figura 5 ilustra el proceso.

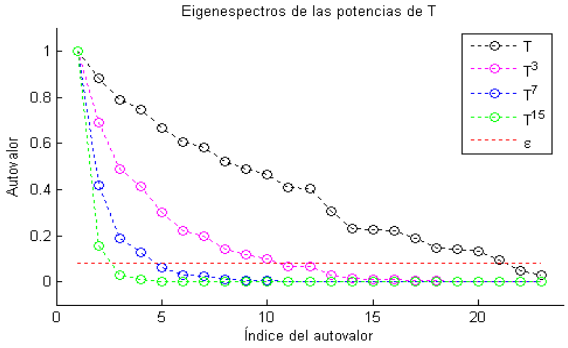


Fig. 5. Autoespectro de las potencias de un operador T. Los autovalores por debajo de ε en cada paso generan los subespacios W_j y los restantes, los V_j.

B. Extensión de Diffusion Wavelets a funciones 2D

Las matrices de tráfico son funciones bidimensionales $F(v_1, v_2)$ de pares de vértices donde v_1 es el nodo origen del tráfico, v_2 el nodo de destino, y $F(v_1, v_2)$ es el volumen de tráfico entre v_1 y v_2. Dado que la transformada DW en su forma original sólo se puede aplicar a funciones bidimensionales, debemos extender y adaptar la DW al caso 2D.

Las wavelets clásicas unidimensionales se pueden utilizar en análisis de imagen para construir una base en 2D combinando la aplicación de sucesivos filtros paso alto y paso bajo en las dimensiones horizontal y vertical de la imagen de entrada I(x,y), generando así 4 subbandas en cada escala con las cuatro combinaciones posibles de esos dos filtros: PB-PB (aproximación) y PB-PA, PA-PB y PA-PA (detalles). El proceso se itera tomando como entrada la aproximación (la salida del primer PB-PB).

La DW en 2D se construye de manera similar: simplemente aplicamos el proceso dos veces, en las dimensiones "entrada" y "salida" de la matriz de tráfico, obteniendo el producto de las subbandas [1]. De manera

similar a como hacíamos con las DW en 1D, llamaremos, en este caso, C_{VV_j}, C_{VW_j}, C_{WV_j} y C_{WW_j} a los coeficientes de la transformada que corresponden a los subespacios VV_j, VW_j, WV_j y WW_j respectivamente (donde VV se refiere al subespacio de la aproximación o baja frecuencia y WW al subespacio del detalle o alta frecuencia). La transformada 2D resultante verifica las propiedades deseables de invertibilidad (podemos reconstruir la función original a partir de sus coeficientes), ortonormalidad y separabilidad.

Dado que (al menos por ahora) no encontramos utilidad en la diferenciación de las subbandas cruzadas, reescribimos la subbanda paso bajo VV_j como V_j, y la paso alto W_j como la unión de VW_j, WV_j y WW_j.

C. *Resultados previos con operadores estáticos*

En [1, 9, 19] se describen los resultados obtenidos con los algoritmos descritos cuando se aplican a datos reales de TMs correspondientes a las redes Abilene y Géant, usando diferentes operadores de difusión. La métrica de interés aquí es la representación del error cuadrático medio (correspondiente a la diferencia entre la matriz original y las aproximaciones de baja frecuencia conseguidas con la DW), en función del porcentaje de coeficientes usados; es decir, representamos la energía conservada por los coeficientes más representativos, tal como se ilustra en la Figura 6. El operador de topología consiste en definir un *random walk* a partir de la topología de la red (es decir, se define una matriz de adyacencia donde la probabilidad de saltar hacia otro nodo *j* es igual al inverso de la suma de enlaces que salen del nodo inicial *i*). El operador de gravedad explota la idea de "correlación espacial" implícita en el modelo de gravedad, ya que corresponde a los valores normalizados (probabilidades) del modelo de gravedad, y su interpretación intuitiva es que dos nodos origen-destino están correlados de manera proporcional al tráfico que intercambian. Como puede verse en la Figura 6 y la Tabla 1, los resultados mejoran notablemente con el operador de gravedad.

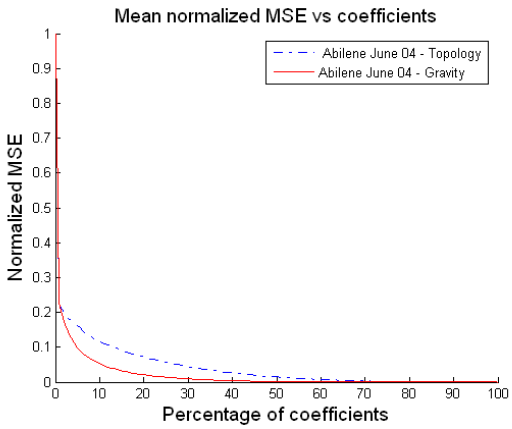


Fig. 6: Error cuadrático medio normalizado en función del porcentaje de coeficientes de la DW para una traza Abilene con dos operadores diferentes.

	90% energía	95% energía
Topología	13.1 %	26.8 %
Gravedad	4.9 %	11.0 %

Tabla 1. Porcentaje de coeficientes necesarios para preservar ciertas fracciones de la energía original en la traza Abilene Junio 2004 (8640 TMs).

IV. Estudio de la autocorrelación de las TM

A continuación se presenta el estudio de la correlación temporal de las matrices de tráfico, paso cuantificar el valor que se usará en el operador de difusión espacio-temporal.

A. *Descripción de los datos*

Disponemos de más de 20000 matrices de tráfico pertenecientes a dos conjuntos de datos de las redes académicas Abilene (EEUU) y Géant (Europa), con 12 y 23 PoPs respectivamente. La granularidad de las TM es de 5 minutos en el caso de las de Abilene, y de 15 minutos en las de Géant. Para más detalles sobre estos datasets véase [8, 17, 18]. Para Abilene se cuenta con datos que se extienden durante 6 meses consecutivos (marzo a septiembre 2004), pero desafortunadamente el *dataset* no es contiguo y contiene numerosos "agujeros" de discontinuidad temporal. En el caso de Géant, a pesar de tener más continuidad, los datos están anonimizados tanto en tiempo (a pesar de que el *dataset* se inicia el 1 de enero de 2005, no podemos asegurar que la fecha sea la real) como en espacio (en vez del nombre de los nodos, disponemos sólo de números, lo que imposibilita su identificación sobre la topología de la red), pero estas limitaciones no afectan a nuestros análisis.

B. *Metodología del estudio y resultados*

El objetivo del estudio inicial es el de encontrar un valor de autocorrelación que se utilice posteriormente para realizar el análisis espacio-temporal multiresolución de matrices de tráfico. Dado que vamos a relacionar cada TM con la anterior, vamos a centrarnos en la autocorrelación a distancia 1 de cada una de las series temporales que se obtienen al considerar el valor de tráfico de cada posición x_{ij} de la TM. Este estudio se hará para cada día (288 matrices). Nótese que estamos asumiendo estacionariedad, lo cual consideramos razonable dado que los intervalos son de 5 y 15 minutos entre pares de TM consecutivas. Posteriormente calculamos la media de las autocorrelaciones diarias de cada una de las rutas de Abilene. Este estudio fue realizado obteniendo los valores de autocorrelación de cada una de las rutas para cada uno de los 167 días de los que se disponen datos.

En un principio el valor de autocorrelación media fue 0.751, pero el estudio de cada una de las rutas desveló que existían rutas que, ya fuera en momentos puntuales o de forma continuada, se mostraban inestables, por lo que procedimos a filtrarlas. Se tomó como criterio de filtrado el hecho de presentar inestabilidad (correlación inferior a 0.5) más del 50% de los días estudiados, es decir a partir de 84 días inestables, con el resultado de 7 rutas inestables de las 144 totales. Prácticamente todas involucran el nodo ATLA-M5, un nodo periférico de Abilene (ver Fig. 1) que genera y recibe muy poco tráfico y a ráfagas, lo que por una parte redunda en inestabilidad relativa, y por otro nos permite eliminar las rutas sin miedo a perder representatividad de la medida. La media de la autocorrelación, una vez descartadas las rutas inestables, tampoco varía sensiblemente y queda en un valor de 0.773. En la Fig. 7 se muestra, en el grafico superior los valores de autocorrrelación de cada una de las rutas y en el inferior únicamente los valores de auto-correlación de las rutas que se han considerado estables.

En el caso de Géant, las autocorrelaciones son bastante más variables, y a pesar de hacer un filtrado mínimo, prácticamente todas las rutas presentan una gran variabilidad.

Este es un hecho conocido y descrito por otros trabajos (ver [22], por ejemplo) y es debido a que el tipo de usuarios finales y la dinámica de las demandas de tráfico son muy diferentes en las dos redes. Por ejemplo, Géant proporciona a sus clientes (los ISPs académicos nacionales, RedIris en el caso español) el servicio de acceso a la Internet global, mientras que Abilene no lo hace. El resultado para Géant es una correlación media a distancia 1 de valor 0.557, claramente inferior a Abilene y mucho más incorrelado.

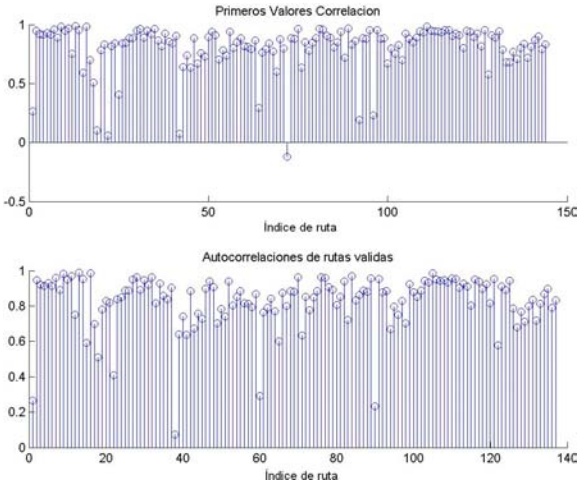


Fig. 7: Valores de la autocorrelación para cada una de las rutas, sin filtrar (arriba) y una vez filtradas las rutas inestables (abajo), para la traza Abilene.

V. Análisis espacio-temporal

Una vez descritos los operadores estáticos (de los que destaca el operador de gravedad) y el cálculo de la autocorrelación, pasamos a comentar como integramos estos dos elementos en un operador espacio-temporal. Nuestra idea es crear un operador tridimensional que, por un lado, contenga el operador de difusión en cada instante temporal, y que además una los diferentes planos temporales a través de la correlación calculada, tal como se ilustra en la Figura 8.

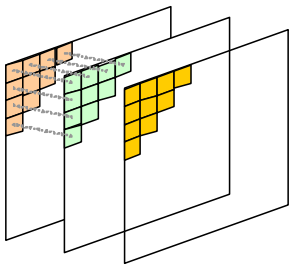


Fig. 8: Operador espacio-temporal. Cada plano corresponde a un operador estático (un instante temporal), y los trazos en gris corresponden a la correlación temporal, uniendo cada ruta con su valor anterior y posterior.

Un problema a solucionar es que, tal como está construido el código Matlab de la DW [21], el operador de difusión se define como una matriz bidimensional, lo que funciona perfectamente para análisis estáticos. Aunque lo ideal sería modificar el código DW para ser "nativo 3D", y es una de las líneas en las que estamos trabajando, requiere cambios estructurales en el código, lo que no es nada trivial ya que están involucradas diversas rutinas optimizadas (código Matlab pasado a C) y no disponemos de todo el código fuente. Por ahora la única solución de la que disponemos, y con la que queremos validar nuestras hipótesis antes de pasar a modificaciones más importantes del código, es la de crear una supermatriz de difusión construida a partir de bloques NxN, de manera que cada bloque de la diagonal corresponda a un instante temporal (un operador completo) y las relaciones temporales aparezcan en los bloques NxN adyacentes a la diagonal, creando bloques donde todos los valores sean idénticos a la autocorrelación calculada. De esta manera unimos temporalmente el valor de cada ruta con ella misma en los instantes anterior y posterior. El resto de la matriz tiene los valores a cero. La Fig. 9 ilustra la técnica utilizada. El operador resultante es simetrizado (por exigencias de construcción de la transformada Diffusion Wavelet) y normalizado a su autovalor más grande, para conseguir un autovalor 1. Estas operaciones también se han realizado en los estudios estáticos (véase [19, 20]).

Operador gravedad 1	0.773	0
0.773	Operador gravedad 2	0.773
0	0.773	Operador gravedad 3

Fig. 9: Esquema de construcción del operador espacio-temporal, para el caso de 3 matrices Abilene. Cada uno de los cuadros corresponde a bloques NxN.

De cara a comparar en igualdad de condiciones la introducción de la correlación temporal, se presentarán también resultados obtenidos con una supermatriz en la que sólo aparecen los bloques de la diagonal (los operadores de difusión). Esencialmente, es idéntico a los resultados aislados (TM a TM) que ya hemos presentado en la Sección III, pero hechos en bloques de una hora (12 TMs Abilene en bloque, pero aisladas).

VI. Resultados

A. Introducción

Se han realizado diversos estudios, limitados por la potencia computacional que requieren los algoritmos, y por el hardware disponible. Por un lado, el hecho de ser pruebas de concepto iniciales ha hecho que la eficiencia del código no sea nuestra prioridad (lo será una vez abordemos el desarrollo del operador "3D nativo" descrito en la Sección V); por otro lado, sólo disponíamos de ordenadores relativamente lentos para hacer nuestras pruebas.

La métrica utilizada es la misma descrita en estudios anteriores e ilustrada en la Fig. 6: la representación del error cuadrático medio (MSE, *mean square error*) cometido al reconstruir la TM original a partir de un cierto número de coeficientes (ordenados éstos por su contribución total a la energía de la matriz original); es decir, el error cometido por las aproximaciones de baja frecuencia de la TM obtenidas con el análisis MRA. El MSE se normaliza a 1 dividiéndolo entre la energía inicial de la matriz (la suma del cuadrado de todos sus coeficientes). Las curvas MSE-procentaje presentan un codo cercano al origen; a más compresión, más abrupto es el codo, y más compresible son los datos.

B. *Pruebas iniciales de validación*

Inicialmente se probó el funcionamiento del algoritmo completo espacio-temporal en intervalos de una hora (12 matrices) de Abilene, correspondiente a un período que nos pareció estadísticamente representativo (desde el punto de estabilidad y volumen de tráfico), correspondiente al intervalo 2004-07-05-1800 a TM-2004-07-05-1855. El análisis se hizo también sobre una hora representativa de Géant (4 matrices), con resultados similares. La Figura 10 ilustra los resultados obtenidos con $\varepsilon=10^{-10}$, que concentran más del 99% de la energía inicial (MSE=0.01) con sólo el 4.4% de los coeficientes. La Tabla 2 presenta la comparación entre el análisis estático y el espacio-temporal, donde se puede ver que la compresión aumenta notablemente.

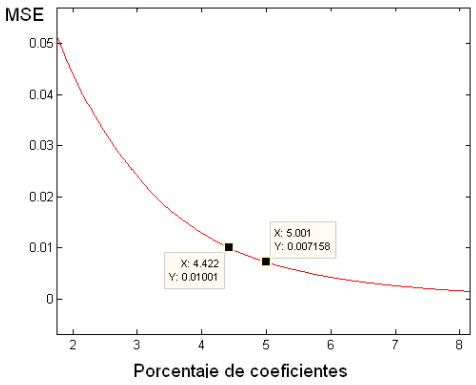


Fig. 10: (ampliación del codo) Error cuadrático medio en función del porcentaje de coeficientes usados en la reconstrucción, para una hora de Abilene (18:00-18:55) con el operador espacio-temporal y $\varepsilon=10^{-10}$.

% Energía	Temporal	Estático
50%	0.60 %	1.39 %
90%	3.26 %	11.06 %
99%	7.76 %	35.90 %

Tabla 2. Comparación de la concentración de energía para el caso estático y el espacio-temporal, para una hora de Abilene (18:00-18:55) y $\varepsilon=10^{-8}$.

Nótese que en los datos anteriores cambia ε, el parámetro que controla el "ancho de banda" (en autovalores) de la descomposición espectral, por lo que se realizó un estudio para determinar su influencia. Sabemos, por estudios anteriores sobre operadores estáticos [1, 9, 12] que cambiar ε en un margen razonable (10^{-4} a 10^{-15}), aunque hace fluctuar ligeramente la compresión, no hace cambiar significativamente los resultados; es decir, la distribución concreta de los autovalores en las subbandas espectrales no se ve excesivamente afectada. La tabla 3 presenta un par de ejemplos con el peor caso encontrado ($\varepsilon = 10^{-8}$) y otro más representativo ($\varepsilon = 10^{-15}$) para Abilene; en el caso de Géant los resultados son casi invariantes, pero se ha mantenido el valor de ε para ser coherentes.

	Abilene		Géant	
% Energía	$\varepsilon = 10^{-8}$	$\varepsilon = 10^{-15}$	$\varepsilon = 10^{-8}$	$\varepsilon = 10^{-15}$
50%	0.60 %	0.49 %	0.97 %	0.99 %
90%	3.26 %	2.62 %	6.18 %	6.13 %
99%	7.76 %	5.18 %	13.59 %	13.54 %

Tabla 3. Variación del porcentaje de concentración de energía en los coeficientes DW para diferentes casos de ε, para trazas de una hora de Abilene (12 matrices) y Géant (4 matrices).

C. *Estabilidad de los resultados*

De cara a evaluar la estabilidad de los resultados obtenidos, se realizó el mismo estudio de 1 hora de Géant y Abilene, pero durante 7 días consecutivos, lo que además nos permitiría detectar efectos relacionados con la variación de volumen de tráfico entre días laborables y fin de semana. El intervalo temporal escogido para Abilene fue la franja 09:00 a 09:55, y para Géant de 08:00 a 08:45. Las Tablas 4 y 5 presentan los resultados, donde destaca la notable estabilidad obtenida.

Abilene	Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7
50 %	0.43%	0.47%	0.54%	0.25%	0.53%	0.54%	0.53%
90 %	2.38%	2.54%	2.58%	2.14%	2.65%	2.64%	2.75%
99 %	5.08%	5.30%	5.22%	4.69%	5.33%	5.41%	5.49%

Tabla 4. Porcentaje de coeficientes necesarios para un cierto nivel de conservación de la energía original. Estudio de una hora de Abilene durante 7 días consecutivos, en la franja horaria 09:00-09:55, con $\varepsilon=10^{-15}$.

Géant	Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7
50 %	1.06%	1.04%	1.02%	1.19%	1.06%	1.08%	1.00%
90 %	6.19%	6.02%	6.29%	6.57%	6.39%	5.71%	5.58%
99 %	13.72%	13.68%	13.99%	14.19%	13.52%	13.15%	12.38%

Tabla 5. Porcentaje de coeficientes necesarios para un cierto nivel de conservación de la energía original. Estudio de una hora de Géant durante 7 días consecutivos, en la franja horaria 08:00-08:45, con $\varepsilon=10^{-15}$.

VII. CONCLUSIONES

El presente artículo presenta el que, a nuestro entender, es el primer método de análisis espacio-temporal multi-resolución de matrices de tráfico. Teniendo en cuenta que el estudio, por razones de coste computacional, se ha realizado con un pequeño conjunto de muestras de matrices de tráfico, no se puede dar como definitivo, pero las pruebas realizadas apuntan en el sentido de mejorar los resultados del que hasta ahora era el operador más potente en cuanto a compresibilidad, que es el basado en el modelo de gravedad estático.

Nuestros esfuerzos se centran ahora en corroborar empíricamente la potencia del método desarrollado en series más largas de TMs, de días o (idealmente) semanas de duración. Dado el coste computacional no es fácil ir más allá de estas duraciones, pero desde el punto de vista práctico es probable que el horizonte de horas o un día sea suficiente para alcanzar una compresibilidad suficiente para empezar la segunda fase del estudio, que consistirá en la identificación de los parámetros que concentran la energía, estudiar su estabilidad temporal, y construir el modelo disperso de la TM en base a ellos. Para más adelante queda el estudio de la predictibilidad de las series de TM a partir del modelo, lo que nos permitiría cerrar el proceso y ofrecer a la comunidad una potente herramienta de modelado y predicción de tráfico.

Otra línea de trabajo consiste en explorar la aplicación del método a la detección de anomalías (en [1] se presentó una prueba de concepto que todavía no se ha explorado en profundidad) y el uso de operadores de difusión alternativos

que permitan integrar, por sí solos y no mediante un proceso externo (tal como hacemos ahora) la dimensión temporal al análisis multiresolución de las matrices de tráfico. Consideramos este estudio el primer paso y la justificación de un esfuerzo posterior que debe culminar en la adaptación del código de cálculo de la Diffusion Wavelet para crear un operador espacio-temporal "nativo", en el sentido de evitar la adaptación a través de la supermatriz que nos permite combinar el operador estático junto con su correlación temporal.

Finalmente, sería muy conveniente comparar los resultados obtenidos con trazas más actuales de la redes Abilene y Géant (pese a las dificultades para obtenerlas, que ya se han descrito) y los que se puedan obtener otras redes, como RedIris.

AGRADECIMIENTOS

Los autores quieren expresar su agradecimiento los revisores anónimos por sus comentarios y sugerencias de mejora, así como a Yin Zhang de la University of Texas por los datos de Abilene, y a Steve Uhlig y el equipo del proyecto TOTEM por los datos de GÉANT, así como a Matthew Roughan (University of Adelaide), Walter Willinger (AT&T) por sus comentarios e ideas, y a Mauro Maggioni por publicar el código Matlab de la Diffusion Wavelet y por sus comentarios.

Este trabajo ha sido financiado parcialmente por el MICINN y FEDER (TEC2009-13901-C02-01), el proyecto GÉANT 3 y EuroNF (INFSO-ICT-216366).

REFERENCIAS

[1] D. Rincón, J. Torres. Contribuciones al análisis multiresolución de matrices de tráfico. Jornadas de Ingeniería Telemática JITEL 2009, Cartagena, España, Septiembre 2009.

[2] D.L. Alderson, H. Chang, M. Roughan, S.Uhlig, and W. Willinger. The many facets of Internet topology and traffic. *Networks and Heterogeneus Media,* 1(4): 569-600, Dec. 2006.

[3] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, and F. True. Deriving traffic demands for operational IP networks: Methodology and experience. *IEEE/ACM Transactions on Networking*, pp. 265-279, Jun. 2001.

[4] M. Roughan, M. Thorup, and Y. Zhang. Traffic engineering with estimated traffic matrices. *Procs. of ACM IMC 03*, pp. 248-258, 2003.

[5] A. Medina, N. Taft, K. Salamatian, S. Bhattacharyya, and C. Diot. Traffic matrix estimation: existing techniques and new directions. *SIGCOMM Comput. Commun. Rev.*, 32(4):161-174, 2002.

[6] Y. Vardi. Network tomography: estimating source-destination traffic intensities from link data. *J. of the Am. Stat. Ass.*, 91:365-377, 1996.

[7] Y. Zhang, M. Roughan, N. Duffield, and A. Greenberg. Fast accurate computation of large-scale IP traffic matrices from link loads. *ACM SIGMETRICS*, pp. 206-217, San Diego, California, Jun. 2003.

[8] S. Uhlig, B. Quoitin, J. Lepropre, and S. Balon. Providing public intradomain traffic matrices to the research community. *SIGCOMM Computer Communication Review*, 36(1):83-86, 2006.

[9] D. Rincón, M. Roughan, W. Willinger. Towards a Meaningful MRA of Traffic Matrices. *Proceedings of ACM IMC 2008*, pp. 331-336, 2008.

[10] Y. Zhang, M. Roughan, C. Lund, and D. Donoho. An information-theoretic approach to traffic matrix estimation. *ACM SIGCOMM*, pp. 301-312, Aug. 2003.

[11] S. Mallat. *A Wavelet Tour of Signal Processing*. Academic Press, 1999.

[12] R. R. Coifman and M. Maggioni. Diffusion Wavelets. *Applied and Computational Harmonic Analysis*, 21(1):53-94, Jul. 2006.

[13] M. Crovella and E. Kolaczyk. Graph wavelets for spatial traffic analysis. *Proceedings of IEEE Infocom*, pp. 1848-1857, Apr. 2003.

[14] A. Lakhina, K. Papagiannaki, M. Crovella, C. Diot, E. D. Kolaczyk, and N. Taft. Structural analysis of network traffic flows. *SIGMETRICS Perf. Eval. Rev.*, 32(1):61-72, 2004.

[15] Y. Zhang, M. Roughan, W. Willinger, L. Qui, Spatio-Temporal Compressive Sensing and Internet Traffic Matrices, ACM Sigcomm, pp.267--278, Barcelona, August 2009.

[16] M. Coates, Y. Pointurier, and M. Rabbat. Compressed network monitoring for IP and all-optical networks. *Proceedings of ACM IMC 2007*, pp. 241-252, 2007.

[17] Y. Zhang's homepage. Abilene Traffic Matrices [online]. http://www.cs.utexas.edu/yzhang/research/AbileneTM/

[18] TOTEM project. http://totem.run.montefiore.ulg.ac.be/datatools.html.

[19] J. Torres, Modelling of traffic matrices with multiresolution analysis techniques. Trabajo fin de carrera, EPSC, UPC, Barcelona, Oct. 2009.

[20] I. Balasch, Anàlisi Espai-Temporal Multiresolució de Matrius de Teletrànsit**,** Trabajo fin de carrera, EPSC, UPC, Barcelona, Junio 2010.

[21] M. Maggioni, DW Matlab code, http://www.math.duke.edu/~mauro/code.html

[22] A. Soule et al, Challenging the supremacy of traffic matrices in anomaly detection. Internet Measurement Conference (IMC), pp 105-110, San Diego, USA 2007.

Implementación y evaluación de la codificación LDPC para la transmisión de ficheros en entornos unidireccionales

Ismael de Fez, Francisco Fraile, Román Belda, Juan Carlos Guerri
Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM)
Universidad Politécnica de Valencia
Camino de Vera s/n, Edificio 8G, 46022 Valencia
isdefez@iteam.upv.es, ffraile@iteam.upv.es, robelor@iteam.upv.es, jcguerri@dcom.upv.es

***Resumen*- La utilización de mecanismos FEC (*Forward Error Correction*) proporciona una mayor fiabilidad en la transmisión de contenido IP en entornos con pérdidas. De entre los distintos tipos de códigos FEC existentes, este artículo presenta una completa evaluación sobre la codificación LDPC (*Low Density Parity Check*) basada en una implementación propia de dicha codificación, según las características definidas por la RFC 5170. Dicha evaluación muestra las ventajas que supone el empleo de codificación a nivel de paquete en la transmisión de ficheros en entornos unidireccionales, y realiza una comparación entre dos tipos de estructuras LDPC: Staircase y Triangle.**

***Palabras Clave*- LDPC, FLUTE, AL-FEC, Descarga de ficheros.**

I. INTRODUCCIÓN

En los últimos años se ha producido un auge en la utilización de redes inalámbricas en la industria de las comunicaciones. No hay más que ver la cantidad de tecnologías que han aparecido, como Wi-Fi, DVB, UMTS, WiMAX, *bluetooth*… Uno de los aspectos clave en el diseño de estas tecnologías es la fiabilidad que proporcionan en la transmisión.

Para mejorar las comunicaciones resulta necesario utilizar mecanismos de protección frente a errores, ya que en las redes inalámbricas se producen pérdidas en la transmisión. Los sistemas de corrección de errores aparecieron prácticamente con el nacimiento de las telecomunicaciones. En un medio de transmisión, ya sea por cable o inalámbrico, siempre se producen errores en el canal, por lo que la existencia de herramientas que detecten y, sobre todo, corrijan dichos errores es algo esencial en cualquier sistema de comunicación.

Aparte de errores a nivel de bit, se pueden producir errores a nivel de paquete, es decir que haya pérdidas en el canal que propicien que un paquete enviado no sea recibido. Para proporcionar protección frente a esta clase de errores, más allá de las técnicas de detección de errores como ARQ (*Automatic Repeat Request*), se emplean mecanismos FEC (*Forward Error Correction*), que permiten reconstruir un paquete que no se ha recibido. FEC se utiliza principalmente en entornos unidireccionales, en los cuales no existe un canal de retorno, o en sistemas en tiempo real en los que la retransmisión de paquetes no resulta válida. La utilización de este tipo de técnicas provoca una disminución del tiempo de recepción de un contenido y una reducción del tráfico en la red, ya que evita la solicitud de paquetes perdidos (lo cual no es siempre posible dependiendo del tipo de canal).

Existen distintas categorías principales de FEC: los códigos convolucionales, los códigos bloque, los códigos fuente y los sistemas híbridos. En los códigos bloque existen diferentes codificaciones, entre las más conocidas se encuentran Reed-Solomon y la recuperada codificación LDPC, nacida en los años 60.

Precisamente, este artículo se centra en el análisis, implementación y evaluación de la codificación *Low Density Parity Check*.

II. TRANSMISIÓN DE FICHEROS EN REDES INALÁMBRICAS MULTICAST

A. Redes inalámbricas multicast

Actualmente existen muchos tipos de redes inalámbricas de difusión estandarizadas. Entre los diversos organismos de estandarización y familias existentes se encuentran DVB, 3GPP y Mobile IPTV, entre otros.

DVB (*Digital Video Broadcasting*) es una organización cuyo objetivo es la creación de estándares técnicos de televisión digital y de servicios de difusión de datos. Dichos estándares se utilizan, sobre todo, en Europa. DVB ha definido distintos sistemas que regulan la distribución de contenido por satélite (DVB-S), por cable (DVB-C), por televisión terrestre (DVB-T) y por televisión terrestre para dispositivos móviles (DVB-H) [1].

Dentro de la amplia gama de estándares que componen el 3G se encuentran los estándares de difusión broadcast MBMS (*Multimedia Broadcast and Multicast Services*) [2] e IMB (*Integrated Mobile Broadcast*) [3]. Ambos estándares utilizan el espectro 3G, el cual ya está regulado y en el que su explotación no requiere de nuevas licencias, al contrario de lo que sucede en DVB.

La última red de difusión señalada es Mobile IPTV [4]. Esta tecnología permite el envío y recepción de contenido multimedia (como televisión digital o servicios de voz) a través de redes de cable e inalámbricas basadas en IP. Proporciona calidad de servicio, seguridad, movilidad y funciones interactivas. Mobile IPTV extiende las funcionalidades del estándar de televisión IPTV para adaptarlas a los dispositivos portátiles.

A la hora de transmitir un contenido, si éste es un fichero no se deben producir errores en la transmisión. Para que un receptor pueda reconstruir correctamente un fichero es necesario recibir todos y cada uno de los paquetes que lo componen. Es por ello que las redes de difusión vistas necesitan garantizar que el contenido que transmiten llega correctamente a los receptores. El problema es que este tipo de redes, por ser casi todas unidireccionales, carecen de mecanismos que proporcionen seguridad en la transmisión. Resulta, pues, necesario el uso de un protocolo que garantice que en la transmisión no se produzca ningún error o, en su caso, que, aunque se produzcan errores, el receptor sea capaz de recuperar el paquete original. El protocolo utilizado para los servicios de descarga de contenido a móviles por los diferentes organismos de estandarización es FLUTE.

B. *FLUTE*

1. *Descripción*

FLUTE (*File Delivery over Unidirectional Transport*), definido en la RFC 3926 [5], es un protocolo para el envío unidireccional de ficheros sobre Internet, especialmente adecuado para redes multicast.

La principal característica de FLUTE es que ofrece fiabilidad en la transmisión. Además, proporciona escalabilidad masiva, ofrece gestión y control de la congestión y es útil para el envío de metadatos. De hecho, DVB-H emplea FLUTE para el envío de la Guía Electrónica de Servicios (ESG).

La transmisión del contenido se produce a través de sesiones de envío. Una sesión está unívocamente identificada por la dirección IP multicast donde se envían los contenidos y por un identificador de sesión llamado TSI (*Transport Session Identifier*). Cada sesión contiene uno o más canales de envío asociados. Cada uno de estos canales transmite en un determinado puerto y a una determinada tasa de transmisión.

Cada fichero que se envía a través de los canales de una sesión está identificado por el TOI (*Transport Object Identifier*), un identificador numérico a nivel de fichero.

2. *Descripción de Sesión*

Antes de poder recibir ficheros tiene que haber un establecimiento de la comunicación desde el cliente hasta el emisor. Para que un cliente pueda unirse a un canal es necesario obtener información del emisor para poder conectarse con él. La información requerida puede ser obtenida mediante la Descripción de Sesión. Ésta se puede transmitir de diferentes formas, siendo la más común el uso del protocolo SDP (*Session Description Protocol*) [6], aunque existen distintos métodos *out-of-band*, como cabeceras HTTP/Mime o a través del protocolo SAP.

La Descripción de Sesión debe incluir obligatoriamente los parámetros que identifican a una sesión: la IP del emisor y el TSI. Asimismo, también incluye información sobre el número de canales, tasa de transmisión y puerto de cada canal, el control de la congestión utilizado, y puede incluir otra información adicional.

3. *Tabla de Envío de Ficheros (FDT)*

Una vez los clientes disponen de la información necesaria para unirse a una sesión y han establecido la conexión, ya pueden empezar a recibir a ficheros. Pero antes, deben conocer qué ficheros se están transmitiendo por el canal y sus características. Esta información se obtiene a través de la Tabla de Envío de Ficheros (FDT).

La FDT (*File Delivery Table*) proporciona un medio para describir varios atributos asociados con los ficheros que se envían en la sesión. Los atributos más importantes son: el identificador del objeto (TOI), la localización y nombre del fichero (especificado por el URI), la longitud del fichero o la codificación, entre otros.

La FDT está escrita en lenguaje XML. Su envío se produce a través de Instancias FDT, que son paquetes de FLUTE con una extensión de cabecera de FDT. El XML propiamente dicho es el que forma la carga del paquete a enviar. Para identificar un paquete como FDT se reserva el valor de TOI igual a cero.

4. *Arquitectura*

La figura 1 muestra la pila de protocolos utilizada por FLUTE. En la parte superior se encuentra el protocolo ALC (*Asynchronous Layered Coding*) [7], que le proporciona el transporte básico a FLUTE. A su vez, éste emplea el bloque LCT (*Layered Coding Transport*) [8] para funciones de gestión de sesión, un bloque de control de la congestión (CC), así como el bloque FEC encargado del control de errores. En las capas inferiores, FLUTE funciona sobre UDP en el nivel de transporte y utiliza IP en el nivel de red.

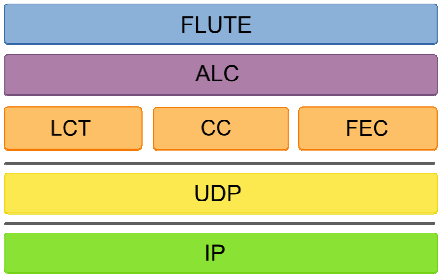


Fig. 1. Pila de protocolos de FLUTE.

El bloque de LCT proporciona soporte a nivel de transporte para protocolos ampliamente escalables utilizando IP multicast. Concretamente, da soporte a dos tipos de aplicaciones: transferencia fiable de contenido y aplicaciones de *streaming*. La cabecera de LCT es la utilizada por FLUTE para el envío de los paquetes. Los campos más importantes de dicha cabecera son: TSI y TOI (para identificar a la sesión y al objeto respectivamente) y el campo *CodePoint*, en el que se indica la codificación utilizada. Además, existen distintas extensiones de cabecera, entre las que destacan dos principales: EXT_FDT (extensión utilizada para la transmisión de la FDT) y EXT_FTI (empleada para pasar los parámetros de la codificación que se utiliza).

A través del bloque de control de la congestión (CC), el emisor es capaz de enviar paquetes a diferentes tasas y cada uno de los receptores regula su tasa de recepción en función del ancho de banda disponible.

El bloque FEC [9] especifica los parámetros relativos tanto a las características de la codificación propiamente dichas, como a su transporte.

5. *Transmisión de ficheros*

Cada fichero que se envía representa un objeto de transporte, es decir, una combinación de símbolos binarios que forman los datos. Tal como refleja la figura 2, cada objeto de transporte se fragmenta en bloques, según un algoritmo

definido por FLUTE. A su vez, cada bloque está compuesto por una serie de símbolos de codificación. Existen dos clases de símbolos de codificación: los símbolos fuente y los símbolos de paridad. Los símbolos fuente son los datos del fichero, mientras que los símbolos de paridad se forman a partir de una combinación entre símbolos fuente para proporcionar fiabilidad en la transmisión. Así, cada bloque contiene *n* símbolos de codificación, de los cuales *k* son símbolos fuente. Si se emplea codificación el número de símbolos de paridad por paquete será, por tanto, igual a *n* - *k*. Cada uno de los símbolos de codificación representa la carga de un paquete FLUTE, al cual se le añade la cabecera correspondiente. También es posible incluir varios símbolos de codificación en un mismo paquete.

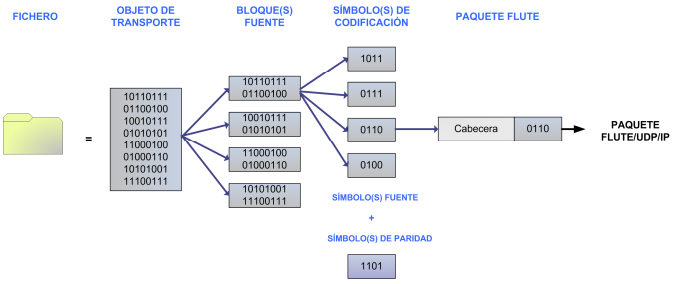


Fig. 2. Formación de paquete FLUTE.

En cuanto a la transmisión, hay definidas dos clases de sesiones de envío de ficheros FLUTE: sesión de transmisión de ficheros y carrusel de ficheros. En esta última clase los ficheros se envían de forma continua a modo de carrusel. A su vez, existen dos tipos de carruseles: estáticos y dinámicos, en función de si se pueden modificar (añadir, eliminar o actualizar) los ficheros que se envían entre un ciclo y el siguiente.

Normalmente se suelen utilizar los carruseles como método de transmisión. De hecho, el uso de carruseles, junto a la utilización de FEC es lo que proporciona fiabilidad en la transmisión, que es la característica principal del protocolo FLUTE.

III. CÓDIGOS FEC

A. *Introducción: tipos de códigos*

Un tipo de código FEC está definido por los valores de *FEC Encoding ID* y *FEC Instance ID*. El valor de estos identificadores viene regulado por la IANA (*Internet Assigned Numbers Authority*).

Los *FEC Encoding ID* especificados por IANA son: 0) Compact No-Code, 1) Raptor, 2) Reed-Solomon sobre GF (2^m), 3) LDPC Staircase, 4) LDPC Triangle y 5) Reed-Solomon sobre GF (2^8).

Compact No-Code [10] implica no utilizar ningún mecanismo de codificación, es decir, se envían únicamente paquetes fuente. En los siguientes apartados se explica el resto de codificaciones.

B. *Raptor*

Los códigos Raptors [11] fueron creados en el año 2001 por la compañía "Digital Fountain Inc.". Pertenecen a la categoría de los códigos *fountain*, en los que se pueden generar tantos símbolos como se necesiten automáticamente a partir de los símbolos fuente de un bloque, es decir, que no es necesaria una tasa fija de codificación. A pesar de ser una implementación propietaria, esta codificación ha sido adoptada por multitud de tecnologías. Entre ellas se encuentra el estándar de transmisión a terminales móviles DVB-H.

Su principal característica es que esta codificación permite generar una cantidad ilimitada de información de paridad, a partir de símbolos fuente. Así, en recepción basta con recibir una cantidad de paquetes ligeramente superior al tamaño del fichero original para poder reconstruirlo, independientemente de los paquetes recibidos, por lo que estos códigos resultan muy eficientes. Además, los algoritmos de codificación y decodificación son excepcionalmente rápidos, lo que posibilita su implementación en *software*.

El proceso de codificación se divide en dos pasos: en primer lugar se realiza una precodificación, que genera *l* paquetes de salida a partir de *k* paquetes de entrada ($l > k$). El segundo paso consiste en la creación de los *n* símbolos fuente a partir de los *l* símbolos precodificados ($n > l$), utilizando los códigos LT (*Luby Transform*) [12], un tipo de códigos *fountain*. Cada uno de los símbolos se genera independientemente del resto, pudiendo de esta manera formarse un número ilimitado de símbolos.

La RFC 5053 [13] describe la formación de los símbolos y el formato de las cabeceras referentes a Raptor.

C. *Reed-Solomon*

La codificación Reed-Solomon fue inventada por Irving S. Reed y Gustave Solomon en el año 1960 [14]. Esta codificación se utiliza en múltiples aplicaciones, como en el almacenamiento de datos (por ejemplo en el CD o DVD), en comunicaciones inalámbricas (telefonía móvil) o por satélite, en comunicaciones por cable (ADSL) y en televisión digital (DVB emplea Reed-Solomon para corregir errores en la capa física).

Reed-Solomon es un código bloque corrector de errores basado en polinomios, que crea símbolos a través de secuencias de *m* bits. Cada palabra código está formada por *n* símbolos, de los cuales *k* son símbolos fuente y *r* son símbolos de paridad. La relación entre la longitud de la palabra código y el número de símbolos viene definida por: $n=2^m-1$. Esta codificación es capaz de corregir errores hasta en *r/2* símbolos.

La RFC 5510 [15] define los esquemas FEC para los códigos Reed Solomon sobre GF (2^8) y sobre GF (2^m). En ambos casos, la creación de los *n* símbolos a partir de los *k* símbolos que componen un bloque se produce a través de una matriz de generación. Dicha matriz hace uso de un polinomio que depende de la longitud de los elementos del campo finito *m*.

D. *LDPC*

La codificación LDPC (*Low Density Parity Check*) fue inventada por Gallager en 1960 [16]. Pero no fue hasta 30 años después, gracias a MacKay y Neal [17], que empezó a utilizarse. La especificación original ha sufrido una serie de mejoras que facilitan su utilización en distintos entornos. Por ejemplo, son la base de las codificaciones Tornado, LT y Raptor, todas ellas implementaciones propietarias.

LDPC pertenece a la categoría de códigos FEC de bloque grande, en los que resulta necesario recibir más de los *k* paquetes que componen un fichero para poder reconstruirlo. Las codificaciones que se engloban dentro de esta categoría

resultan convenientes a la hora de codificar ficheros grandes, ya que el coste computacional no crece de forma excesiva.

Los LDPC son códigos bloque lineales sistemáticos basados en una matriz de comprobación de paridad utilizada en el proceso de codificación y decodificación. Dicha matriz define las relaciones entre los distintos símbolos de codificación (símbolos fuente y símbolos de paridad). La matriz está formada por elementos con valores "0" y "1", y es dispersa, ya que la mayoría de elementos son nulos. A través de dicha matriz el codificador crea los símbolos de paridad a partir de los símbolos fuente (y otros símbolos de paridad ya creados). Asimismo, en recepción, la matriz se emplea para reconstruir símbolos que no se han recibido, mediante los símbolos de codificación ya disponibles. La siguiente figura muestra un ejemplo de matriz de paridad, y establece las relaciones entre los símbolos de paridad y los símbolos fuente.

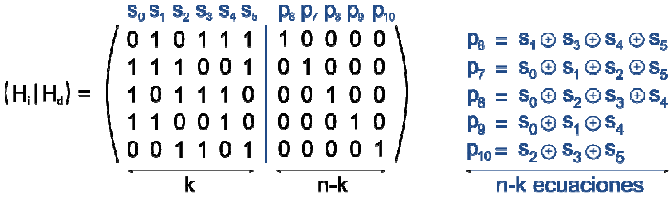


Fig. 3. Matriz de comprobación de paridad LDPC (k=6, n=11).

En la figura se observa una matriz con valores *k*=6 y *n*=11, generándose por lo tanto 5 símbolos de paridad por bloque. El tamaño de la matriz es de *n* x (*n*-*k*), por lo que existen *n* - *k* filas, cada una de las cuales representa una ecuación. Las columnas se corresponden con cada uno de los símbolos del bloque. Cada entrada de la matriz con el valor "1" indica que el símbolo *i*-ésimo participa en la ecuación *j*-ésima. Así, por ejemplo, el primer símbolo de paridad (identificado como p_6), está formado por la suma XOR de los símbolos s_1, s_3, s_4 y s_5. Un símbolo de paridad puede formar parte de la creación de otros símbolos de paridad. Cada uno de los símbolos fuente normalmente participa en un número fijo de ecuaciones, que corresponde al número de 1s que contiene esa columna. Ese parámetro se denomina como N1. Al número de elementos no nulos de una fila o columna se le llama grado.

La matriz de paridad está dividida, a su vez, en dos submatrices: la izquierda y la derecha. La primera de ellas está referida a los símbolos fuente, mientras que la submatriz derecha hace referencia a los símbolos de paridad.

Por lo que respecta al receptor, cuando ha recibido todos los símbolos que componen una ecuación excepto uno, es capaz de recuperar éste haciendo la suma XOR del resto de símbolos de esa ecuación.

Evidentemente tanto el transmisor como el receptor deben utilizar la misma matriz de paridad para que el proceso de decodificación resulte válido. Para la creación de la matriz se emplea un algoritmo definido (en función del tipo de estructura LDPC) que conocen tanto uno como otro. Dicho algoritmo genera la matriz a partir de una serie de parámetros de entrada, estos son: número de símbolos fuente (*k*), número de símbolos de codificación (*n*), número de ecuaciones en las que participa cada símbolo fuente (*N1*) y semilla utilizada para la generación de números pseudoaleatorios (*seed*). Todos estos parámetros los envía el transmisor a través de la extensión de cabecera EXT_FTI de LCT.

En función de la estructura de la matriz de comprobación de paridad se distinguen dos clases de códigos LDPC: regulares e irregulares. En los regulares, todas las filas de la matriz tienen el mismo grado, y todas las columnas de la matriz tienen el mismo grado. Un código LDPC es irregular si no cumple alguna de estas características. Los códigos de Gallager y Mackay son ejemplos de códigos LDPC regulares, mientras que LDPC Staircase y Triangle son irregulares.

Al respecto, este artículo se centra en la implementación y análisis de LDPC Staircase y Triangle, que difieren únicamente en el algoritmo de generación de la submatriz derecha, tal como se puede apreciar en la figura 4.

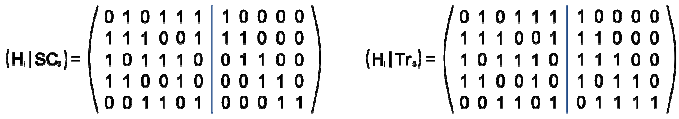


Fig. 4. Ejemplo de matrices LDPC Staircase y Triangle (k=6, n=11).

IV. Implementación

A. *Especificaciones RFC 5170*

La RFC 5170 [18], *LDPC Staircase and Triangle FEC*, de Junio de 2008, presenta los códigos completamente especificados con FEC Encoding ID 3 y 4, basados en la codificación LDPC Staircase y Triangle, respectivamente. Ambos esquemas pertenecen a la clase de códigos de bloque largos, según la definición de la RFC de FEC [10].

La RFC 5170 define la generación de la matriz de paridad en ambos tipos de estructuras. Para ello, proporciona un algoritmo que, a partir de ciertos parámetros de entrada (como los valores *k* y *n*, o el N1), crea la matriz de paridad. Para ambas estructuras el algoritmo es idéntico a la hora de generar la submatriz izquierda, mientras que difiere en la creación de la submatriz derecha. Para la creación de la matriz la RFC propone el uso del algoritmo generador de números pseudoaleatorios de Park-Miller [19]. La RFC, además, define los campos de la extensión de cabecera EXT_FTI para LDPC, donde van los parámetros de la codificación.

En este artículo se presenta una implementación propia de la codificación LDPC. Dicha implementación respeta los requisitos establecidos por la RFC 5170. El codificador y decodificador LDPC Staircase y Triangle desarrollado se explica en los siguientes apartados.

B. *Codificador LDPC*

La siguiente figura muestra la arquitectura del servidor de ficheros implementado, basado en el protocolo FLUTE.

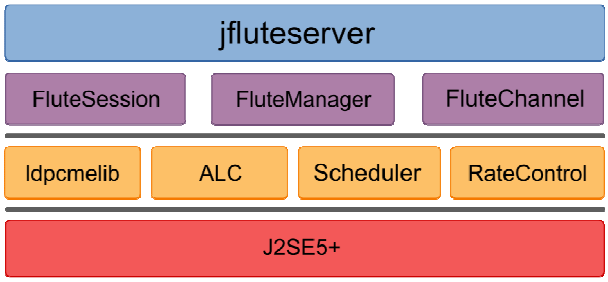


Fig. 5. Estructura del servidor de ficheros.

La gestión de las sesiones y canales de FLUTE, así como el envío a través del protocolo ALC, se realiza a través de las clases correspondientes. El envío de los paquetes se realiza a

una tasa fijada por la clase "RateControl" y utilizando un modelo de transmisión gestionado por "Scheduler".

La librería "ldpcmelib" implementa tanto el codificador como el decodificador LDPC (Staircase y Triangle). Está programada en J2ME, para que pueda ser utilizada en dispositivos móviles. Esta librería se encarga de la creación de la matriz de paridad, que define la relación entre los símbolos fuente y los de paridad.

Asimismo, el transmisor también se encarga de crear la cabecera donde se señalan los parámetros que definen la codificación, con el objetivo de que el receptor pueda generar la misma matriz de paridad y así realizar la decodificación.

C. *Decodificador LDPC*

La estructura del cliente de FLUTE utilizado se muestra en la figura 6, muy similar a la del servidor de ficheros:

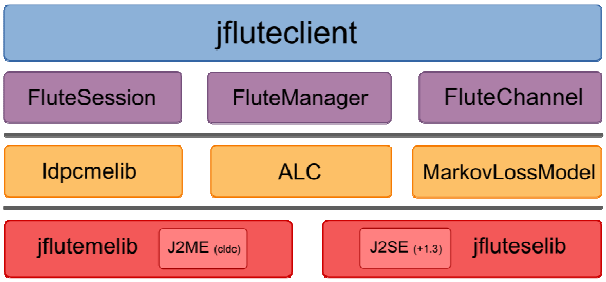


Fig. 6. Estructura del cliente FLUTE.

El cliente está diseñado para J2SE y J2ME, por lo que funciona tanto sobre PC como sobre dispositivos móviles. Para simular pérdidas en el canal se ha implementado el modelo de Markov de 2 estados, debido a que este modelo simula bien las pérdidas en ráfagas (típicas de redes inalámbricas) y por ser un modelo ampliamente utilizado en la literatura [20].

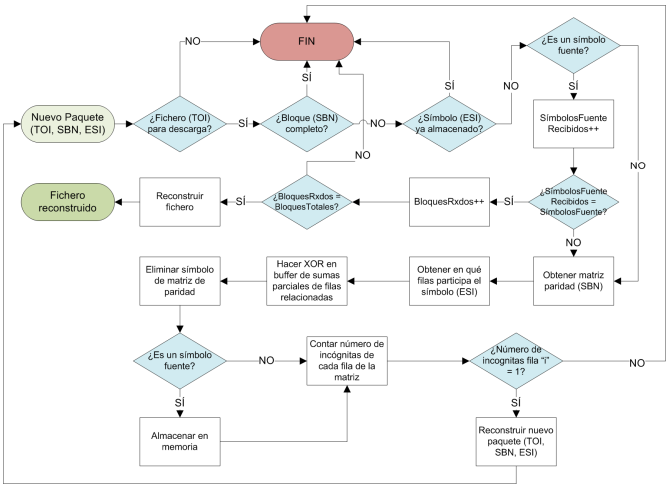


Fig. 7. Flujograma de recepción de paquete.

Por otro lado, la decodificación se realiza utilizando el algoritmo de decodificación iterativa. Esto es, la decodificación se basa en la existencia de *buffers* de sumas parciales en cada fila de la matriz de paridad. Cada *buffer* contiene la suma XOR de los símbolos recibidos de una fila. Cuando se han recibido todos los paquetes que forman parte de la fila excepto uno, los datos del símbolo que faltan se corresponden con la suma parcial del *buffer* de esa fila, reconstruyendo de esta forma el símbolo que aún no se ha recibido. El flujograma de la figura 7 representa el proceso que se lleva a cabo cada vez que se recibe un nuevo paquete.

El algoritmo utilizado a la hora de decodificar es un factor muy importante que afecta tanto a la eficiencia de la codificación como al consumo de memoria en el receptor. Estudios sobre la utilización de otros algoritmos se pueden encontrar en [21].

V. EVALUACIÓN

Para analizar el códec LDPC implementado se han realizado una serie de pruebas que se explican a continuación. Los parámetros a evaluar han sido:

- Ratio de ineficiencia: representa la relación entre el número de paquetes necesarios para decodificar un fichero y el número de paquetes fuente que componen dicho fichero. Cuanto menor es el ratio de ineficiencia, más eficiente resulta la codificación. Idealmente este valor es 1.

$$inefficiency\_ratio = \frac{n_{necesarios\_para\_decodificar}}{k} \quad (1)$$

- Número de ciclos del carrusel necesarios para reconstruir un fichero.

Las pruebas se han realizado con un Pentium Dual-Core a 2.50 GHz con 2 Gbytes de memoria RAM, utilizando el sistema operativo Windows XP. Para las pruebas con teléfonos móviles se ha usado el Nokia E90.

La tabla 1 muestra los parámetros de la codificación utilizados en cada uno de los estudios, remarcándose en cursiva aquellos que se evalúan en cada caso. Señalar que el tamaño del fichero está expresado en número de paquetes que lo forman, cada uno de los cuales tiene un tamaño de 1428 bytes. El número de emulaciones elegida nos da unos valores de desviación estándar y de intervalo de confianza (99%) adecuados.

Estudio	**A**	**B**	**C**	**D**	**E**	**F**
Modelo pérdidas	*Markov*	*Markov*	No	No	No	Wi-Fi
Modelo transm.	Sec.	*Sec. vs Ale.*	Aleat.	Aleat.	Aleat.	Aleat.
Code rate	0.67	0.67	*[0.2, 0.9]*	0.67	0.67	*0.20, 0.67*
Tamaño fichero	3000	3000	3000	*[10, 100000]*	6400	*300, 1500*
Número bloques	1	1	1	1	*[1,100]*	1
N1	3	3	3	3	3	3
Número emulac.	100	100	200	200	200	30

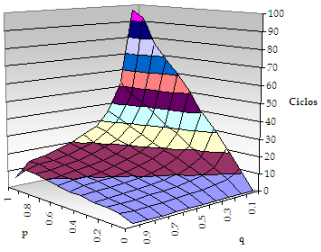
Tabla 1. Parámetros de los estudios.

A. *Número de ciclos de reconstrucción*

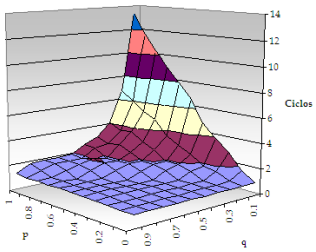
El primer estudio muestra el número de ciclos que a un cliente le cuesta reconstruir un fichero en función de las pérdidas del canal (simuladas a partir del modelo de Markov de 2 estados). En el modelo de Markov la probabilidad de pasar a un estado de pérdidas desde un estado sin pérdidas es *p*, mientras que el parámetro *q* representa la probabilidad de recibir un paquete cuando no se ha recibido el anterior. El número de ciclos está directamente relacionado con el tiempo de descarga de un contenido, por lo que resulta un parámetro

importante. Las gráficas de la figura 8 reflejan los resultados obtenidos.

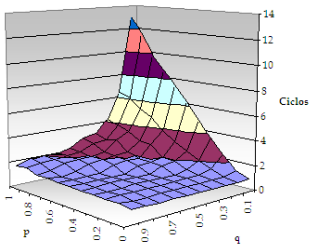
Mirando la escala de cada una de las gráficas se ve claramente la conveniencia de utilizar codificación (en LDPC no se superan los 15 ciclos, mientras que en No-FEC se llegan a superar los 90 ciclos con altas pérdidas). La diferencia entre ambas codificaciones es mayor conforme aumentan las pérdidas. En entornos con bajas pérdidas (esto es, cuando *p* es bajo y *q* es alto), las gráficas muestran que la codificación LDPC (tanto Staircase como Triangle), presenta un comportamiento más estable y cercano a 1 ciclo, mientras que cuando no se emplea codificación el número de ciclos aumenta rápidamente tras un ligero aumento de las pérdidas.



(a) No-FEC



(b) LDPC Staircase



(c) LDPC Triangle

Fig. 8. Número de ciclos según codificación.

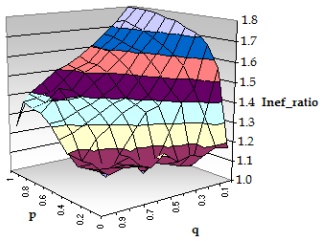
B. *Modelo de transmisión*

En este estudio se muestra cómo afecta a la eficiencia de la codificación el modelo de transmisión utilizado a la hora de enviar los paquetes. Para ello se analizan dos modelos: uno secuencial, en la que los paquetes se envían en orden (primero los símbolos fuente y luego los símbolos de paridad); y uno aleatorio, donde los paquetes se transmiten de forma aleatoria (intercalando los símbolos fuente y los de paridad).

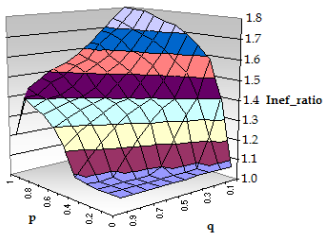
El parámetro de medida utilizado es el ratio de ineficiencia. El resultado de este estudio se muestra en las gráficas de la figura 9.

Dichas gráficas reflejan que en entornos de bajas pérdidas (que se corresponde con los canales donde se suele trabajar), el modelo de transmisión aleatorio presenta un mejor comportamiento y resulta más eficiente que el modelo de transmisión secuencial. Esto es lógico teniendo en cuenta que normalmente las pérdidas se producen a ráfagas y que en la codificación LDPC un símbolo de paridad depende del símbolo anterior, por lo que la pérdida de paquetes consecutivos impide la reconstrucción de símbolos fuente. Por otro lado, con altas pérdidas el comportamiento de los dos modelos es similar.

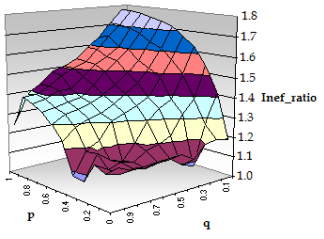
Por esta razón, en los siguientes casos de estudio se utilizará el modelo aleatorio.



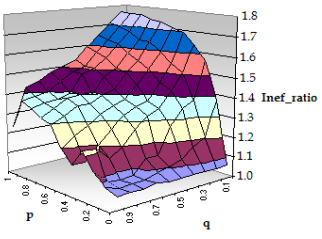
(a) LDPC Staircase, Secuencial



(b) LDPC Staircase, Aleatorio



(a) LDPC Triangle, Secuencial



(b) LDPC Triangle, Aleatorio

Fig. 9. Modelo de transmisión.

C. *Tasa de codificación*

La tasa de codificación (o *code rate*) es un parámetro fundamental en la transmisión. Se define como *k/n*, es decir, representa la relación entre el número de símbolos fuente y el número de símbolos de codificación de un fichero. El número de símbolos de paridad introducidos resulta, pues, *k-n*, por lo que cuanto mayor es la tasa de codificación menos se está protegiendo la información.

Otro parámetro que se suele utilizar es el *FEC ratio*, definido como *n/k*, que se corresponde con la inversa de la tasa de codificación.

Se ha analizado cómo afecta la tasa de codificación al ratio de ineficiencia de la codificación, utilizando para ello un canal sin pérdidas. El resultado se muestra en la siguiente gráfica (se ha ampliado el eje de valores de *code rate* superiores a 0.4 para ver en detalle el comportamiento de cada una de las estructuras):

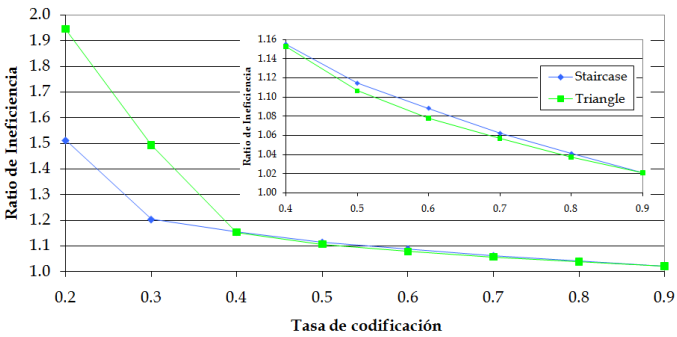


Fig. 10. Evaluación de la tasa de codificación.

Conforme aumenta la tasa de codificación el ratio de ineficiencia es menor (y por lo tanto, mejor). La figura refleja que la estructura LDPC Staircase resulta mucho más eficiente cuando la tasa de codificación es inferior a 0.4, mientras que LDPC Triangle ofrece mejores resultados para tasas de codificación superiores a dicho valor. Aunque a partir de 0.4 la diferencia entre ambas estructuras es mínima, dicha diferencia resulta muy significativa cuando se transmiten ficheros grandes.

Cuanto mayor es el *code rate* (y en consecuencia menor es el *FEC ratio*), menos paquetes de paridad se envían, por lo

que en entornos sin pérdidas el ratio de ineficiencia será más bajo (ya que se reciben menos paquetes "inútiles"). Idealmente, en un entorno sin pérdidas si la tasa de codificación es 1 (es decir, no se codifica) el ratio de ineficiencia es 1. Pero, desgraciadamente, todos los canales tienen pérdidas. Para ver el comportamiento en un entorno con pérdidas, se ha realizado el mismo estudio en un canal con unas pérdidas elevadas (del 25%), con valores p=0.1 y q=0.3, que se refleja en la figura 11.

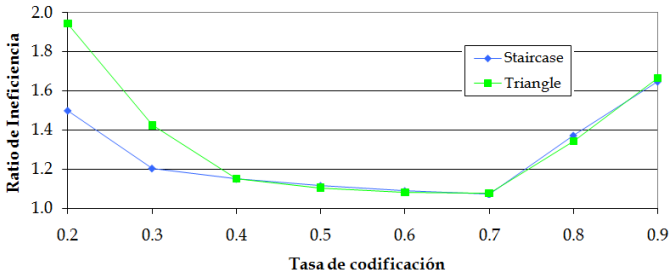


Fig. 11. Evaluación de la tasa de codificación con pérdidas (p=0.1, q=0.3).

Con esta gráfica se concluye que para elegir una tasa de codificación adecuada hay que tener en cuenta las pérdidas del canal. Al elegir tasas de codificación muy altas puede que no se esté protegiendo lo suficiente la información, de ahí que el ratio de ineficiencia aumente. En este caso, para un canal con esas características el valor de *code rate* igual a 0.7 es el que ofrece mejores resultados.

D. *Tamaño del fichero*

El ratio de ineficiencia depende del tamaño del contenido que se está enviando. Para comprobarlo, se ha realizado un estudio en el que se evalúa cómo afecta el tamaño del fichero. La figura 12 muestra, a escala logarítmica, el ratio de ineficiencia en función de los paquetes que componen un fichero.

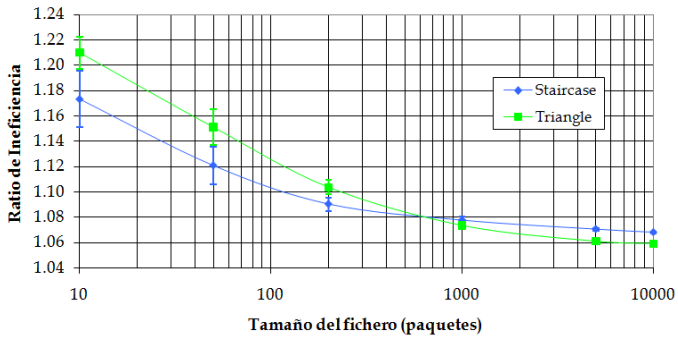


Fig. 12. Evaluación del tamaño del fichero.

La codificación LDPC se comporta de una forma más eficiente cuando se utiliza en ficheros grandes, tal como refleja la gráfica. Por ejemplo, para ficheros de 10000 paquetes (unos 14 Mbytes), para el caso de Triangle el ratio de ineficiencia es de 1.0593. Esto significa que sólo hará falta recibir un 5.93% más de paquetes que componen un fichero para poder reconstruirlo, lo que implica que se está proporcionando fiabilidad en la transmisión sin aumentar excesivamente el tiempo de reconstrucción en recepción.

Por lo que respecta al tipo de estructura, la tendencia de la gráfica demuestra que Staircase ofrece mejores resultados que Triangle con ficheros pequeños, mientras que con ficheros grandes LDPC Triangle tiene un ratio de ineficiencia mejor.

Las conclusiones alcanzadas coinciden, respecto al tamaño del fichero y a la tasa de codificación, con las publicadas en [22].

E. *Número de bloques*

Un estudio que surge a raíz del caso anterior es el número de bloques que se utiliza para transmitir. Resulta lógico pensar que si el códec es más eficiente cuantos más paquetes componen un bloque, será mucho más eficiente transmitir el fichero en un solo bloque que en varios bloques, ya que cada uno de ellos tendrá menor número de símbolos.

Al respecto, la siguiente gráfica muestra el ratio de ineficiencia de un fichero formado por 6400 paquetes, que se ha transmitido utilizando distinto número de bloques:

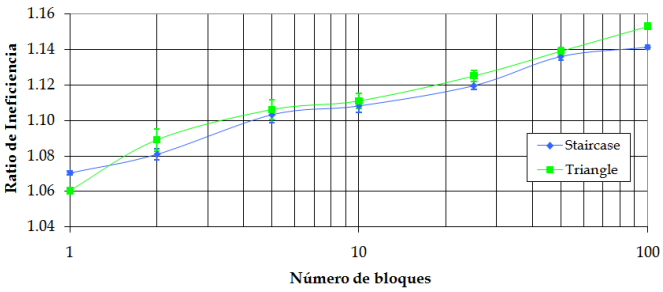


Fig. 13. Evaluación del número de bloques.

Las conclusiones alcanzadas en este caso son consecuencia de las anteriores. Cuantos más bloques haya más ineficiente es la codificación. Cuanto mayor es el número de bloques, menos símbolos hay por bloque, por lo que la estructura Staircase resulta más eficiente que la Triangle.

Aunque resulta, pues, más eficiente emplear un solo bloque para la transmisión, esto no significa que siempre sea lo más conveniente. Dependiendo de la situación, puede ser preferible enviar un fichero en varios bloques debido, sobre todo, a limitaciones en cuanto a la memoria. Hay que tener en cuenta que cuanto mayor sea el bloque más consumo de memoria se requiere.

F. *Evaluación en dispositivos móviles*

El último estudio que se ha realizado consiste en la evaluación del códec implementado en dispositivos móviles y en un entorno inalámbrico. Concretamente, el terminal móvil utilizado ha sido el Nokia E90. Se ha elegido dicho dispositivo por ser un representante de la familia de *smartphones* con sistema operativo Symbian S60, que cuenta con el mayor número de dispositivos en el mercado. La red inalámbrica utilizada ha sido Wi-Fi.

El procedimiento es similar al de los estudios anteriores. Un servidor envía por Wi-Fi un fichero a una dirección y un puerto determinados y un receptor se descarga dicho fichero a través de un teléfono móvil. Para ello, en el dispositivo móvil se ha instalado una aplicación cliente receptora de ficheros FLUTE, que se conecta a una sesión y un canal para descargarse un contenido, todo ello a través de Wi-Fi. Cuando se ha descargado, se mide el ratio de ineficiencia obtenido.

En este caso, para contrastar las conclusiones alcanzadas en los estudios anteriores en un entorno real, se ha optado por realizar tres pruebas en las que se varía la tasa de codificación y el tamaño del fichero, así como la estructura LDPC empleada. Los resultados se muestran en la tabla 2, que refleja

el valor medio del ratio de ineficiencia, así como la desviación estándar y el intervalo de confianza del 99%:

		STAIRCASE			TRIANGLE		
CR	**Tamaño**	**Media**	**Desv.**	**I. Conf.**	**Media**	**Desv.**	**I. Conf.**
0.20	300	1.4916	0.0420	±0.0216	2.1419	0.0283	±0.0146
0.67	300	1.4584	0.0733	±0.0378	1.4527	0.0070	±0.0036
0.67	1500	1.4187	0.0168	±0.0087	1.4294	0.0229	±0.0118

Tabla 2. Evaluación en entorno inalámbrico.

La tabla refleja que las pérdidas en el canal afectan mucho al ratio de ineficiencia. Mientras que en el resto de casos se obtenían normalmente valores inferiores a 1.1 en cuanto al ratio de ineficiencia, en pruebas con Wi-Fi los valores obtenidos han sido siempre superiores a 1.25.

Algunas de las conclusiones alcanzadas en estudios anteriores también se reflejan en la tabla. Por ejemplo, con tasas de codificación bajas la estructura Staircase mejora considerablemente a la Triangle, reduciéndose esa diferencia conforme la tasa de codificación aumenta. Utilizar una tasa de codificación mayor supone una disminución del ratio de ineficiencia. Por otro lado, un aumento del tamaño del fichero conlleva una mejora del ratio de ineficiencia.

VI. Conclusiones y Trabajo Futuro

La codificación LDPC permite reducir de manera considerable el número de ciclos necesarios para reconstruir un fichero y, por lo tanto, el tiempo de descarga. La reducción en dicho tiempo es aún mayor en canales con elevadas pérdidas.

Por otro lado, la planificación en el envío de paquetes es un parámetro que afecta a la eficiencia de la transmisión. En entornos de bajas pérdidas, un modelo de envío aleatorio resulta mucho más eficiente que uno secuencial, ya que es más inmune a las pérdidas de paquetes en forma de ráfagas.

LDPC es más eficiente con ficheros grandes, por lo que resulta más óptimo, en términos de eficiencia, la transmisión utilizando un único bloque.

En cuanto a las dos estructuras LDPC, Staircase y Triangle, la primera de ellas resulta más eficiente con tasas de codificación inferiores a 0.4 y cuando se codifican ficheros pequeños.

Los parámetros de codificación óptimos en cada caso (tasa de codificación, número de bloques…) dependen de las características de la transmisión: pérdidas del canal, ficheros que se transmiten o capacidades de procesamiento de los receptores.

Precisamente, uno de las líneas futuras es el estudio de la memoria requerida por los terminales para realizar el proceso de decodificación. Al respecto, uno de los parámetros que afecta a la memoria es el algoritmo de decodificación utilizado. Emplear otros algoritmos, como un esquema de eliminación Gaussiana [23], hace mejorar el ratio de ineficiencia a costa de aumentar la memoria requerida en el terminal.

Otra línea a investigar es la aplicación de la codificación LDPC a la transmisión de vídeo, haciendo uso de la librería desarrollada, a través del bloque LCT del protocolo FLUTE.

Agradecimientos

Este trabajo ha sido realizado con el apoyo del Proyecto MIQUEL del Ministerio de Educación y Ciencia (TEC2007-68119-C02-01/TCM).

Referencias

[1] G. Faria, J. Henriksson, E. Stare and P. Talmola, *DVB-H: Digital Broadcast Services to Handheld Devices*. Proc. of the IEEE, vol. 94, no. 1, pp. 194-209, January 2006.

[2] *Mobile Broadcast/Multicast Service (MBMS)*. White Paper, August 2004.

[3] *Integrated Mobile Broadcast (IMB): The Power of Predictive Broadcasting for 3G Multimedia Applications.* White Paper, September 2009.

[4] S. Park and S. Jeong, *Mobile IPTV: Approaches, Challenges, Standards, and QoS Support*. IEEE Internet Computing, vol. 13, no. 3, pp. 23-31, June 2009.

[5] T. Paila, M. Luby, R. Lehtonen, V. Roca and R. Walsh, *FLUTE – File Delivery Over Unidirectional Transport*. IETF RFC 3926, October 2004.

[6] M. Handley and V. Jacobson, *SDP: Session Description Protocol*. IEFT RFC 2327, April 1998.

[7] M. Luby, M. Watson and L. Vicisano, *Asynchronous Layered Coding (ALC) Protocol Instantiation*. IEFT RFC 5775, April 2010.

[8] M. Luby, M. Watson and L. Vicisano, *Layered Coding Transport (LCT) Building Block*. IEFT RFC 5651, October 2009.

[9] M. Watson, M. Luby and L. Vicisano, *Forward Error Correction (FEC) Building Block*. IETF RFC 5052, August 2007.

[10] M. Watson, *Basic Forward Error Correction (FEC) Schemes.* IETF RFC 5445, March 2009.

[11] A. Shokrollahi, *Raptor Codes*. IEEE Transactions on Information Theory no. 6, June 2006.

[12] M. Luby, *LT Codes*. Proc. IEEE Symposium on Foundations of Computer Science (FOCS), Vancouver, Canada, 2002.

[13] M. Luby, A. Shokrollahi, M. Watson and T. Stockhammer, *Raptor Forward Error Correction Scheme for Object Delivery*. IETF RFC 5053, September 2007.

[14] I. S. Reed and G. Solomon, *Polynomial Codes over Certain Finite Fields*. SIAM Journal of Applied Math, vol. 8, pp. 300-304, 1960.

[15] J. Lacan, V. Roca, J. Peltotalo and S. Peltotalo, *Reed-Solomon Forward Error Correction (FEC) Schemes.* IETF RFC 5510, April 2009.

[16] R. G. Gallager, *Low Density Parity Check Codes*. IEEE Transactions on Information Theory, 8(1), January 1962.

[17] D. MacKay and R. Neal, *Good codes based on very sparse matrices*. In 5th IAM Conference: Cryptography and Coding, LNCS No. 1025, 1995.

[18] V. Roca, C. Neumann, and D. Furodet, *Low Density Parity Check (LDPC) Staircase and Triangle Forward Error Correction (FEC) Schemes*. IETF RFC 5170, June 2008.

[19] S. Park and K. Miller, *Random Number Generators: Good Ones are Hard to Find*. Communications of the ACM, Vol. 33, No. 1, pp. 87-88, January 1990.

[20] H. Bai and M. Atiquzzaman, *Error modeling schemes for fading channels in wireless communications: a survey*. IEEE Communications Surveys and Tutorials, 5(2), 2003.

[21] M. Cunche and V. Roca, *Optimizing the Error Recovery Capabilities of LDPC-Staircase Codes Featuring a Gaussian Elimination Decoding Scheme*. Proc. of the 10th IEEE International Workshop on Signal Processing for Space Communications (SPSC), Rhodes Island, Greece, October 2008.

[22] V. Roca and C. Neumann, *Design, Evaluation and Comparison of Four Large Block FEC Codecs, LDPC, LDGM, LDGM Staircase and LDGM Triangle, plus a Reed-Solomon Small Block FEC Codec*. INRIA Research Report RR-5225, June 2004.

[23] M. Cunche and. V. Roca, *Improving the Decoding of LDPC Codes for the Packet Erasure Channel with a Hybrid Zyablov Iterative Decoding/Gaussian Elimination Scheme*. INRIA Research Report RR-6473, March 2008.

Implementación de un esquema de localización privada y segura para interiores

Rubén Ríos del Pozo, Isaac Agudo Ruiz
Dpto. de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: {ruben,isaac}@lcc.uma.es

José Luis Gonzalez
Telefónica I+D
Madrid
Email: jluis@tid.es

***Resumen*—Las aplicaciones basadas en localización proporcionan a los usuarios servicios personalizados dependiendo de su ubicación. Las estimaciones prevén que estos servicios se extenderán enormemente en los próximos años reportando grandes beneficios tanto a la industria como a los usuarios finales. Sin embargo, para que estos avances sean posibles se hace necesario analizar en profundidad las distintas implicaciones de seguridad y privacidad que la utilización de tales servicios pueden traer consigo a los usuarios.**

En este trabajo proponemos un sistema de localización que da soporte a la provisión de servicios basados en localización para entornos *indoor* y que se fundamenta en la tecnología de redes de sensores inalámbricos. En este esquema hemos tenido en cuenta diversos aspectos de seguridad y privacidad, prestando especial atención a la limitación extrema de recursos característica de las redes de sensores. Finalmente hemos desarrollado una prueba de concepto para comprobar la viabilidad de nuestro esquema dentro del ámbito del proyecto OSAmI.

I. Introducción

Los servicios basados en localización (*Location-Based Services*, LBS) han ido ganando popularidad en los últimos años gracias al auge de las comunicaciones móviles y a los avances en los sistemas de localización. Los LBS tienen como objetivo proporcionar un servicio personalizado a los usuarios basándose en la ubicación en la que estos se encuentran. Para ello se hace necesaria la existencia de dos componentes fundamentales en estos sistemas, en primer lugar la utilización de alguna tecnología de posicionamiento, ya sea obtenida por el propio cliente (e.g. mediante GPS) o suministrada por un servidor de localización externo (e.g. la propia infraestructura de red GSM), y por otra parte, una tecnología de comunicación que permita al cliente interactuar con el proveedor del servicio.

Las aplicaciones típicas basadas en localización ofrecen servicios de navegación (indicación de direcciones, búsqueda de aparcamiento), emergencias (asistencia en carretera, llamadas de emergencia), ocio (búsqueda de amigos, redes sociales), información (páginas amarillas geográficas, guías turísticas), etcétera.

Si bien GPS es el estándar de facto, a la espera de que Galileo entre en acción [1], esta tecnología no permite localizar en espacios cerrados. Es precisamente en este ámbito, el de la localización en interiores (*indoor*), donde se están presentando más avances en los últimos años. Por poner un ejemplo, los populares servicios de audio guías de museos actualmente requieren de una interacción del usuario para seleccionar la zona en la que se encuentran, sin embargo ya son varias las iniciativas para hacer que estas guías sean sensibles a la posición [2].

Compañías como Cisco proporcionan soluciones de localización *indoor* [3] aunque por lo general están orientadas a entornos empresariales donde la privacidad no se considera un requisito fundamental. Por otra parte, Nokia está implementando en fase de pruebas un servicio de localización en interiores para móviles en el centro comercial Kamppi en Helsinki, Finlandia. Este sistema permite que cualquier persona dentro del centro comercial pueda localizar los comercios más cercanos, compartir su localización con otros y buscar amigos que se encuentren cerca.

La localización en interiores presenta nuevos retos técnicos en la determinación y representación de la información de localización [4]. Las tecnologías utilizadas para el posicionamiento en exteriores presentan ciertas limitaciones que imposibilitan su utilización en entornos *indoor*. Los principales obstáculos que encuentran son, por un lado la atenuación o pérdida de la señal dentro de edificios y, por otro lado, la imposibilidad de ofrecer una información de localización exacta o una representación adecuada de la misma dependiendo de las necesidades del servicio. La capacidad de proporcionar coordenadas lógicas o relativas, en lugar de coordinadas físicas, simplifica en gran medida la provisión de servicios de localización dentro de edificios, donde los espacios se encuentran claramente diferenciados por zonas, como son diferentes plantas y habitaciones.

La mayoría de LBS para interiores se basan en la provisión de servicios por proximidad. En este caso el sistema de localización se basa en tecnologías de comunicaciones de medio o corto alcance como Wi-Fi, Bluetooth (BT), infrarrojos (IR) o una combinación de las anteriores [3], [5], [6]. El aprovechamiento de una infraestructura preexistente hace de Wi-Fi y Bluetooth las tecnologías a considerar en el momento de desarrollar un sistema de localización con una inversión inicial reducida. Dado que éstas no son tecnologías específicas de posicionamiento los aspectos de seguridad se suelen relegar a un segundo plano.

En este trabajo se plantean dos esquemas de localización segura para interiores. Por un lado se describe un esquema inicial junto a su implementación, cuyo objetivo principal es comprobar la viabilidad de la propuesta. Además se analizan los retos de seguridad y privacidad a cubrir y se proporcionan soluciones a éstos en un segundo esquema con características avanzadas. Este último esquema permite autenticar a las partes involucradas en el proceso de localización al mismo tiempo que es capaz de preservar la privacidad de los usuarios.

El articulo se organiza de la siguiente manera. La sección II analizan diferentes aspectos a considerar en el diseño de un

esquema de localización *indoor* seguro utilizando la tecnología de redes de sensores. En la siguiente sección se presenta el esquema propuesto, y se dan detalles sobre la plataforma utilizada, la arquitectura del sistema, la implementación de la prueba de concepto y su aplicación con éxito dentro del ámbito de un proyecto. La sección IV analiza posibles mejoras de nuestro esquema para implementaciones futuras. Finalmente, en la sección V se exponen las conclusiones del trabajo.

II. Localización Indoor usando Redes de Sensores

Las redes de sensores (*Wireless Sensor Network*, WSN) se componen de pequeños dispositivos de bajo coste (sensores) con capacidad para monitorizar los fenómenos físicos que tienen lugar en su entorno y comunicarlos a un dispositivo con mayor capacidad para procesar y analizar tal información (estación base). El elenco de sensores que pueden ir acoplados a los nodos que conforman la red es amplísimo, entre los cuales es posible encontrar sensores de temperatura, humedad, luminosidad, presión, radiación, etcétera [7]. Esto los convierte en dispositivos muy versátiles capaces de desempeñar tareas muy diversas, lo cual unido a su reducido coste y tamaño hace de las WSNs una tecnología ideal para la monitorización de diversos entornos y recursos.

Por ello, las WSNs han aparecido en diversos ámbitos, tanto en exteriores como en interiores [8]. Entre las aplicaciones más características que pueden desempeñar en exteriores se encuentra la monitorización de los niveles de contaminación atmosférica y recolección de datos climáticos, gestión eficiente de cultivos, detección y prevención de incendios forestales, etcétera. En interiores, las WSNs pueden ser utilizadas como medio para la vigilancia del hogar frente a intrusiones, detección de fugas de aguas o gases y monitorización de personas en situación de dependencia, entre otros.

Otra de las posibilidades que las WSNs son capaces de ofrecer es la localización de recursos o individuos. Por un lado se pueden localizar elementos externos a la red gracias a los diferentes sensores que llevan acoplados los nodos, por ejemplo, un sensor de presencia o una cámara. Por otro lado, también es posible localizar elementos pertenecientes a la red a través la medición de ciertas características de las señales de radio intercambiadas entre los dispositivos.

Es de suponer que en un futuro cercano, cuando todos los objetos de nuestro entorno formen parte de una única red, la Red de Objetos o *Internet of Things* [9] esta última forma de localización prevalezca sobre la anterior. Existen principalmente tres métodos dependiendo de la característica observada [10]: basados en la potencia de la señal recibida (*Received Signal Strength*, RSS), basados en el ángulo de llegada de la señal (*Angle of Arrival*, AoA) y basados en el tiempo de llegada (*Time of Arrival*, ToA). Este proceso se conoce como fase de observación.

De forma general podemos distinguir cuatro grandes grupos en los que englobar las soluciones de localización dependiendo de la entidad que realiza la observación y el cálculo de la posición del dispositivo [11]. Así pues, podemos identificar soluciones en las que ambos procesos son llevados a cabo por el dispositivo o por la infraestructura de red, y otras soluciones en las que el proceso de observación es realizado

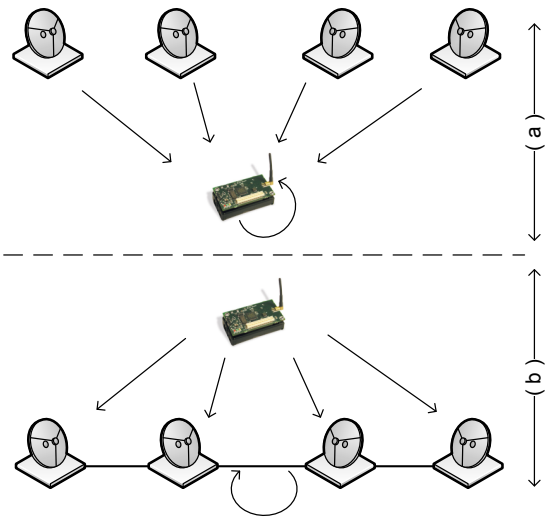


Figura 1. Esquemas de localización

por el dispositivo, que comunica tal información a la red para que realice el cálculo, y viceversa. En la Figura 1 se muestran dos esquemas básicos de sistemas de localización, en los que se presentan de manera simplificada los elementos que conforman el sistema y las partes involucradas en cada proceso. En el caso (a), el dispositivo sensor es el encargado de recoger la información recibida del sistema así como de procesar su propia localización a partir de ésta. Mientras que en el otro caso, (b), es el sistema de posicionamiento el que realiza las observaciones y calcula la ubicación del dispositivo. Esta información puede ser simplemente almacenada en el punto del sistema que realiza el cálculo o puede ser enviada a la otra parte (o una tercera) para que tenga constancia de la localización del dispositivo.

Esta clasificación es interesante por las implicaciones que tiene desde el punto de vista de la seguridad y la privacidad de los (portadores de los) dispositivos. Dependiendo de la entidad o entidades involucradas en la observación y el cálculo posterior de la posición, el sistema puede verse vulnerado desde diferentes ángulos. Así por ejemplo, si la infraestructura se limita a informar ciertos datos que permiten a los dispositivo determinar su posición, como es el caso de GPS, el dispositivo tiene pleno control sobre su información de localización quedando la privacidad de localización del usuario asegurada frente a posibles infracciones del sistema de posicionamiento.

Existen diferentes tipos de ataques que pueden afectar a la correcta localización del dispositivo. De manera general podemos encontrar dos tipos de ataques, aquellos realizados por atacantes externos y los realizados por atacantes internos [12]. Los atacantes externos son aquellos que no forman parte de la infraestructura y por tanto no pueden autenticarse con el resto de la red; su intención es convencer a un nodo o a la infraestructura de posicionamiento de que tal nodo se encuentra en una posición diferente de su posición real. Por otra parte, son atacantes internos aquellos que forman parte del sistema pero que se comportan de forma maliciosa, tratando de convencer al sistema de localización de que se encuentra en una posición diferente de la que realmente se encuentra. Asimismo, ambos tipos de atacantes pueden

tratar de suplantar a otros nodos para que el sistema de posicionamiento crea que está localizando a un nodo cuando en realidad es otro nodo el que se encuentra en esa posición. Este tipo de ataques suele tener como finalidad obtener acceso a los recursos que el nodo suplantado está autorizado o inculpar a otro dispositivo en la realización de determinadas acciones. Del mismo modo, un atacante podría hacerse pasar por el sistema de posicionamiento para intentar conseguir información confidencial de los nodos de la red. Desde el punto de vista de la privacidad, los atacantes tratan de determinar la posición de un dispositivo o hacer un seguimiento (*tracking*) del mismo sin estar autorizados para ello. La posibilidad de realizar un seguimiento de individuos abre las puertas a que se puedan llevar a cabo acciones indeseadas, desde el envío de publicidad personalizada hasta incluso acciones criminales como robos y secuestros.

Es importante en este punto recalcar que son las características físicas de la señal las que en última instancia permiten determinar la localización de los dispositivos, ubicando la fuente de la señal. Sin embargo, para identificar al dispositivo necesitamos intercambiar información adicional a nivel lógico que describa de forma única al dispositivo. Esta información en el caso de tecnologías como Bluetooth y Wi-Fi se encuentra en la forma de una dirección MAC, que no es más que un identificador que corresponde de manera única a un interfaz de red. Este identificador permanece constante a lo largo del tiempo [1], por tanto, se utiliza generalmente como medio para autenticar el origen de los paquetes de información. El uso de la MAC en las comunicaciones hace que sea posible averiguar que elementos se están comunicando en la red sin que los nodos tengan conocimiento de este hecho.

Este trabajo no pretende ofrecer una solución global a los problemas de seguridad y privacidad en sistemas de posicionamiento. Podemos afirmar que no existe tal solución, de hecho, cualquier sistema puede ser vulnerado aunque en muchas ocasiones el coste puede superar los beneficios. Incluso podemos encontrar trabajos como [13] en el que mediante el análisis de ciertas características de las señales de radio durante su etapa transitoria es posible reconocer a los dispositivos que generan tales señales de forma unívoca. Sin embargo, este tipo de análisis es bastante costoso y requiere la utilización de equipos altamente sofisticados. Por ello, en este trabajo proponemos un primer acercamiento que permita dificultar la labor de un posible atacante, resolviendo algunas de las amenazas que impedirían el buen funcionamiento de un servicio basado en localización. A continuación se describen los principales retos que nos encontramos:

- Autenticación del cliente: tenemos que evitar que un atacante puede hacerse pasar por un usuario legítimo del sistema y por tanto pueda acceder a los servicios a los que de otra forma no estaría autorizado a acceder
- Autenticación del sensor de referencia (rastreador): tenemos que evitar que un atacante pueda impersonar a los elementos del sistema de posicionamiento haciendo pensar al usuario que está comunicándose con un elemento legítimo y consiga así hacer un seguimiento de la posición del usuario.
- Privacidad de la localización: tenemos que evitar que un atacante externo con acceso a todas las comunicaciones sea incapaz de inferir los clientes que se encuentran encuentran en una determinada posición por la observación de los mensajes intercambiados entre el cliente y el sistema de posicionamiento.

Además de los retos de seguridad y privacidad propuestos hemos de tener en cuenta la usabilidad de las soluciones. Esto también supone un reto en el momento de la implantación del sistema. No es deseable que los usuarios tengan que participar constantemente y de manera activa en el proceso de localización o que se introduzca una sobrecarga excesiva en el sistema como consecuencia de querer mantener ciertos niveles de seguridad y privacidad. Es necesario encontrar un equilibrio entre los niveles de seguridad y usabilidad. En la Cuadro I se muestra una comparativa entre las tecnologías más utilizadas para localización *indoor* en la que se hace referencia tanto a aspectos de seguridad como de usabilidad.

	Wi-Fi	BT	RFID
Autenticación Cliente	Si	Si	Si
Autenticación Rastreador	Si	Si	Si
Privacidad Localización	No	No	Si
Sin Interacción Usuario	Si	Si	No

Cuadro I
COMPARACIÓN DE TECNOLOGÍAS

En lo relativo a la autenticación, tanto del cliente como del rastreador, las tres tecnologías consideradas en Cuadro I pueden proporcionar esta característica. Sin embargo, en el caso de optar por Wi-Fi y Bluetooth, que suelen utilizar como mecanismo para la localización la transmisión de beacons (o balizas), éstas no ofrecen los mecanismos pertinentes para facilitar la autenticación. Si bien es cierto que de manera opcional puede optarse por realizar la autenticación entre las partes comunicantes, ésta sólo se considera en el momento de realizar una conexión entre dispositivos. El problema de requerir el establecimiento de una conexión entre ambos dispositivos es su excesivo coste tanto en tiempo como en recursos (batería). Por su parte, las tecnologías utilizadas en las tarjetas sin contacto fueron diseñadas para mecanismos de control de acceso, por tanto pueden proporcionar autenticación mutua.

Debido a que los dispositivos dotados de tarjetas Wi-Fi y/o Bluetooth suelen utilizar su dirección física en el proceso de localización y que esta dirección es por lo general estática, un atacante que se encuentre a la escucha de las comunicaciones sería capaz de hacer un seguimiento de los dispositivos involucrados. Estas tecnologías no ofrecen ningún mecanismo que evite esta seria amenaza. Si bien hay algunos protocolos de autenticación para tarjetas inteligentes que proporcionan privacidad de localización, se presupone que dado que las comunicaciones por inducción electromagnética se realizan a muy corta distancia, es difícil que se puedan interceptar las comunicaciones incluso cuando el protocolo no proporcione privacidad de localización.

Asimismo, en este trabajo consideramos la usabilidad como un factor fundamental y por tanto requerir al usuario que

[1] Aunque existe la forma de modificar la dirección MAC de algunos interfaces de red, no es un proceso que se realice de manera automática sin necesidad de que intervenga el usuario. Además, el cambio de la dirección MAC es posible únicamente en determinados dispositivos, siendo una tarea vetada en la mayoría de dispositivos móviles.

intervenga en el proceso de localización supone una traba en el diseño del sistema de localización. En el caso de las tecnologías Wi-Fi y Bluetooth, no se requiere la interacción por parte del usuario, basta con que éste lleve consigo su dispositivo con el interfaz de red correspondiente activado para que el sistema de localización pueda ubicarlo. Sin embargo, esto no es así en el caso de las tarjetas sin contacto, que debido a su corto alcance requiere que el usuario acerque su etiqueta al lector para que éste sea capaz de detectar su presencia.

La utilización de nodos sensores para localización de los usuarios puede resultar por si mismo utópico e intrusivo puesto que el usuario tendría que llevar consigo un dispositivo cuyo único cometido es interactuar con el sistema de localización. Sin embargo, se prevé que en un futuro próximo los sensores serán elementos de uso generalizado en la sociedad al igual que lo son ahora los teléfonos móviles [14][9]. Bajo estas previsiones todos llevaremos con nosotros algún dispositivo con capacidad computacional y para comunicarse basado en estándares como IEEE 802.15.4 [15], ya sea en forma de una red de área corporal (*Body Sensor Network*, BSN) o como dispositivos independientes (p.ej.: un llavero o un reloj), que puedan desempeñar las funciones que se presentan en este trabajo.

Por tanto, nuestro objetivo es proporcionar una solución de localización segura que proporcione privacidad de localización y que además no requiera de interacción por parte del usuario.

III. Esquema de Localización Privada y Segura con WSN

La funcionalidad básica que se espera de un servicio de localización es el posicionamiento de los usuarios dentro de un mapa del edificio. De esta forma los usuarios pueden compartir su localización con otros usuarios que se encuentren en el mismo edificio o incluso en otro edificio. Para ello, una solución es que la posición de cada individuo se reporte directamente a un servidor de localización que mantiene una base de datos con la posición de todos los usuarios registrados del sistema.

Idealmente cuando un usuario se aproxima a un edificio su dispositivo de localización *indoor* inicia una negociación con el edificio de forma que se establece una relación de confianza entre ambos, lo cual permite que el usuario pueda acceder a los servicios basados en localización prestados por el edificio. Para ello se le puede requerir al usuario que presente ciertas credenciales que lo identifiquen como un usuario autorizado a hacer uso los servicios disponibles en el edificio. Cuando un usuario es desconocido por el edificio se le puede permitir un acceso limitado a los servicios de localización ofertados.

La pieza básica para que este esquema funcione es la localización de los nodos sensores por parte de los nodos que forman parte del sistema de referencia. Esta localización se tiene que llevar a cabo de forma segura tanto para el sistema como para sus usuarios. Ahí es donde entra nuestro desarrollo.

III-A. Plataforma de Programación

Para demostrar la viabilidad de nuestro esquema de localización hemos diseñado una prueba de concepto utilizando la plataforma de sensores MICAz [16] de la compañía Crossbow Technology. Este tipo de dispositivos permite la creación de redes de sensores de bajo consumo gracias principalmente al transceptor de radio y al microcontrolador que incorporan. El transceptor se trata del CC2420 de Texas Instruments [17], el cual es compatible con IEEE 802.15.4 y Zigbee. Por tanto, es capaz de trabajar en la banda de frecuencia de 2.4 GHz y de ofrecer una tasa de transferencia de datos que puede llegar a alcanzar los 250 Kbps, con potencias de transmisión que oscilan entre los -25 dBm y 0 dBm. El microcontrolador es el ATmega128L fabricado por Atmel [18]. Se trata de una arquitectura RISC de 8 bits con capacidad para trabajar a una velocidad de hasta 8MHz. Es interesante notar que, aunque la especificación establece una frecuencia máxima de procesamiento de 8 MHz, al estar alimentados por dos baterías del tipo AA (3 voltios), la frecuencia de funcionamiento suele reducirse a 4 MHz[2]. Además, ofrece una memoria flash programable de 128 KB, una memoria RAM de 4 KB y finalmente una memoria externa de 512 KB dedicada principalmente al almacenamiento de mediciones.

Los nodos sensores utilizan el sistema operativo TinyOS [19]. TinyOS es un sistema operativo de código abierto diseñado específicamente para su utilización en redes de sensores inalámbricas. Presenta una arquitectura basada en componentes lo cual posibilita la fácil integración y eliminación de funcionalidades al tiempo que se minimiza el tamaño del código, lo cual es un factor determinante en las plataformas para las que está diseñado. Entre las funcionalidades ofrecidas de forma nativa se encuentran protocolos de red, componentes para el acceso a los sensores, mecanismos para la comunicación a través del puerto serie con un PC y así hacer las veces de estación base, herramientas para la lectura y escritura en memoria, etcétera. El lenguaje de programación utilizado para el desarrollo de aplicaciones es NesC [20], que es básicamente una extensión del lenguaje C diseñado para incorporar los conceptos de estructuración y el modelo de ejecución de TinyOS.

III-B. Arquitectura del Sistema

El sistema desplegado para la realización de la prueba de concepto se compone principalmente de dos tipos de nodos, los primeros son aquellos que los usuarios llevan consigo y en el segundo tipo se encuentran los nodos que forman parte del sistema de localización, que en adelante llamaremos indistintamente *anchors* o rastreadores. Ambos tipos de nodos son idénticos en cuanto a las capacidades que ofrecen, salvo que los integrantes del sistema de posicionamiento se encuentran conectados a través del puerto serie del ordenador para la comunicación de los datos de localización al servidor central que mantiene una base de datos sobre la ubicación de los diferentes usuarios del sistema.

III-C. Implementación de la Prueba de Concepto

La implementación de nuestro esquema se ha basado principalmente en la utilización de cuatro elementos que han posibilitado la localización de los usuarios de manera no intrusiva al mismo tiempo que se preserva la privacidad de localización de los usuarios, evitando que puedan ser

[2]Este valor es establecido por defecto en el sistema operativo TinyOS para reducir así el consumo energético

rastreados por agentes externos, y se autentica a las partes comunicantes:

- Compartición de una clave simétrica: tanto los sensores legítimos del sistema como los elementos del sistema de localización comparten una clave que en la implementación actual es cargada durante el despliegue del sistema. Esta clave puede ser actualizada de manera ocasional mediante un mecanismo de refresco de claves.
- Eliminación de identificador: los mensajes transmitidos por los nodos de una red de sensores son, por norma general, encapsulados en tramas compatibles con el estándar IEEE 802.15.4. Éstas contienen una serie de campos que sirven para identificar a los nodos que componen la red. Para evitar que un atacante que se encuentre escuchando las comunicaciones pueda tracear a un individuo es necesario eliminar esta información.
- Ajuste de la potencia de transmisión: limitar la potencia en la que los rastreadores emiten las señales de beaconing permite a los sensores responder únicamente a aquellas señales emitidas por dispositivos que se encuentran en un rango de acción reducido.
- Frescura de los datos: es necesario garantizar que los datos generados son frescos, es decir, que ningún adversario sea capaz de reproducir un mensaje de respuesta a una baliza antigua y así conseguir suplantar a un usuario. Este tipo de ataque se conoce como ataque por repetición.

Las limitaciones en términos computacionales, energéticos y de almacenamiento inherentes a los nodos de una red de sensores dificultan la utilización de primitivas criptográficas complejas. Por este motivo, en los primeros trabajos de seguridad en WSNs se consideraba que la criptografía de clave pública era excesivamente exhaustiva para poder ser utilizada en este ámbito [21][22], al requerir unos tiempos para la generación de la claves y verificación de firmas de varias decenas de segundos. Aunque esta visión ha ido cambiando en los últimos años gracias a la evolución de la criptografía de curva elíptica, que ha conseguido reducir los tiempos a pocos segundos, desde el punto de vista del rendimiento aún sigue siendo más aconsejable utilizar criptografía de clave simétrica al ser capaz de ofrecer tiempos del orden de micro segundos [23]. El principal inconveniente de los algoritmos de clave simétrica es la gestión de claves.

Esto ha motivado la elección del algoritmo de clave simétrica AES con un tamaño de bloque de 128 bits y por tanto con el mismo tamaño de clave. Esta implementación fue desarrollada en el ámbito del proyecto europeo SMEPP [24] y ha sido adaptada para nuestros propósitos actuales. Además, para reducir el problema de la distribución de claves se ha optado por precargar a los sensores involucrados en el proceso de localización con la clave AES antes del despliegue del sistema.

Por otra parte se hace necesario eliminar de los paquetes de datos cualquier información que pudiera identificar a los nodos. Esto se convierte en un requisito indispensable ya que en caso de mantener un identificador constante por cada usuario del sistema, un agente externo tendría la posibilidad de hacer un seguimiento de sus movimientos. Este es uno de los problemas principales de tecnologías como Wi-Fi y Bluetooth, que en las capas más bajas de la pila de protocolos proporcionan direcciones de enlace (MAC) que son únicas para cada dispositivo. Existen principalmente dos formas de solventar este problema, la primera es utilizar pseudónimos y la segunda es utilizar un mismo identificador para todos los dispositivos. En caso de optar por la utilización de pseudónimos, es decir, un identificador que se utiliza en lugar del verdadero identificador, éste no puede ser estático ya que sería cuestión de tiempo que un atacante pudiera rastrearlo. Por tanto, es necesario que los pseudónimos vayan cambiando de manera ocasional, lo que requiere de un mecanismo de sincronización entre dispositivos para que la comunicación sea posible. El segundo caso es utilizar un identificador común para todos los dispositivos, lo cual los hace indistinguibles entre sí. Esto no permite la identificación a nivel de enlace y por tanto el encaminamiento de paquetes se ve imposibilitado. Sin embargo, nuestro esquema al no requerir de mecanismos de encaminamiento, la identificación se puede realizar a nivel de aplicación, información que se encuentra debidamente protegida mediante AES.

Asimismo en nuestra implementación hemos utilizado un mecanismo basado en el ajuste de la potencia de transmisión con el fin de limitar el radio de acción de los nodos que forman parte del sistema de posicionamiento. Al reducir el alcance de las señales emitidas por los rastreadores, sólo aquellos usuarios que se encuentran en sus proximidades tendrán acceso a las balizas y serán capaces de responder. El tiempo de respuesta debe encontrarse debidamente limitado, lo cual se deja a la elección del administrador del sistema. De manera obvia, el tiempo de espera para la llegada de balizas no debe ser excesivamente elevado por una razón principal: un tiempo elevado permite que un nodo que se encuentra en las proximidades del *anchor*, y que tiene acceso a las balizas, pueda repetir esta información a otro nodo que se encuentra fuera del alcance de éste. El nodo remoto, a su vez, respondería al nodo que hace de puente en la comunicación para hacer pensar al *anchor* que el nodo remoto también se encuentra en las inmediaciones del *anchor*. Del mismo modo, la potencia de transmisión es también un parámetro que se deja a la elección del administrador del sistema, dependiendo de las necesidades de cada instalación. En concreto, los nodos que se han utilizado para la prueba de concepto, los cuales integran el chip de radio CC2420, permiten utilizar diferentes potencias de transmisión. TinyOS ofrece una función (`CC2420Packet.setPower`) que permite modificar el registro que controla el nivel de transmisión para cada mensaje de manera individual. En nuestro caso hemos utilizado un valor que ofrece un rango de transmisión que se encuentra en torno a los 30 centímetros.

Para garantizar la frescura de los datos enviados, evitando así ataques por repetición, se ha optado por que las balizas enviados por los sensores que componen el sistema de localización contengan datos generados a partir de una función pseudoaleatoria. En particular, los balizas contienen un número pseudoaleatorio con una longitud de 32 bits, lo cual ofrece un espacio de direccionamiento lo suficientemente grande como para evitar que se produzcan colisiones en un largo espacio de tiempo. Los nodos llevados por los usuarios, al recibir las balizas, extraerán su contenido y lo anexionarán

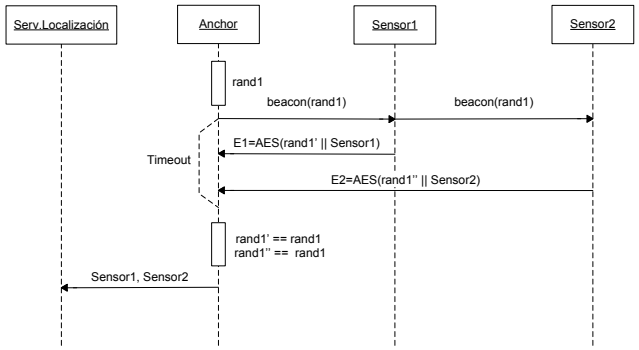


Figura 2. Diagrama de secuencia de la prueba de concepto

con su número de serie, el cual es único para cada dispositivo y que es precargado en la fase previa al despliegue del sistema. Finalmente, se aplicará el algoritmo de cifrado sobre esta información y se enviará de vuelta al *anchor*, el cual utilizará la clave compartida entre ambos para descifrar tal información. En caso de tratarse de un usuario legítimo del sistema, el número aleatorio corresponderá con el enviado por el *anchor* instantes previos y éste podrá extraer el número de serie del dispositivo, identificando así al usuario.

En la Figura 2 se muestra un ejemplo reducido de un posible intercambio de mensajes realizado entre los participantes del sistema de localización y los usuarios del sistema. En concreto se muestra una secuencia completa de localización en la que un *anchor* envía una baliza con un número aleatorio, el cual es recibido por Sensor1 y Sensor2. Estos generan el mensaje de respuesta e inmediatamente después lo envían a el *anchor*, que los procesa y comprueba su autenticidad. En caso afirmativo, los números de serie de los sensores se envían al Servidor de Localización, que almacena la información sobre la ubicación de tales sensores.

Además, es interesante notar que cualquier usuario puede decidir en un momento determinado deshabilitar su dispositivo sensor para evitar ser localizado por el sistema o por otros usuarios que compartan la misma clave. Esto supone un valor añadido a la privacidad de los usuarios, que tienen el control sobre cuándo pueden ser localizados.

III-D. Aplicación dentro del proyecto OSAmI

El proyecto OSAmI-Commons [25] es un proyecto avalado por el programa Eureka-ITEA2 y financiado por el Plan Avanza a nivel nacional, en el que participan empresas líderes europeas, institutos de investigación y universidades, y que tiene como objetivo el desarrollo de la plataforma base para aplicaciones de *Inteligencia Ambiental*. La Inteligencia Ambiental se puede ver como el espacio de interacción de las personas y las tecnologías en su vida cotidiana. Estas tecnologías identifican nuestra presencia y son capaces de dar respuesta a nuestras necesidades y hábitos de una forma invisible y anticipatoria. Por otra parte, las necesidades de privacidad de los usuarios tienen que verse salvaguardadas de igual forma.

Uno de los escenarios de aplicación del proyecto, proporcionado por Telefónica, se centra en servicios multimedia que sean sensibles a la localización, de forma que el contenido multimedia vaya siguiendo al usuario mientras de mueve por el edificio. El desarrollo proporcionado no depende de la tecnología de posicionamiento utilizada. Para ello se ha desacoplado el servidor de localización, que mantiene información de la posición de los usuarios, de los sistemas de referencia que captan la posición del usuario. De esta forma se puede localizar a un mismo usuario usando varias tecnologías de forma simultánea.

Uno de los problemas que quedaban abiertos y que se pretenden resolver dentro de OSAmI en el campo de servicios basados en la localización es el de proporcionar otros mecanismos de localización que permitieran un alto grado de seguridad para el usuario y que a su vez se acoplaran con los desarrollos existentes dentro del proyecto. Podemos considerar este trabajo como un primer acercamiento en esa dirección.

IV. Mejoras sobre el esquema inicial

Uno de los mayores problemas de seguridad que presenta nuestra prueba de concepto es que todos los usuarios comparten la misma clave con el sensor del sistema de localización. Esto implica que un usuario legítimo del sistema puede descifrar el mensaje de respuesta enviado por otro usuario y obtener su número de serie, que podrá utilizar para suplantarlo. Una posible solución, que está actualmente en fase de desarrollo, es utilizar, de manera adicional a la clave compartida (K_A), una clave simétrica (K_i) diferente por cada nodo, que sería compartida entre cada nodo y el servidor de localización, de manera análoga al servicio de autenticación de la identidad del subscriptor en GSM [26]. De esta forma, en la respuesta de los sensores, en lugar de cifrar únicamente con la clave compartida por todos los nodos legítimos el número de serie junto al número aleatorio enviado por los sensores de referencia, se utilizaría la clave K_i de cada nodo para cifrar dicho número aleatorio, que junto con el número de serie del nodo, sería nuevamente cifrado con la clave del grupo K_A. De esta forma, los nodos legítimos no son capaces de impersonar a otros nodos, ya que no serían capaces de cifrar el número aleatorio con la clave correspondiente. Como contrapartida necesitamos que el servidor de localización se involucre de forma activa en el proceso de localización, dejando de ser una mera base de datos y liberando de carga computacional a los *anchors*s de la red que pasarían a comportarse como proxies del proceso de localización. La Figura 3 muestra el diagrama de secuencia que describe este proceso.

Si bien es cierto que un atacante externo podría enviar balizas haciéndose pasar por un rastreador, ya que no se ofrece información que autentique que una baliza ha sido generada de manera legítima por un rastreador, el atacante no podría obtener la identidad del usuario puesto que desconoce la clave de descifrado. No obstante, esto puede suponer un ataque de denegación de servicio específico en el ámbito de las redes de sensores, el ataque por agotamiento de baterías. Aunque en la presente propuesta no se proporcionan los mecanismos adecuados para hacer frente a este tipo de amenaza, en la actualidad nos encontramos desarrollando una nueva versión del prototipo que tiene en cuenta esta forma de ataque.

En nuestro esquema, tanto los usuarios que quieren acceder a los servicios basados en localización como los equipos de localización o rastradores comparten un clave simétrica

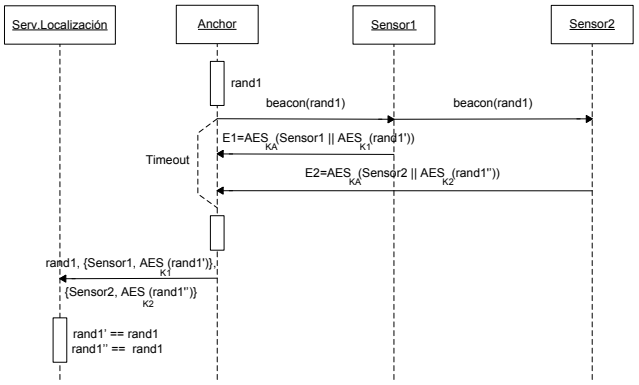


Figura 3. Diagrama de secuencia esquema avanzado

de cifrado. Esta clave puede ser la misma para todos los edificios o puede ser una diferente para cada zona *indoor*. En nuestra implementación de referencia solo hemos trabajado con una zona de localización *indoor* y por tanto solo se comparte una clave. En caso de que quisiéramos usar una clave distinta por cada edificio se podría que definir un conector con GPS para que al acercarse a cada edificio se estableciera la clave apropiada. Otra posibilidad sería enviar junto al número aleatorio un identificador de zona que podría servir para indicar la clave a utilizar. Por último, podríamos establecer un protocolo de intercambio de claves entre la zona y el sensor, basado en criptografía de clave pública, que nos permita negociar la clave de zona apropiada cada vez que cambiemos de zona. Trabajos recientes en criptografía de clave pública basada en curvas elípticas para WSNs, en concreto basada en la misma plataforma que hemos utilizado para nuestra prueba de concepto, dan tiempos inferiores a los 500 ms [27] por operación de firma o cifrado.

Al utilizar todos los usuarios la misma clave dentro de la misma zona *indoor* se permite que los usuarios puedan localizar de forma autónoma a sus compañeros, a la vez que se impide que usuarios externos al sistema, es decir que no conozcan la clave, puedan inferir nada de nuestra localización. Si utilizamos el esquema de autenticación avanzado donde cada nodo usa una clave diferente para cifrar el número aleatorio tenemos el inconveniente de que los otros nodos no podrán verificar la identidad de sus compañeros al desconocer la clave que cada nodo comparte con el servidor de localización. De hecho los vecinos, aunque son capaces de obtener el número de serie del nodo, no son capaces de saber a ciencia cierta si se trata de un nodo legítimo el que crea el mensaje ya que sólo el servidor de localización puede comprobar que el número aleatorio cifrado es legítimo.

Por último, en el desarrollo inicial se considera que la comunicación entre los *anchors* y el servidores de localización se realiza por un canal seguro. En la práctica esto se traduce en la necesidad de utilizar algún mecanismo criptográfico para proteger las comunicaciones entres los anchos y el servidor. Dado que los *anchors* tiene suficiente poder computacional, para este fin se podrían utilizar protocolos estándar como WS-Security o incluso TLS.

Actualmente estamos trabajando en una nueva versión del sistema que tenga en cuenta todos estos aspectos.

V. Conclusiones y Trabajo Futuro

En este trabajo hemos presentado el desarrollo de un sistema de localización para entornos *indoor* capaz de resolver algunos de los problemas de seguridad y privacidad que pueden acontecer a lo hora de proporcionar servicios basados en localización. En concreto nos hemos centrado en resolver principalmente dos de los problemas que consideramos de mayor relevancia para este tipo de servicios, es decir, evitar la suplantación de los usuario que hacen uso del sistema y evitar que un atacante externo sea capaz de obtener información privada sobre los usuarios, p.ej. qué usuarios acceden a qué servicios o dónde se encuentra un usuario en un momento determinado. Al mismo tiempo, al encontrarse basada en el uso de redes de sensores inalámbricas, nuestra propuesta trata de ser lo menos intrusiva y lo más liviana posible. Por ello, en lugar de centrarse en la utilización de innumerables intercambios de mensajes entre el dispositivo del usuario y el sistema de localización o operaciones criptográficas con un elevado nivel de complejidad, la propuesta se centra principalmente en el uso de un cifrado AES de 128 bits para la generación de pseudónimos dinámicos para cada nueva transacción.

Un aspecto que queremos hacer notar es que el esquema que se presenta en este trabajo no trata de ser la solución definitiva a los problemas planteados a lo largo del artículo. Nuestro objetivo con este trabajo es hacer notar la necesidad de estudiar la problemática de seguridad que aparece en este tipo de entornos así como la necesidad de proporcionar la implantación de mecanismos de identificación privada en futuros desarrollos, de manera que sea posible acceder a diferentes servicios sin que entidades externas sean capaces de identificar al usuario que hace uso de estos. Además, es interesante recalcar que los problemas de privacidad siguen existiendo ya que este problema puede aparecer a distintos niveles. En nuestro caso nos hemos centrado en el nivel más bajo, el de las comunicaciones físicas. Sin embargo, si consideramos que un servicio determinado al que estamos accediendo puede seguirnos a medida que nos movemos, por ejemplo un flujo multimedia, a pesar de utilizar pseudónimos en los niveles más bajos, un observador podría relacionar un flujo determinado con un dispositivo.

Como trabajo futuro pretendemos ampliar nuestro esquema de manera que los dispositivos que llevan los usuarios puedan ser localizados no sólo por un único elemento del sistema de referencia, sino que los distintos *anchors* colaboren entre sí para determinar la posición de los usuarios del sistema. Esto traerá consigo nuevas oportunidades gracias a la posibilidad de incorporar a las técnicas hasta el momento propuestas, otros mecanismos de localización más avanzadas, como la triangulación. Sin embargo, esto también dará lugar a nuevos desafíos tanto desde el punto de vista de la comunicación y coordinación entre los distintos dispositivos del sistema como desde la perspectiva de la seguridad y la privacidad. En concreto, al existir más interacción entre dispositivos y la necesidad de realizar comunicaciones salto a salto hasta alcanzar a la estación base, la privacidad de localización se verá afectada.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado a través de los siguientes proyectos: OSAmI (TSI-020400-2009-92), financiado por el Ministerio de Industria, Turismo y Comercio mediante el Plan Avanza; y SPRINT (TIN2009-09237), financiado por el Ministerio de Ciencia e Innovación y cofinanciado por FEDER (Fondo Europeo de Desarrollo Regional).

REFERENCIAS

[1] Z. Hunaiti, A. Rahman, M. Denideni, and W. Balachandran, "The impact of galileo on pedestrians navigation systems," *Electronics, Communications, and Computers, International Conference on*, vol. 0, p. 40, 2006.

[2] G. Ghiani, F. Paterno, C. Santoro, and L. D. Spano, "UbiCicero: A location-aware, multi-device museum guide," *Interacting with Computers*, vol. 21, no. 4, pp. 288 – 303, 2009.

[3] CISCO, "Wi-Fi Location-Based Services - Design and Deployment Considerations." [Online]. Available: https://learningnetwork.cisco.com/docs/DOC-3418

[4] M. Thomson, J. Winterbottom, and A. Corporation, *Locations with Locally-Defined Coordinate Reference Systems for PIDF-LO*, IETF Network Working Group Internet draft, 2009. [Online]. Available: http://tools.ietf.org/html/draft-thomson-geopriv-indoor-location-01

[5] A. Zafeiropoulos, I. Papaioannou, E. Solidakis, N. Konstantinou, P. Stathopoulos, and N. Mitrou, "Exploiting Bluetooth for deploying indoor LBS over a localisation infrastructure independent architecture," *International Journal of Computer Aided Engineering and Technology*, vol. 2, no. 2, pp. 145–163, 2010.

[6] S. Aparicio, J. Pérez, P. Tarrío, A. M. Bernardos, and J. R. Casar, "An indoor location method based on a fusion map using bluetooth and wlan technologies," in *DCAI*, 2008, pp. 702–710.

[7] Crossbow Technology, "MTS/MDA Sensor Board Users Manual," 2007. [Online]. Available: http://www.xbow.com/support/Support_pdf_files/MTS-MDA_Series_Users_Manual.pdf

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393 – 422, 2002.

[9] European Commission, "Internet of Things in 2020 - A Roadmap for the Future," Sept. 2008. [Online]. Available: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[10] M. Vossiek, L. Wiebking, P. Gulden, J. Wieghardt, C. Hoffmann, and P. Heide, "Wireless Local Positioning," *Microwave Magazine, IEEE*, vol. 4, no. 4, pp. 77 – 86, dec. 2003.

[11] A. I. G.-T. Ferreres, B. R. Álvarez, and A. R. Garnacho, "Guaranteeing the Authenticity of Location Information," *IEEE Pervasive Computing*, vol. 7, no. 3, pp. 72–80, 2008.

[12] S. Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," in *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, Feb. 2006, pp. 221–232.

[13] K. Bonne Rasmussen and S. Capkun, "Implications of Radio Fingerprinting on the Security of Sensor Networks," in *Proceedings of IEEE SecureComm*, sept. 2007, pp. 331 –340.

[14] M. Chui, M. Löffler, and R. Roberts, "The Internet of Things," McKinsey Quarterly, March 2010. [Online]. Available: https://www.mckinseyquarterly.com/High_Tech/Hardware/The_Internet_of_Things_2538

[15] IEEE 802.15 WPAN TG4b, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Computer Society Std., 2006. [Online]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

[16] Crossbow Technology, "MICAz 2.4 GHz - Wireless Module." [Online]. Available: http://www.xbow.com/Products/productdetails.aspx?sid=164

[17] Texas Instruments, "CC2420 - 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver." [Online]. Available: http://focus.ti.com/lit/ds/symlink/cc2420.pdf

[18] ATMEL, "ATmega128l Datasheet." [Online]. Available: http://www.atmel.com/dyn/resources/prod_documents/doc2467.pdf

[19] TinyOS Community Forum, "An open-source OS for the networked sensor regime." [Online]. Available: http://www.tinyos.net/

[20] P. Levis, "TinyOS Programming," June 2006. [Online]. Available: http://csl.stanford.edu/~pal/pubs/tinyos-programming.pdf

[21] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[22] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. New York, NY, USA: ACM, 2004, pp. 162–175.

[23] R. Roman, C. Alcaraz, and J. Lopez, "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes," *Mobile Networks and Applications*, vol. 12, no. 4, pp. 231–244, 2007.

[24] SMEPP Project, "Secure middleware for embedded p2p systems." [Online]. Available: http://www.smepp.org/

[25] OSAMI, "Open source ambient intelligence commons for an open and sustainable internet." [Online]. Available: http://www.osami-commons.org/

[26] H. Imai, *Wireless Communications Security*, M. G. Rahman and K. Kobara, Eds. Artech House, Inc., 2006.

[27] D. Aranha, L. Oliveira, J. Lopez, and R. Dahab, "NanoPBC: Implementing Cryptographic Pairings on an 8-bit Platform," in *CHiLE 09 - Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc*, 2009.

Computación Segura Multiparte Aplicada a Subastas Electrónicas

José A. Montenegro, Javier López
Dpto. Lenguajes y Ciencias de la Computación
ETSI Informática Málaga. Universidad de Málaga
monte@lcc.uma.es, jlm@lcc.uma.es

Rene Peralta
Computer Security Division
National Institute of Standards and Technology.
peralta@nist.gov

***Resumen*—La confidencialidad ha pasado de ser un requisito de seguridad a ser considerado como requisito funcional y de obligado cumplimiento e inclusión en todos los sistemas de comunicaciones. Un inconveniente que presenta las técnicas criptográficas, utilizadas para obtener la confidencialidad de la información, surge cuando varias entidades se ven forzadas a compartir información secreta para realizar tareas puntuales de colaboración, ya que las primitivas tradicionales utilizadas para conseguir la confidencialidad resultan poco flexibles. La situación ideal permitiría hacer posible dicha colaboración sin que ninguna de las partes revele la información aportada. En este escenario entra en juego la tecnología de Computación Segura Multiparte (CSM) que posibilita realizar operaciones con la información compartida sin tener que hacerla pública. Este trabajo muestra una solución CSM aplicada a una subasta electrónica que permite la realización de la subasta sin que las apuestas sean reveladas a ningún participante, incluyendo el subastador, por lo que no necesita el estableciendo de ninguna autoridad confiable. Aunque la literatura ofrece una amplia variedad de propuestas teóricas de CSM desde su creación en la década de los ochenta, no es común su aplicación práctica en situaciones reales.**

***Palabras Clave*—Pruebas Discretas, Protocolo Conocimiento Cero, Cifrado Probabilístico, Computación Multiparte, Subastas Electrónicas.**

I. Introducción

La Computación Segura Multiparte (CSM), es un tipo de protocolo de comunicación que permite a una serie de participantes ponerse de acuerdo con el valor resultante de una función pública aplicada a sus datos privados, sin hacerlos públicos. Una amplia serie de problemas en e-commerce y e-government pueden ser resueltos aplicando CSM. Como ejemplo concreto de escenarios de aplicación destacamos los dos siguientes:

- Subastas públicas donde una organización gubernamental muestra el interés en subastar un bien público y las empresas participantes no quieren desvelar información sobre sus apuestas. Numerosos estudios establecen la convicción que la revelación de las cantidades subastadas podría perjudicar a las empresas en sucesivas subastas, así como revelar importante información sobre el estado financiero de la empresa.
- Voto electrónico donde los datos confidenciales a preservar son las decisiones de los votantes sobre los candidatos y el valor de la función representa el ganador de la elección.

La solución tradicional aplicada a ambos casos, ha sido la utilización de sobres de papel para preservar la información confidencial. Para realizar una transición de estas aplicaciones a un mundo electrónico, es necesario establecer un modelo criptográfico que simule el sobre tradicional. Aunque existen actualmente varias soluciones genéricas CSM, y que cumplen con una complejidad polinómica, desde el punto de vista de utilización de recursos computacionales pueden ser catalogadas de poco prácticas. Este es el principal motivo por el cual planteamos un nuevo modelo que pretende establecer una solución acorde con requisitos reales a este tipo de problemas.

Como marco de aplicación hemos seleccionado una subasta electrónica pública, concretamente la denominada subastas Vickrey. Este tipo de subasta recibe el nombre del ganador del premio Nobel de Economía en 1996, William Spencer Vickrey. Su característica más representativa, y que la distingue de los otros modelos de subastas, es que el ganador de la subasta es el usuario que realiza la mayor apuesta, sin embargo el precio del objeto subastado es el valor de la segunda apuesta más elevada. Esta simple característica tiene un impacto regulador en el precio de los elementos subastados, evitando que los postores paguen más por el elemento subastado que su valor real [24].

Aunque las subastas que siguen el modelo Vickrey aportan propiedades deseables en las subastas públicas, el diseño original no contempla la necesidad de mantener confidencial las apuestas de los usuarios. Por este motivo hemos considerado la necesidad de desarrollar una variación denominada como Subasta Vickrey a sobre cerrado, donde la apuesta de un usuario es desconocida por los restantes usuarios del sistema, revelando solamente las dos apuestas más elevadas de la subasta. Para conseguir dicha tarea haremos uso de CSM así como de elementos criptográficos adicionales que serán detalladas durante el trabajo.

El artículo es estructurado de la siguiente forma, la sección II establece una revisión en la literatura de las propuestas realizadas sobre subastas electrónicas. El diseño del sistema de subasta electrónica es descrito en la sección III, detallando los componentes del sistema que forman parte de él.

La sección IV realiza una breve introducción a la Computación Segura Multiparte y define la función utilizada para comparar dos apuestas confidencialmente. Debido a que las apuestas no son reveladas es necesario establecer un proceso de generación y verificación de retos sobre la función de comparación, así como también es necesario el establecimiento de una estructura de datos y un proceso de verificación de los retos. Para completar esta sección será presentado el concepto de Pruebas Discretas así como los distintos modelos de pruebas discretas que es posible

desarrollar: Pruebas Manuales, Pruebas No Interactivas y Pruebas No Interactivas Reducidas.

Los detalles sobre la implementación del sistema son especificados en la sección V, así como el rendimiento del sistema traducido al tiempo de creación y verificación de las pruebas en sus distintas modalidades. Para finalizar, la sección VI ofrece las conclusiones sobre el trabajo desarrollado y las líneas de trabajo futuras.

II. Trabajo Previo sobre Subastas a sobre cerrado

El diseño de una subasta segura o subasta a sobre cerrado ha sido una área de trabajo activa durante la última parte de los noventa y en la actual década. Esta situación fue estimulada por la decisión de la Comisión Federal de Comunicaciones NorteAmericana (FCC) de asignar las licencias en 1994 para el espectro electrónico mediante subastas competitivas y la necesidad de cumplir principalmente los requisitos de confidencialidad.

Desafortunadamente la mayoría de las soluciones propuestas hacen un mayor hincapié en la creación de nuevas primitivas criptográficas que en el diseño de un sistema seguro que mantenga las propiedades de seguridad de una subasta.

El artículo [9] puede ser considerado como el primer acercamiento para abordar los requisitos de las subastas electrónicas. El trabajo básicamente está orientado a la creación de una nueva primitiva criptográfica denominada *verifiable signature sharing*. A grandes rasgos, la primitiva habilita al titular de un mensaje firmado para compartir la firma entre un grupo de usuarios. Sólo los miembros de un grupo pueden reconstruir la firma. El principal inconveniente de esta propuesta es que todas las apuestas son reveladas a la finalización del periodo de apuesta.

Los autores en [17] diseñan una nueva primitiva denominada *oblivious transfer*, pero el diseño del sistema resultante puede ser catalogado como poco práctico. Esta primitiva fue mejorada en el trabajo [14] con la modificación de la primitiva y la creación de *verifiable proxy oblivious transfer*. Aunque la nueva propuesta fue diseñada para resolver un fallo de seguridad de la propuesta anterior, los autores hacen una declaración implícita de que la nueva primitiva requiere una cantidad excesiva de cómputo y de comunicación entre las partes involucradas.

Omote et al. presentan en [19] un esquema que hace uso de dos tipos de administradores de la subasta, uno que es el encargado del registro de los postores, y otro que administra la fase de apuestas. Únicamente la cooperación de ambas entidades y el ganador pueden decidir determinar cuál es la apuesta ganadora. La propuesta es una mejora del trabajo [2] que hace uso de cifrado homomórfico y de la técnica *mix match*. Aunque el trabajo ofrece una descripción técnica muy considerable, no incluye ninguna información sobre el diseño.

Durante el desarrollo de nuestra propuesta, Damgard et al. hicieron público el desarrollo de una subasta pública [6] basada en Computación Multiparte y *pseudorandom secret sharing* [5].

III. Diseño de un Sistema de Subasta Seguro

La creación de un sistema de subastas seguras requiere del diseño y desarrollo de determinados servicios, y los protocolos que conectan dichos servicios. El trabajo [15] determina un modelo de objetos y un diagrama de flujo de datos de una subasta que hemos considerado muy útiles para la realización de nuestro sistema.

Los componentes de la subasta deben cumplir los requisitos funcionales y de seguridad que establece la naturaleza de una subasta segura. En nuestro caso, además de los requisitos de seguridad nos centraremos en cumplir con los estándares, incluso si alguno de los servicios han de ser diseñados desde cero.

- Servicio de Aleatoriedad: Tal y como conocemos los protocolos criptográficos actuales sería prácticamente imposible concebirlos sin la existencia de números aleatorios. El documento [10] es una buena referencia que demuestra el papel que juegan los números aleatorios en la criptografía. Además de la necesidad de este servicio como base para la creación de primitivas y protocolos, varios sistemas son diseñados bajo la asunción de la existencia de un generador de números aleatorios.
  La generación de números aleatorios puede llevarse a cabo mediante el uso de técnicas software o hardware. Normalmente los componentes hardware necesitan de máquinas dedicadas por lo que su utilización no resulta adecuada para los usuarios. Desafortunadamente no existe ningún estándar que define los métodos necesarios para llevar a cabo un servicio, tal como un protocolo de comunicación o la estructura de datos del protocolo.
  Por otro lado, la creación de números aleatorios basado en software es considerado como un proceso pesado desde el punto de vista computacional, por lo que usualmente hacemos uso de algoritmos más livianos como son los algoritmos pseudo aleatorios. Algunas vulnerabilidades están originadas debido a una incorrecta implementación, un uso impropio o un ataque al generador de número aleatorio o un ataque [13], [1], [11].
  Para la inclusión en nuestro sistema proponemos la creación de un servicio de aleatoriedad confiable que pueda ser creado mediante software, hardware o mediante un uso híbrido de componentes, basándonos en las recomendaciones de [7], [22].
  El servicio proporcionará números aleatorios certificados así como una prueba de la calidad del servicio. Es importante resaltar que los números que ofrece el servicio deben ser certificados para asegurar su origen.
- Servicio de Tiempo: La secuencia temporal de los eventos en una subasta tiene una influencia significativa en el rendimiento del sistema y en el desarrollo de la subasta. Normalmente, las apuestas son eventos controlados por los participantes, pero ciertos eventos importantes como la finalización del periodo de subasta implica la necesidad de incluir una fuente de tiempo confiable para determinar y verificar que las acciones han sido realizadas en un instante concreto de tiempo.
  El trabajo [25] establece un estudio en profundidad de los requisitos de tiempo real de las subastas

electrónicas. Además de la citada importancia que tiene el establecimiento de un servicio de tiempo en las tareas de la subasta, juega un papel muy importante en los protocolos criptográficos, debido a que cada paso debe ser ejecutado en un instante de tiempo preciso.
Al contrario que en el caso del servicio de aleatoriedad, el servidor y el protocolo no ha tenido que ser desarrollado, sino que específicamente hacemos uso el servicio de tiempo estándar proporcionado por National Institute of Standard and Technology (NIST)[1]. Actualmente existen tres protocolos disponibles para acceder a información relativa al tiempo. Time Protocol [21] y Daytime Protocol [20] proporciona un servicio básico y eficiente pero están considerados como obsoletos y además sus especificaciones no incluyen el soporte para los mecanismos de certificación. El tercer estándar Network Time Protocol (NTP) [18] mejora los dos anteriores estandares e incluye las propiedades de seguridad que lo hacen adecuado para nuestros requisitos.

- Servicio Clave Pública: Nuestra propuesta está basada en criptografía de clave pública, por lo que cada postor posee su par de claves criptográficas. Es bien conocido que la criptografía asimétrica necesita de la existencia de una autoridad de certificación. Estas entidades confiables vinculan la clave pública con la identidad del usuario. Varias soluciones de certificación han sido expuestas y principalmente difieren en el modelo de confianza, jerárquico o anárquico, y la estructura de los datos del certificado. En nuestro caso, siguiendo los estándares, hemos implementado solamente un nodo raíz de una Infraestructura de Clave Pública (PKI).
- Servicio de Tablón de Anuncios: Todos los servicios anteriores tienen una vinculación directa o indirecta con las propiedades de seguridad. El tablón de anuncios es un servicio impuesto por los requisitos del sistema de subasta, estando su diseño dirigido por sus propiedades.Básicamente, el tablón de anuncios es un repositorio confiable donde todos los datos relativos a la subasta son publicados. El principal objetivo es que todos los postores tengan acceso a la información generada en la subasta.
  Un requisito indispensable es que todas las apuestas sean publicadas en el tablón de forma cifrada en el momento que los postores la emitan y antes que el periodo de apuesta finalice, ya que, en caso contrario, el usuario no es considerado como un postor y no puede participar en las fases finales de resolución. Además, la apuesta publicada en el tablón será la información utilizada posteriormente como entrada de la función de comparación. El tablón de anuncio tiene una dependencia directa con el servicio de tiempo, debido a que es tan importante publicitar la información como su correcta datación.
  Una vez que la resolución de la subasta finaliza y son publicados los resultados en el tablón, comienza la fase de verificación donde las pruebas de veracidad de las funciones de comparación generadas por cada postor serán también publicadas en el tablón. A modo de resumen, la función principal del tablón es que todos los elementos de la subasta sean públicos a todos los participantes, para que todos los participantes posean la misma información y una posición igualitaria en la subasta.

[1]El servicio puede ser accedido en http://tf.nist.gov/service/its.htm y además, en la dirección http://tf.nist.gov/tf-cgi/servers.cgi podemos consultar los servidores de tiempo disponibles así como su estado en cada momento.

A. *Etapas de la Subasta*

Aunque normalmente una subasta tiene dos fases, la fase de apuesta y de resolución, hemos decidido incluir nuevas fases para hacer un mayor énfasis en cómo la seguridad incide en la subasta, de esta forma el sistema queda configurado con cinco fases:

- Configuración: El subastador establece los parámetros de la subasta y envía todos los datos al usuario después de que cada uno de ellos realice su proceso de autenticación. Básicamente, hay dos parámetros relativos a la subasta y otros dos relativos a los algoritmos criptográficos. Los dos primeros parámetros son relativos a la subasta, mientras que los restantes son parámetros de seguridad:
  - Intervalo del Precio: Establecemos el límite inferior (T1) y superior (T2) así como la cantidad de incremento (S). Esta información es utilizada, además de en la subasta, para optimizar la entrada de la función de comparación, reduciendo los bits necesarios para su representación y optimizando el circuito de comparación. Por tanto, las entradas válidas quedan reducidas al intervalo definido entre (T2-T1)/S.
  - Duración Subasta: Determina la finalización del proceso de apuesta. Después de este punto no es posible realizar más apuestas y los protocolos de seguridad comienzan a transmitir la información relativa a la seguridad.
  - Alfa: Este parámetro tiene relación con las pruebas criptográficas y por ende con la seguridad del sistema. Cuanto más elevado sea el valor de Alfa más seguridad tendrá el sistema resultante pero por contra más tiempo de cómputo es necesario. Por ello, es necesario configurar el valor apropiado de Alfa basándonos en los recursos del sistema. A modo de ejemplo, un valor de Alfa igual a 20 significa que el sistema es seguro con una probabilidad de $1 - 2^{-20} \sim 99,99\%$.
  - Método Matriz: Si seleccionamos esta opción, se utilizará una matriz booleana para reducir las pruebas criptográficas. Una descripción más detallada del proceso de creación y verificación de pruebas discretas reducidas es realizada en la sección IV-C3.
- Apuestas: Una vez que han sido establecidos los parámetros de la subasta por parte del subastador, los usuarios deben pasar un proceso de autenticación. Para ello, se han desarrollado dos métodos, un método básico basado en el par (usuario, palabra de paso) y un método de autenticación avanzado haciendo uso de las claves criptográficas del usuario y del servicio de números aleatorios.

- Finalización del tiempo de subasta: Después de este momento ningún usuario puede realizar una apuesta y pasamos a las fases de determinación y verificación. Como mencionamos anteriormente es extremadamente importante la sincronización de los relojes de los integrantes del sistema, y de ahí la importancia del servicio de tiempo.
- Determinación del Ganador y del Precio: Consideramos que nuestro sistema es una subasta a sobre cerrado ya que las apuestas son enviadas de forma cifrada. Debido a que hemos seleccionado la subasta Vickrey, la segunda apuesta ganadora es la que establece el precio de la subasta por lo que necesitamos dos rondas para determinar el ganador y el precio de la subasta. El proceso de determinación es un proceso de muestreo donde el servidor realiza una consulta a todos los usuarios sobre los apuestas válidas y recibe una respuesta de cada uno de ellos de forma positiva o negativa. El proceso de muestreo comienza en el valor más elevado (T2) que fue establecido previamente en el proceso de configuración, hasta encontrar los valores ganadores o finalizar con el valor más pequeño (T1), decreciendo la cantidad en cada paso el valor configurado determinado como (S). En el caso que un usuario conteste de forma afirmativa, el postor debe revelar la apuesta, abriendo así el sobre electrónico. Por tanto, en este punto, el usuario ejecuta la fase de revelación del protocolo de compromiso de bit para probar que el valor enviado anteriormente era correcto. Obtendremos un ganador cuando el proceso de verificación del compromiso de bit sea válido, y en ese momento comenzará el proceso de determinación del precio de venta. En caso contrario, el postor ha mentido por lo que el proceso de determinación de un ganador continúa sin el postor que ha mentido. Si estamos en la situación de empate, la subasta Vickrey se convierte en una subasta normal donde el ganador es el postor que realizó primero la apuesta y su apuesta es el precio de venta.
- Publicación y Verificación de las Pruebas: Mientras que la apuesta del ganador y el precio de venta son revelados en el etapa anterior, las apuestas restantes nunca lo son. Para probar la veracidad de las apuestas de los restantes participantes deben publicar sus pruebas discretas. La definición, contenidos, así como los procesos de creación y verificación de las pruebas discretas, son ampliamente descritos en la sección IV-C. Básicamente, en esta fase, los postores deben publicar la información necesaria para reconstruir los circuitos de comparación y realizar la verificación de las puertas del circuito sin revelar la cantidad apostada.

IV. Aplicación práctica de Computación Segura Multiparte

El protocolo de los Millonarios de Yao [27] puede ser considerado como el punto de inicio de la Computación Segura Multiparte. Todos los desarrollos teóricos sobre CSM fueron realizados en la década de los ochenta y actualmente sigue siendo un campo activo aunque ha sido retomado de forma más práctica. Ejemplos de ello son el trabajo sobre el cual escribimos, así como los resultados obtenidos en los trabajos [3], [6]. Como hemos mencionado anteriormente, el principal objetivo de nuestra propuesta es que las apuestas no sean reveladas en ningún momento, haciéndose solamente pública las apuestas que obligatoriamente requiere el proceso de subasta, como son la ganadora y la apuesta que establece el precio de venta. Para llevar a cabo este requisito aplicamos los conceptos de CSM. La principal virtud de CSM es que permite a los usuarios realizar tareas computacionales de forma distribuida sobre su información sin revelarla. El diseño de CSM debe cumplir los requisitos de confidencialidad y correctitud incluso si existe un ataque de una entidad externa o por un conjunto de participantes.

La confidencialidad es obtenida mediante la utilización previa de un protocolo de compromiso de bit donde cada usuario realiza un cifrado de su apuesta bit a bit. Los bits cifrados son utilizados como la entrada del circuito de comparación que describiremos en la siguiente sección IV-A. La propiedad homomórfica del criptosistema elegido permite que los valores de entrada sean distribuidos por el circuito de comparación sin perder en ningún momento la confidencialidad. Por otro lado, las pruebas discretas definidas en la sección IV-C permitirán verificar la corrección de la función de comparación de cada postor.

A. Creación de un Circuito que muestra que un número es menor que otro dado

Supongamos que un postor *B* ha realizado una apuesta *X*, siendo un número positivo. La representación binaria de *X* utilizando *n* bits es $x_{n-1}2^{n-1} + ... + x_1 2^1 + x_0 2^0$, por tanto $(x_{n-1}, ..., x_1, x_0)$ es un vector donde $x_i \in \{0, 1\}$. Dado un número *S*, también en representación binaria $s_{n-1}2^{n-1} + ... + s_1 2^1 + s_0 2^0$, el postor quiere construir una función de comparación tal que $S \geq X$. Para resolver este problema, primero definiremos un circuito cuya salida es 1 sii $S \geq X$.

Siendo $A = 2^n + S - X$ y su representación binaria como $(a_n, a_{n-1}, ..., a_1, a_0)$. Entonces a_n es 1 sii $S \geq X$. Además, *A* puede ser $A = S + (2^n - 1 - X) + 1 = S + \bar{X} + 1$ donde $\bar{X}$ es el complemento a bit de *X*. Por ello, a_n es simplemente el bit de acarreo n^{th} cuando sumamos S, $\bar{X}$ y 1. La representación de *A* utilizando puertas booleanas AND ($\wedge$), XOR ($\oplus$), y NOT ($\neg$) es:

$$F(S => X) = C_k \text{ donde } C_k = (S_k \oplus C_{k-1}) \wedge (\neg\ X_k \oplus C_{k-1}) \oplus C_{k-1}) \text{ y } C_0 = 1$$

aunque existe una ecuación equivalente, que ha sido la escogida, ya que causa un mejor rendimiento.

$$F(S => X) = \neg\ C_k \text{ donde } C_k = (\neg\ S_k \oplus C_{k-1}) \wedge (X_k \oplus C_{k-1}) \oplus C_{k-1}) \text{ y } C_0 = 0$$

B. Generación y Verificación de los Retos

La función de comparación es la piedra angular de la seguridad de nuestra propuesta. Cada postor tendrá su propio circuito $(PCircuit)$ cuya misión es básicamente demostrar a los demás participantes que no ha mentido en su apuesta y, por otro lado, tendrá acceso a los circuitos $(VCircuit)$ de los demás postores para verificar su veracidad.

Los nodos en el $(PCircuit)$ tendrán sus valores binarios y sus correspondientes compromisos de bit (en la práctica pueden tomarse como valores cifrados), mientras que en el $(VCircuit)$ solamente conoceremos los valores cifrados de los nodos. Por consiguiente, un circuito de comparación tendrá una instancia como $(PCircuit)$ y tantas instancias $(VCircuit)$ como usuarios quieran probar la función de verificación, sin riesgo a revelar la información.

Cada postor debe proveer a los verificadores los valores cifrados de las puertas AND, que junto a las apuestas cifradas que se enviaron en la fase de apuesta, permiten completar los valores cifrados del circuito. A nadie escapa la posibilidad de que el postor mienta sobre los valores cifrados de las puertas AND, por lo que es necesario establecer un mecanismo para conocer si esos valores son válidos y, por ende, el circuito de comparación construido. El mecanismo creado es un par de desafíos que permiten verificar si el postor conoce el valor binario de la salida y las entradas de las puertas AND del circuito, basándose en la elección de tres números aleatorios (A, B, C) que deben cumplir las propiedades detalladas en ambos retos.

El reto 1 se centra en la demostración de la salida de la puerta AND utilizando su compromiso de bit (bO) que permite que no se revele su información binaria. El postor X debe ejecutar los siguientes pasos para generar el desafío 1 que será verificado por el usuario Y:

- (A, B, C) debe cumplir, sin seguir ningún orden específico, que dos de ellos $(E0_1, E0_2)$ deben ser equivalentes al compromiso de bit bO de la salida de la puerta AND que estamos procesando.
- X envía (A, B, C) a Y.
- X envía las raíces a Y $\sqrt{E0_1 \times b0\, mod N}$ y $\sqrt{E0_2 \times b0\, mod N}$ donde N es la clave publica de X.

El usuario Y debe por tanto realizar el siguiente proceso para verificar el reto 1:

- Y calcula $U = (\sqrt{E0_1 \times b0 mod\, N})^2$ y $V = (\sqrt{E0_2 \times b0 mod\, N})^2$
- Y elige un número (γ) en (A, B, C) y calcula $\delta = bO \times \gamma$. Si δ es igual a U o V realiza el siguiente paso. En caso contrario X ha mentido.
- Y elige otro número distinto (β) en (A, B, C) y calcula $\theta = bO \times \beta$. Si θ es igual a U o V X no ha mentido.

Haciendo uso del reto 1 cualquier usuario puede verificar si la salida de la puerta AND era correcta, pero existe la posibilidad que el postor mintiera sobre las entradas de la puerta AND, enviando previamente el compromiso de bit inverso. Para tal caso debemos definir un nuevo reto.

El reto 2 verifica si el postor no mintió en las entradas de la puerta AND, siguiendo una técnica similar a la realizada en el reto 1, pero utilizando los compromisos de bit de la entrada (bI_1,bI_2). De esta forma, para establecer el reto 2, el usuario X debe realizar los siguientes pasos:

- (A, B, C) debe cumplir, sin seguir ningún orden específico, que dos de ellos (EI_1, EI_2) serán equivalente al compromiso de bit de las entradas bI_1 y bI_2 de la puerta que estamos procesando.
- X envía (A, B, C) a Y.
- X envía las siguientes raíces a Y $\sqrt{EI_1 \times bI_1 mod\, N}$, $\sqrt{EI_2 \times bI_2 mod\, N}$ y $\sqrt{EZero}$ donde N es la clave pública de X.

Los pasos utilizados para verificar el reto 2 son básicamente similares a aquellos que utilizamos en el reto 1 con algunas modificaciones.

- Y calcula $U = (\sqrt{EI_1 \times bI_1 mod\, N})^2$ y $V = (\sqrt{EI_2 \times bI_2 mod\, N})^2$
- Y elige un número (γ) en (A, B, C) y calcula $\delta = bI_1 \times \gamma$. Si δ es igual a U o V iremos al siguiente paso. En otro caso, Y repite el proceso asignándole a γ alguno de los otros dos número en S. Si al menos uno de los casos es válido iremos al siguiente paso. Si no podemos realizar ninguna asignación el usuario X ha mentido sobre la entrada bI_1.
- Y elige otro número diferente del paso anterior (β) en (A, B, C) y calcula $\theta = bI_2 \times \beta$. Si θ es igual a U o V (uno de los valores que no ha sido seleccionado previamente), podemos concluir que las entradas son correctas. Si la asignación no puede realizarse entonces X ha mentido en la entrada bI_2.

C. Pruebas Discretas

Los trabajos [12], [4] establecen el concepto de *Pruebas Discretas*. Este tipo de pruebas es considerado como un tipo nuevo de pruebas de conocimiento cero debido a que no puede clasificarse en ninguna de las categorías anteriores. Esta afirmación está basada en la creación de un conjunto de certificación, que contiene un vector de compromisos de bit que codifica un vector de bits en un conjunto dado sin revelar el vector de bits. Es por ello que las pruebas discretas constituyen una herramienta perfecta para establecer las verificaciones de los circuitos de comparación establecidos anteriormente.

Es posible establecer tres modelos de pruebas, las cuáles serán especificadas en detalle en las siguientes secciones, incluyendo en cada caso sus ventajas y desventajas de cada propuesta y qué contexto es más apropiada su aplicación.

1) Pruebas Manuales: La primera de las opciones disponibles son las pruebas Manuales. Este tipo de prueba es recomendable realizarla si existe una representación visual del circuito de comparación, ya que el usuario que realiza las comprobaciones debe interactuar con la información como veremos a continuación.

Las ventajas de este método es que el usuario que está realizando la verificación define la seguridad del sistema ya que la prueba puede ser ejecutada cuantas veces desee. Como inconveniente principal, además de la necesidad de

implementar un interfaz visual, este método requiere que los postores o un agente que lo represente este siempre online.

La figura 1 es una representación visual del protocolo que es necesario realizar para llevar a cabo las pruebas manuales. En la figura podemos observar que el verificador lanza el protocolo de verificación cuando selecciona una puerta AND del circuito. Básicamente, se basa en la ejecución de los retos 1 o 2 definidos anteriormente, según la elección del usuario.

Cada solicitud tiene asignada un identificador de sesión para evitar los deadlocks del protocolo ya que debemos recordar que es posible que cada usuario pueda actuar en distintos roles en el protocolo o incluso que varios usuarios verifiquen un mismo circuito a vez.

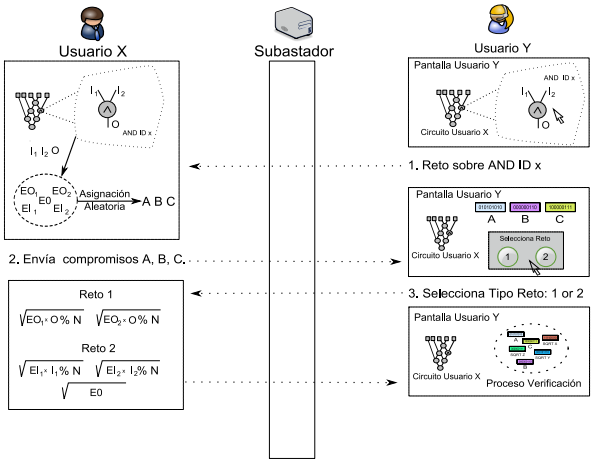


Fig. 1. Secuencia de mensajes generados en las pruebas manuales

La estimación de los mensajes intercambiados que son necesarios para probar la veracidad del circuito pueden ser calculados utilizando la siguiente ecuación:

$$mensaje = N\_user \times 4 \times ANDs\_circuit$$

donde N_user es el número de postores en la subasta, $ANDs\_circuit$ es el número de puertas AND del circuito de comparación y cuatro mensajes son los necesarios para completar cada prueba. Esta fórmula sólo tiene en cuenta la ejecución de un reto, por lo que sería el doble de mensajes si el verificador decide ejecutar ambos retos.

2) Pruebas No Interactivas: Las pruebas manuales hacen posible que el usuario establezca la seguridad del sistema, por tanto el nivel de confianza es administrado por el usuario a su merced. Aunque esta propiedad es la deseada por cualquier sistema de seguridad, su ejecución produce una considerable cantidad de mensajes en la red y además requiere que todos los participantes estén conectados para interactuar en los retos.

La pruebas No Interactivas han sido diseñadas con el objetivo de eliminar la dependencia en la interacción con los postores. Esta decisión implica que las pruebas tengan que ser automatizadas y por ello es necesario simular el comportamiento aleatorio del verificador. La solución viene por utilizar el servidor de aleatoriedad como fuente confiable de números aleatorios para simular que el usuario selecciona un reto especifico. Además, el proceso de automatización implica que el usuario no debe seleccionar cuántas veces el reto será aplicado a cada puerta AND, por lo que depende del parámetro Alfa (α) definido durante la fase de configuración.

El sistema será probablemente seguro con una probabilidad equivalente a $1 - 2^{-\alpha}$, por lo que grandes valores α darán lugar a un sistema más seguro, mientras el proceso de creación y verificación de las pruebas consumirá más tiempo de computación y por ende las pruebas tendrán un tamaño mayor. Teniendo en cuenta esta situación es necesario estimar su valor apropiado, ya que tendremos que tener en cuenta la capacidad de cómputo del dispositivo utilizado.

La figura 2 es un esbozo del proceso de creación de las pruebas interactivas. A grandes rasgos, el algoritmo para crear las pruebas no interactivas es el procesado de todas las puertas AND del circuito α veces y seleccionaremos de forma aleatoria el reto a aplicar en cada ocasión.

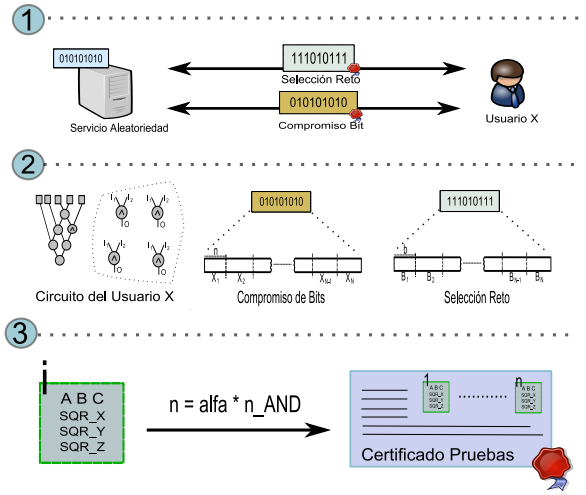


Fig. 2. Proceso de creación de pruebas no interactivas

3) Pruebas No Interactivas Reducidas: La complejidad de las pruebas no interactivas dependen directamente del número de puertas AND del circuito y del valor del parámetro de seguridad α. Introduciendo una pequeña modificación en las pruebas no interactivas la complejidad computacional y la carga en las comunicaciones puede ser reducida y además eliminar la dependencia con el tamaño del circuito. La solución pasa por la utilización de una matriz aleatoria de valores binarios para reducir el número de compromisos de bits generados. La figura 3 muestra un esquema del proceso de creación de las pruebas discretas no interactivas reducidas.

Inicialmente el objetivo de este método era reducir drásticamente la longitud de las pruebas criptográficas, pero su implementación nos constató el hecho que los procesos de creación y verificación reducidos consumen menos cómputo que el caso de las pruebas no reducidas. Esta situación se debe a que el tiempo consumido por la multiplicación de la matriz y el vector de retos es incluso menor que la ejecución de una raíz cuadrada.

V. Detalles de Implementación

El sistema de subasta descrito en el trabajo ha sido implementado utilizando la tecnología Java. La figura 4 muestra una captura de la aplicación. La selección de Java es justificada ya que hace posible un rápido desarrollo del prototipo, es un lenguaje multi-plataforma y posee una implementación eficiente de números grandes, requisito

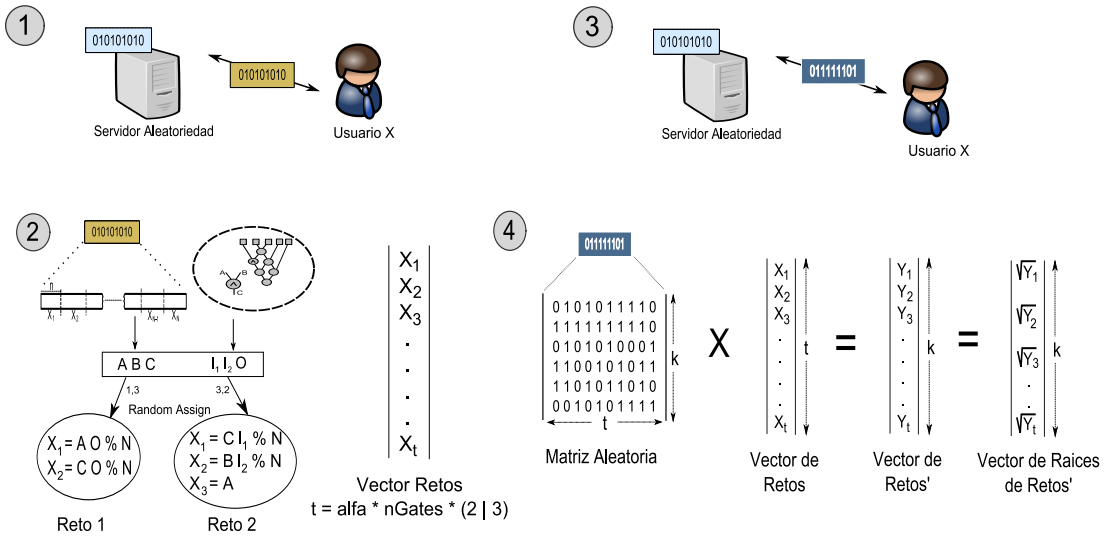


Fig. 3. Proceso de creación de pruebas no interactivas reducidas

necesario para el establecimiento de los protocolos y primitivas criptográficas.

El desarrollo del sistema cuenta además con la utilización de librerías de código abierto como es el caso de: *Derby* para añadir soporte de base de datos SQL; *iText* es utilizado para almacenar la información criptográfica en un documento con formato portable como es el caso de PDF; *jGraph* es una librería gráfica que hace posible la descripción visual de la función de comparación, así como permitir la ejecución de las pruebas manuales (sección IV-C1) y *Barcode4J* utilizada para representar grandes números en forma de matriz visual, así como facilitar la tarea de comparar dos grandes números.

El principal objetivo de la fase de desarrollo era cumplir con unos requisitos computacionales aceptables y un ancho de banda bajo. Después de un estudio detallado de los requisitos del sistema, determinamos que la carga del sistema está principalmente basada en los procesos de creación y verificación de pruebas. Más concretamente, podemos determinar que el proceso de creación es 13.52 veces más costoso computacionalmente que el proceso de verificación.

A modo de ejemplo nos centramos en una de las funciones más utilizadas en el sistema, que resulta ser el cálculo del número de Jacobi. Por desgracia, Java no incluye una implementación propia del número de Jacobi, por lo que ha sido necesaria su implementación teniendo en consideración un uso intensivo y la necesidad de que la aplicación cumpla con un rendimiento de tiempo real. Para su elaboración fue necesario comparar las distintas implementaciones existentes en la literatura. El trabajo [8] selecciona y compara los tres algoritmos más eficientes para calcular el número de Jacobi: Williams [26], Lesbegue [16] y Modified Binary [23]. Tenemos que remarcar que las implementaciones realizadas en el trabajo original no eran realizadas en Java, sino en la tecnología accesible en la época que el trabajo fue realizado, por lo que aunque en el trabajo se consideraba que el método *Modified Binary* era el más eficiente, la posterior implementación en Java de los tres algoritmos y la comparación de tiempos, mostró que la propuesta de *Williams* era la solución más eficiente para su implementación en Java.

Anteriormente hemos constatado el hecho de que el proceso de creación de pruebas depende del número de puertas *AND* en el circuito de comparación y del parámetro de seguridad *Alfa*. La figura 5 muestra los valores obtenidos en un test de rendimiento utilizando un circuito con 20 puertas, una clave de 1024 bits y diferentes valores de α entre el intervalo de 1 y 100. El mismo test ha sido realizado con una clave de 2048 bits y el tiempo computacional es incrementado *6.858* veces con respecto a la utilización de claves de 1024 bits. Como conclusión del test de rendimiento un incremento de la seguridad utilizando una clave de doble longitud, produce un sistema siete veces más lento.

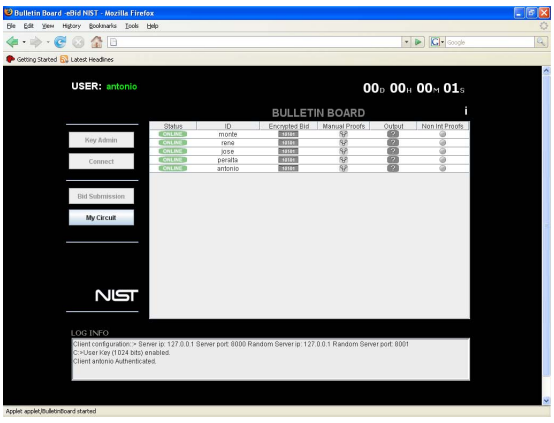


Fig. 4. Captura de pantalla de la aplicación del postor

Por otro lado, si optamos por utilizar las pruebas no interactivas reducidas, el tiempo de computación se reduce considerablemente. Concretamente, en la situación que requiere más computo en nuestro test (α = 100, puertas AND = 20), el método de pruebas no interactiva tarda aproximadamente unos 153,675 milisegundos, mientras que el método reducido sólo necesita unos 38,954 milisegundos, por lo que la utilización de la matriz consigue una reducción del tiempo de computo en casi cuatro veces.

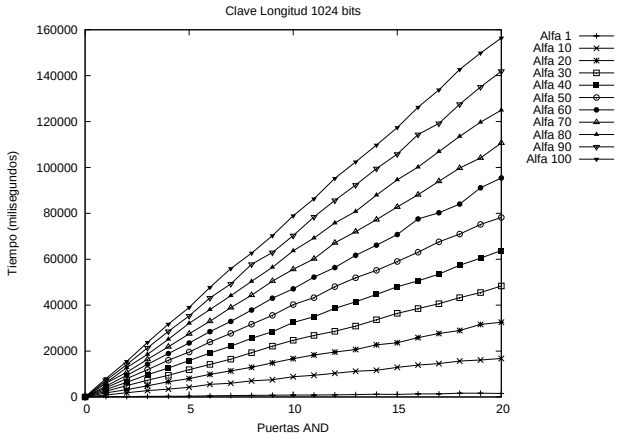


Fig. 5. Tiempo de procesamiento de las pruebas con una clave 1024 bit

VI. Conclusiones

El principal objetivo de esta investigación ha sido el desarrollo de un sistema de computación multiparte que cumpla con requisitos técnicos realistas, debido a que los sistemas de computación multiparte que existen en la literatura, desde la definición inicial de Yao, son soluciones difíciles de llevar a la práctica. Como banco de pruebas de nuestra propuesta nos hemos centrado en el diseño e implementación de una subasta electrónica a sobre cerrado, concretamente la denominada *sealed-bid Vickrey*.

Además, la inclusión de las pruebas criptográficas discretas permite verificar la veracidad de las apuestas de forma cifrada sin revelar su valor. La propiedad de discreta permite que la apuesta ganadora y el precio de venta puedan ser procesados sin que las apuestas perdedoras sean hechas públicas (incluso por el subastador). Los principales objetivos de la propuesta han sido utilizar la menor cantidad de recursos, que por su naturaleza son escasos, como tiempo de computación, ancho de banda de comunicación, número de bits comunicados, utilización de memoria, aleatoriedad e interacción (los protocolos con muchas rondas de comunicación son menos prácticos que aquellos que realizan pocas rondas).

Los tests realizados al sistema desarrollado muestran que las pruebas discretas son realmente prácticas y debido a la generalidad que prestan dicho método, nuestra investigación abre las vías a un gran número de aplicaciones sobre Internet en el terreno del *e-commerce* y *e-goverment* (elecciones, administración segura de informes médicos distribuidos, etc.).

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Educación a través de la concesión de una beca postdoctoral Fulbright (FU-2006-1527) al primer autor en Computer Security Division de National Institute of Standards and Technology y por el proyecto de investigación ARES (CSD2007-0004) del Ministerio de Ciencia e Innovación.

Referencias

[1] M. Szydlo A. Juels. A two-server, sealed-bid auction protocol. In *Financial Cryptography 2002*, pages 72–86, June 2002.

[2] M. Abe and K. Suzuki. M+1st price auction using homomorphic encryption. In *5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC*, volume 2274, pages 115–124, February 2002.

[3] P. Bogetoft, D. Christensen, I. Damgard, M. Geisler, T. Jakobsen, M. Krigaard, J. Nielsen, J. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, and T. Toft. Multiparty computation goes live. 2008.

[4] J. Boyar and R. Peralta. Short discrete proofs. In *EUROCRYPT*, pages 131–142, August 1996.

[5] I. Damgard and R. Thorbek. Non-interactive proofs for integer multiplication. In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515, pages 412–429, May 2007.

[6] I. Damgard and T. Toft. Trading sugar beet quotas - secure multiparty computation in practice. *Ercim News*, 73:32–33, 2008.

[7] D. Eastlake, S. Crocker, and J. Schiller. *Randomness Recommendations for Security*. IETF Network Working Group, request for comments: 4086 edition, June 2005.

[8] S. M. Eikenberry and J. P. Sorenson. Efficient algorithms for computing the jacobi symbol. *Source Journal of Symbolic Computation*, 26(1):509 – 523, 1998.

[9] M. Franklin and M. Reiter. The design and implementation of a secure auction service. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 302–312, May 1995.

[10] R. Gennaro. Randomness in cryptography. *IEEE Security & Privacy*, 4(2):64 – 67, March 2006.

[11] I. Goldberg and D. Wagner. Randomness and the netscape browser. *Dr. Dobb's Journal*, pages 66–70, January 1996.

[12] I. Damgard J. Boyar and R. Peralta. Short non-interactive cryptographic proofs. *Journal of Cryptology*, 138(4):449–472, 2000.

[13] D. Wagner J. Kelsey, B. Schneier and C. Hall. Cryptanalytic attacks on pseudorandom number generators. In *Fifth International Fast Software Encryption*, pages 168–188, March 1998.

[14] A. Juels and M. Szydlo. A two-server sealed-bid auction protocol. In *Financial Cryptography*, volume 2357, pages 72–86, March 2002.

[15] M. Kumar and S. Feldman. Internet auctions. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, pages 49–60, September 1998.

[16] V.A. Lebesgue. Sur le symbole (a/b) et quelques unes de ses applications. *J. Math. Pures Appl*, 12(1):497–517, 1847.

[17] B. Pinkas M. Naor and R. Summer. Privacy preserving auctions and mechanism design. In *1st ACM Conference on Electronic Commerce*, pages 129–139, November 1999.

[18] D. Mills. *Network Time Protocol (Version 3) Specification, Implementation and Analysis*. IETF Network Working Group, request for comments: 1305 edition, May 1992.

[19] K. Omote and A. Miyaji. A second-price sealed-bid auction with public verifiability. *Transactions of Information Processing Society of Japan*, 43(8):2405–2413, 2002.

[20] J. Postel. *Daytime Protocol*. IETF Network Working Group, request for comments: 867 edition, May 1983.

[21] J. Postel and K. Harrenstien. *Time Protocol*. IETF Network Working Group, request for comments: 868 edition, May 1983.

[22] A. Rukhin and et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Computer Security Division, NIST, special publication 800-22 edition, May 2001.

[23] J. Shallit and J. Sorenson. A binary algorithm for the jacobi symbol. *SIGSAM Bulletin*, 27(1):4 – 11, 1993.

[24] W. Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of Finance*, 16(1):8 – 37, 1961.

[25] M. Wellman and P. Wurman. Real time issues for internet auctions. In *1st IEEE Workshop on Dependable and Real Time E-commerce System (DARE)*, pages 54–56, June 1998.

[26] H. Williams. A modification of the rsa public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6):726 – 729, 1980.

[27] A. Yao. Protocols for secure computations. In *Symposium on Foundations of Computer Science*, pages 160–164, November 1982.

AUTOMATIZACIÓN DE LA CAPTURA DE EVIDENCIAS DIGITALES VOLÁTILES

Virginia Aguilar, Victor Villagrá
Dpto. de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid, E.T.S.I. de Telecomunicación
Av. Complutense, s/n, E-28040 Madrid, Spain.
aguilar.virginia@gmail.com, villagra@dit.upm.es

***Resumen*- Los delitos informáticos se han vuelto más frecuentes y sofisticados con la generalización en el uso de sistemas informáticos. Por ello, se recomienda que las compañías u organizaciones creen y mantengan procedimientos para llevar a cabo tareas de análisis forense que, entre otros objetivos, eviten la pérdida de información, estén estandarizados y cumplan con las necesidades de cadena de custodia. El objetivo de este artículo es describir una solución que, considerando estos requisitos, automatice los procedimientos de obtención de las evidencias digitales volátiles.**

Palabras Clave- evidencia digital, sistemas automáticos de respuesta ante incidentes, obtención de evidencias digitales, adquisición de evidencias digitales.

I. INTRODUCCIÓN

Un delito informático es todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes [1]. Sin embargo, las categorías que definen un delito informático pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales se han empleado ordenadores y redes [2], [3].

Este tipo de delitos se ha vuelto más frecuente y sofisticado [4] con la generalización en el uso de sistemas informáticos, por lo que han aumentado considerablemente los casos en los que es necesario recurrir a la informática forense para tratar de esclarecer incidentes acaecidos tanto en compañías, organismos públicos o usuarios particulares.

Por ello, se recomienda que las compañías u organizaciones creen y mantengan procedimientos para llevar a cabo tareas de análisis forense que estén basadas en las políticas de la organización [5].

En estos procedimientos, se deben contemplar procedimientos específicos para la captura de evidencias relevantes para la investigación. El primer tipo de información que se debe recopilar es la información volátil, como por ejemplo, la memoria del sistema, las conexiones establecidas o los usuarios conectados [6].

Sin embargo, destruir evidencias es muy fácil, en algunas situaciones incluso se alteran o se pierden datos de manera inadvertida. Una de las recomendaciones para evitar esta destrucción o alteración intencionada o no es automatizar en la medida de lo posible los procedimientos de captura de información [7].

Siguiendo esta línea, la propuesta que presentamos en este artículo es un método automatizado para la captura de datos o evidencias volátiles. Entre otros, la automatización nos va a permitir:

- **Evitar la pérdida de información relevante**, disminuyendo el tiempo de respuesta y realizando la obtención de evidencias mediante las herramientas y procedimientos adecuados que minimicen la alteración de las evidencias.
- **Estandarizar los procedimientos de obtención de evidencias**, definiendo qué tipos de evidencias se deben recopilar según el tipo de incidente detectado y minimizando el número de evidencias no relevantes recogidas.
- **Facilitar los mecanismos de cadena de custodia que verifiquen la integridad de las evidencias**, permitiendo auditar los pasos seguidos en la obtención de las evidencias, que incluirán el cálculo del hash de las evidencias recogidas.

En los siguientes apartados de este articulo, describiremos los conceptos claves del análisis forense y de la metodología que hemos considerado para el diseño de la solución presentada; a continuación, haremos un breve repaso de algunas líneas de investigación en este ámbito; finalmente, detallaremos el método automatizado de captura de evidencias propuesto.

II. ASPECTOS CLAVE DE ANÁLISIS FORENSE

En este apartado definiremos qué son las evidencias digitales y sus características principales para, a continuación, describir una metodología forense adecuada para su obtención y análisis.

A. Definición de Evidencia Digital

La definición que el Standard Working Group on Digital Evidence, define evidencia digital como cualquier información probatoria almacenada o transmitida en formato digital [8].

Las evidencias digitales pueden convertirse en un reto para los analistas forenses debido a algunas de sus características:

- Dificultad en el manejo de la evidencia, que puede tratarse simplemente de cadenas de caracteres, de donde hay que extraer y convertir información que sea entendible.
- Son abstracciones de un evento u objeto digital.
- Pueden ser manipuladas, de manera consciente o inconsciente, con facilidad.
- Es circunstancial, por lo que es complicado atribuir una actividad de un ordenador a un individuo en concreto.

Por otro lado, las evidencias digitales pueden ser volátiles o no en función del tipo de evidencia y su persistencia [9]. Por ejemplo, un fichero almacenado en un disco duro sólo se destruirá en caso de ser borrado y sobrescrito; mientras que la memoria RAM se modifica en cualquier operación realizada sobre el sistema operativo y se pierde totalmente al reiniciar el equipo.

En este caso, nos centraremos en las evidencias digitales volátiles cuyo soporte no es un dispositivo de almacenamiento persistente y que, por lo tanto, son más sensibles a los procedimientos de análisis forense empleados.

B. Metodología de Análisis Forense

Las evidencias digitales requieren de una metodología detallada y adecuada para su gestión y análisis que permita transformar los bits contenidos en un soporte informático en evidencias que puedan ser utilizadas en un procedimiento judicial. Una de las metodologías, propuesta por el NIST [5], establece cuatro fases básicas del procedimiento de análisis forense:

- **Obtener**. En esta etapa, los datos relacionados con un evento específico son identificados, etiquetados, registrados y, finalmente, recopilados mediante técnicas forenses (hardware o software) preservando en todo momento su integridad.
- **Examinar**. Se emplean las técnicas y herramientas forenses apropiadas en cada caso para identificar y extraer la información relevante que se haya recogido inicialmente, preservando la integridad en todo el proceso.
- **Analizar**. Mediante el análisis de los resultados obtenidos será posible derivar información útil que de respuesta a las cuestiones que iniciaron el proceso.
- **Presentar**. El informe final debe contener las acciones llevadas a cabo, siguientes pasos y recomendaciones de mejora en políticas, procedimientos, herramientas y cualquier otro aspecto del proceso de análisis forense.

Debido a que nuestro trabajo está centrado en proporcionar una mejora en el momento de la obtención de las evidencias, describiremos en mayor detalle la primera fase de la metodología. Esta fase de obtención de datos consta de dos acciones principales:

2.B.1) Identificar posibles fuentes de información

El amplio uso de la tecnología digital en el entorno profesional y personal conlleva que el número de fuentes de información posible sea muy elevado. Las fuentes de información más comunes son ordenadores de sobremesa o portátiles, teléfonos móviles, servidores, dispositivos de almacenamiento de red o dispositivos de almacenamiento externo.

Además de estas evidencias, pueden resultar de gran interés otros tipos de evidencias como la actividad de red o de uso de aplicaciones; e incluso evidencias de terceras partes (ISP).

Asimismo, las organizaciones pueden tomar medidas proactivas para recopilar datos que podrían ser muy útiles ante un eventual incidente de seguridad que requiera el uso de análisis forense. En este sentido, por ejemplo, es posible configurar un sistema operativo para que registre eventos como intentos de autenticación o modificaciones en la política de seguridad; o se pueden establecer mecanismos de monitorización de controlen la instalación o desinstalación de aplicaciones.

Otra medida que puede aportar un elevado beneficio es implementar un sistema de registro de logs o de correlación de eventos centralizado para garantizar que un atacante no puede modificar información importante para un análisis y, además, permite identificar el mismo evento en diferentes dispositivos de seguridad de la compañía.

2.B.2) Realizar la imagen (adquisición u obtención) de la evidencia

En esta fase, se lleva a cabo el duplicado de la evidencia original. Para ello, es recomendable considerar los siguientes aspectos:

- **Planificar el proceso de adquisición**. Debido a que, habitualmente, existen varias fuentes de información que pueden resultar de utilidad, debemos priorizar aquellas que consideramos más relevantes y establecer un orden de copiado. Este orden de copiado debe tener en cuenta el valor de la evidencia, su volatilidad y el esfuerzo de adquisición.
- **Adquisición o imagen de la evidencia**. En esta fase incluimos el uso de herramientas forenses para obtener la información volátil y no volátil. Existen numerosos métodos tanto hardware como software para llevar a cabo este duplicado, que puede ser (i) bit a bit o (ii) un copiado lógico.
- **Verificar la integridad de la evidencia**. Es particularmente importante para un analista forense poder demostrar la integridad de una evidencia en todo momento para garantizar, de este modo, que ésta no ha sido modificada desde su adquisición.

Una vez definido qué es una evidencia digital, las dificultades que presenta y qué pasos deben seguirse para su obtención, en el siguiente apartado analizaremos algunas alternativas y líneas de investigación existentes actualmente para la adquisición automatizada de evidencias digitales, centrándonos fundamentalmente en aquellas soluciones planteadas para las evidencias digitales volátiles.

III. SOLUCIONES PARA LA OBTENCIÓN DE EVIDENCIAS DIGITALES VOLÁTILES

Además de herramientas *Open Source* y comerciales, diversas universidades han presentado estudios con planteamientos o herramientas que optimizan la obtención de evidencias digitales volátiles. En los siguientes apartados, haremos un breve resumen de algunas de las líneas que se están siguiendo en la actualidad.

A. Captura de evidencias integrada con herramientas de monitorización

Existen herramientas de monitorización que permiten la captura de evidencias, como los sistemas de detección de intrusos.

Una de estas herramientas es *Snort*, sistema de prevención y detección de intrusiones que ha sido desarrollado por Marty Roesch. *Snort* combina los beneficios de la monitorización basada en firmas, protocolos y anomalías y se ha convertido en la tecnología IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) más desplegada a nivel mundial, siendo considerado un estándar de facto [10].

La característica más apreciada de *Snort*, además de su funcionalidad, es su subsistema flexible de firmas de ataques. En este contexto, una firma es una secuencia de datos que identifican un ataque en una red, habitualmente aprovechando una vulnerabilidad de un sistema operativo o de una aplicación. *Snort* tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear firmas basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de *Snort*.

Asimismo, *Snort* cuenta con un módulo denominado *log Tcpdump* que permite registrar tráfico en caso de que se cumpla con un determinado patrón [11]. Esta funcionalidad se útil para un análisis forense posterior y es posible analizar la captura con cualquier visor de tráfico que sea compatible con el formato de captura de Tcpdump. El único parámetro que recibe este módulo es el nombre del fichero en el que se almacenará el tráfico, nombre al que se le añade un sello de tiempo.

Por lo tanto, *Snort* puede recopilar evidencias de tráfico de red del segmento en el que se encuentre. Sin embargo, no cuenta con mecanismos integrados para la obtenención de otros tipos de evidencias digitales volátiles en equipos remotos o para gestionar las evidencias obtenidas verificando su integridad.

B. Captura de evidencias digitales volátiles: Tráfico de red

El tráfico de red es uno de los tipos de evidencias digitales volátiles que podemos necesitar en el transcurso de una investigación y existen cuatro tipos de evidencias relacionadas: tráfico, datos de sesión, datos de alertas y datos estadísticos [12].

Recoger y almacenar de manera proactiva todo el tráfico de red de una compañía, para, posteriormente, analizarlo en el transcurso de una investigación es un reto que a menudo queda fuera de compañías y organizaciones.

Debido a la gran importancia de este tipo de evidencias, que son una de las principales y más completas fuentes de información, se plantean diferentes alternativas, tanto harware como sofware, para su recopilación.

Dos ejemplos de este tipo de soluciones son las planteadas por Bruce J. Nikkel y Asha Nagesh, respectivamente.

Bruce J. Nikkel diseña un dispostivo hardware denominado PN-FEC [13] para la recopilación optimizada del tráfico de red de manera *on-line* en modo promiscuo. Basado en OpenBSD, este dispositivo dispone, entre otras, de herramientas de acceso seguro, captura de paquetes (tcpdump), cifrado, algoritmos de hash para la preservación de evidencias y borrado seguro.

La principal desventaja de este dispositivo es que puede perder paquetes en redes con una carga muy elevada. En concreto, en redes a 100Mbps ya es necesario optimizar su configuración para reducir este riesgo. Además, es necesario disponer de un dispositivo por cada segmento de red independiente para que pueda capturar todo el tráfico.

Por otro lado, Asha Nagesh creó una solución de agentes móviles basada en JADE para la captura de tráfico de red [14]. Este sistema está diseñado para utilizar un servidor que actúe de *sniffer* mediante herramientas como, por ejemplo, Tcpdump.

Los agentes de esta solución distribuida, se mueven entre los sistemas para recopilar de manera selectiva registros de tráfico de red, examinarlos y mostrar los resultados en una interfaz de usuario.

El encargado de iniciar una captura de tráfico de red será un usuario que indicará la información exacta que considere que va a necesitar para la investigación de un incidente.

C. Herramientas comerciales de análisis forense

Una de las herramientas comerciales empleadas en el análisis forense de sistemas informáticos es Encase Enterprise Edition, herramienta desarrollada por Guidance Software.

Encase Enterprise Edition permite visibilidad de la red, respuesta inmediata y capacidad de realizar procedimientos de análisis forense de servidores y equipos en cualquier punto de la red [15].

Uno de los componentes de Encase Enterprise Edition es el denominado Snapshot, que está orientado a la respuesta de incidentes, y que permite la captura de evidencias digitales volátiles de manera automática mediante el módulo Automated Incident Response System (AIRS) de Guidance Software.

Las evidencias digitales volátiles que puede recopilar este sistema, verificando en todo momento la integridad de las mismas, son: puertos abiertos, procesos activos, registro de windows, servicios, información de sockets TCP, usuarios registrados o que han accedido a la máquina. Asimismo, se pueden añadir módulos para recuperar drivers de dispositivos, ficheros abiertos o información de las tarjetas de red.

Esta solución, que recopila información de manera distribuida, es un sistema con una funcionalidad muy completa para la obtención, gestión y análisis de todo tipo de evidencias digitales. Sin embargo, no está preparada para obtener todo el tráfico de red y almacenarlo como una evidencia.

D. Consideraciones sobre las soluciones presentadas

Las soluciones presentadas anteriormente presentan diversas desventajas que trataremos de solventar con nuestra alternativa. En concreto, *Snort* no cuenta con mecanismos integrados para la obtención de evidencias digitales volátiles en equipos remotos y su ubicación en la red puede ser determinante a la hora de recopilar tráfico de red.

Por otro lado, PN-FEC guarda todo el tráfico de red que pasa por un segmento, por lo que puede perder información en momentos de carga elevada, almacena una cantidad masiva de información y su efectividad depende en cierto

modo del lugar en el que sea ubicado. Además, no permite obtener otro tipo de evidencias digitales volátiles.

La solución basada en agentes móviles solventa el problema del rendimiento puesto que distribuye la carga entre los diferentes servidores, sin embargo, dependen de un usuario que inicie la captura de red y sólo obtiene este tipo de evidencias.

Finalmente, Encase Enterprise tiene un buen rendimiento, es compatible con la mayoría de los tipos de evidencias digitales volátiles pero no es capaz de capturar todo el tráfico de red que pase por un segmento de red.

IV. CAPTURADOR OPTIMIZADO DE EVIDENCIAS (COE)

Partiendo de las ideas adquiridas de las soluciones o líneas de investigación descritas en el apartado anterior, hemos diseñado el Capturador Optimizado de Evidencias (en adelante, COE). Esta solución distribuida, que como veremos posteriormente emplea herramientas existentes en el mercado para la obtención de evidencias digitales volátiles, es actualmente compatible con entornos de Microsoft Windows, incluyendo el tráfico de red entre los tipos de evidencias que puede recopilar .

En este apartado describiremos qué es COE, su arquitectura, beneficios principales y los resultados obtenidos en un entorno de pruebas.

A. *Descripción de COE*

El Capturador Optimizado de Evidencias es una aplicación cliente/servidor desarrollada en Perl que, en función del incidente ocurrido y de manera automática, obtiene las evidencias necesarias que se almacenan de manera centralizada controlando su integridad mediante un algoritmo de hash (MD5).

COE no detecta que un incidente de seguridad se está produciendo, por lo que debe ser invocado por un sistema externo de monitorización como por ejemplo un IDS o un antivirus, pasándole como parámetro el tipo de incidente que está siendo detectado.

En función del incidente indicado, COE obtiene las evidencias digitales volátiles que se han considerado relevantes para ese tipo en concreto y que han sido previamente definidas en un fichero de configuración de la propia herramienta. En este fichero se enumeran las evidencias necesarias en cada caso, ordenadas siguiendo un estándar como el definido en [7]. Como hemos mencionado anteriormente, la captura se realiza con herramientas ya existentes en el mercado como Wireshark, FPort o diferentes utilidades de PsTools [16][17][18].

COE almacena las evidencias obtenidas de manera temporal en el cliente utilizando, para evitar la sobreescritura de información en el disco local, un disco duro externo que debe estar permanentemente conectado al sistema informático que tenga instalado COE y, una vez enviadas al servidor, se eliminan.

Una alternativa a este diseño sería disponer de un espacio remoto de almacenamiento, pero podría saturar la red al volcar evidencias de gran tamaño y, además, una caída de red impediría la recuperación de la evidencia.

Como hemos visto, el servidor necesita mucho espacio de almacenamiento permanente puesto que recopila todas las evidencias recibidas de los clientes de COE, por lo que se recomienda disponer de una cabina de discos externa preferiblemente configurada en RAID-5, para recuperar información ante un fallo físico de un disco. En el servidor también se guarda un fichero con todos los hashes de las evidencias almacenadas y el path exacto en el que se encuentran.

Los tipos de evidencias que COE puede obtener son tráfico de red, volcado de memoria, fecha y hora del sistema, procesos en ejecución, puertos abiertos, conexiones establecidas, tablas de NetBios en caché, usuarios conectados, tabla interna de encaminamiento, servicios ejecutándose en el sistema, trabajos planificados y ficheros abiertos.

En la Fig. 1 se muestra un ejemplo de instalación de COE en un entorno de red sencillo y se detallan los pasos seguidos para la obtención y preservación de evidencia.

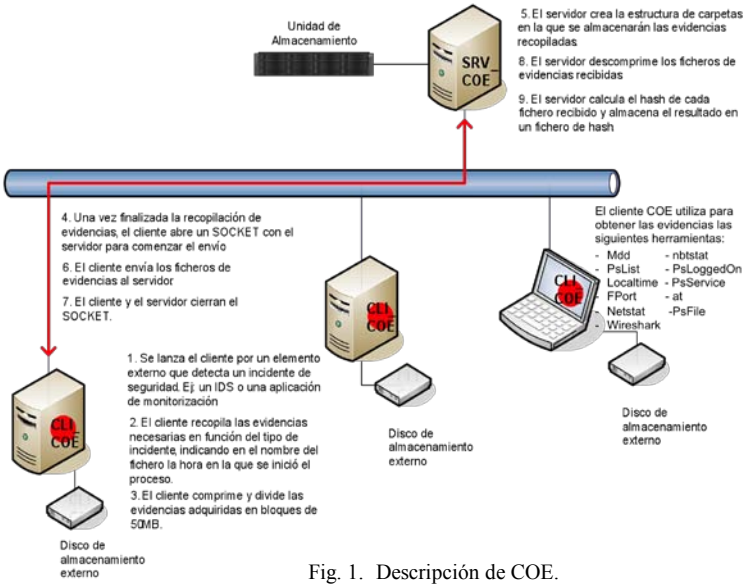


Fig. 1. Descripción de COE.

B. *Arquitectura de COE*

La funcionalidad principal del cliente de COE es recopilar las evidencias digitales altamente volátiles que sean necesarias, mientras que el servidor de COE se encarga del almacenamiento centralizado de dichas evidencias, controlando su integridad.

En la Fig. 2, mostramos un diagrama de secuencia en el que se describe la interacción entre los diferentes elementos que conforman el sistema propuesto.

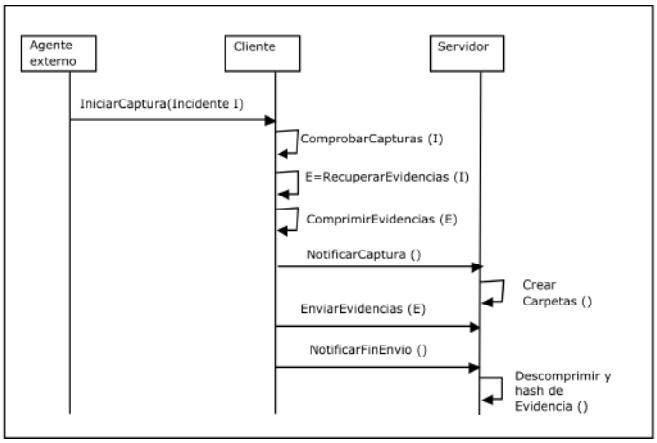


Fig. 2. Diagrama de secuencia de COE.

Por otro lado, en las Fig. 3 y 4 mostramos los flujogramas que detallan el funcionamiento del servidor y del cliente de COE, respectivamente.

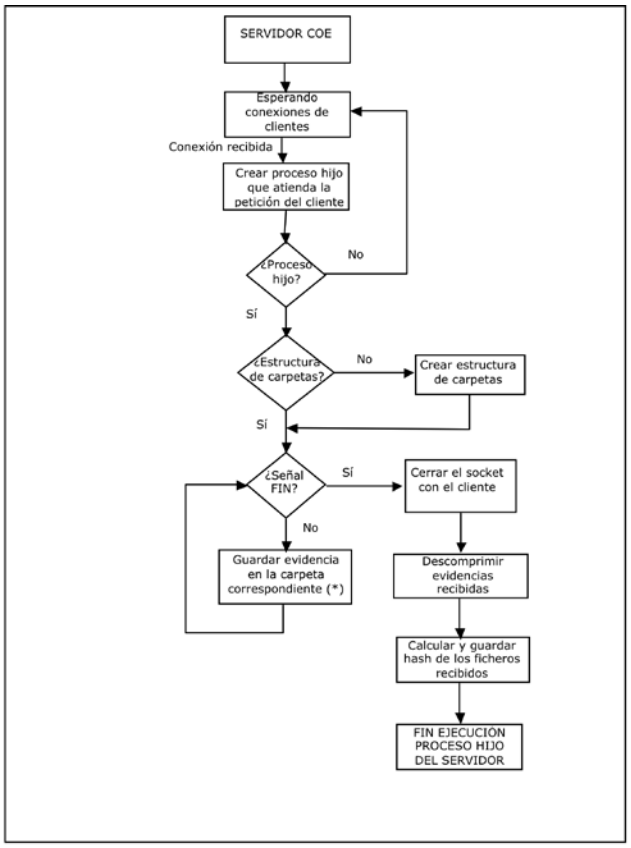


Fig. 3. Flujograma del servidor de COE.

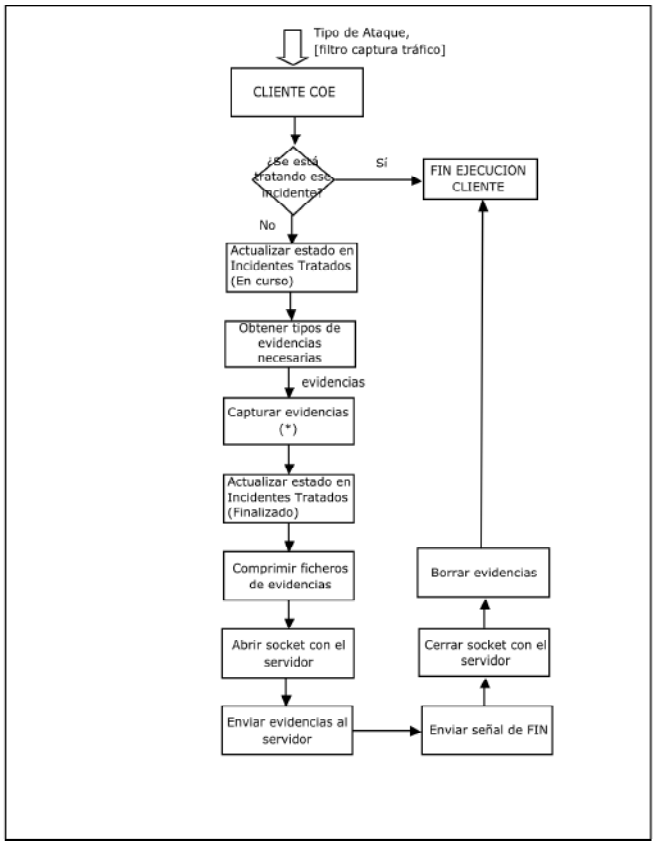


Fig. 4. Flujograma del cliente de COE

C. *Beneficios de COE*

Las principales ventajas del diseño de COE son las que se enumeran a continuación:

- **Reducción del tiempo de respuesta**, puesto que es invocado automáticamente por programas externos de monitorización. De este modo, se mitiga el riesgo de pérdida o alteración de evidencias relevantes.
- **Mejora en el rendimiento** mediante un diseño cliente/servidor que hace que la adquisición de evidencias se realice de manera distribuida. Asimismo, las evidencias capturadas se comprimen antes de su envío al servidor, minimizando así el tiempo de transmisión de información y reduciendo la carga de tráfico en la red.
- **Reducción de la cantidad de información a capturar**. Se recogen únicamente aquellas evidencias que se consideren relevantes para el análisis del incidente que, en concreto, se ha detectado. Así se consigue un ahorro de tiempo de captura, envío y procesamiento; así como de espacio de almacenamiento de las evidencias.
- **Mejora en la obtención de tráfico de red**. Los dispositivos que habitualmente recopilan este tipo de evidencias se sitúan entre el router y el firewall. Sin embargo, COE permite obtener el tráfico que se considere necesario para analizar un incidente en todos los puntos de la red en los que situemos un cliente. De manera adicional, evitamos que aquellos ataques que no pasen entre estos dispositivos, debido a un diseño de red inseguro o por incidentes producidos en el mismo segmento de red, pasen desapercibidos y sin ser registrados.
- **Protección ante pérdidas de conectividad con el servidor**. Los clientes pueden recopilar información de manera independiente, almacenando las evidencias hasta que la conectividad con el servidor sea restablecida.
- **Reducción de la alteración de evidencias**. Para ello, emplea herramientas forenses para la obtención de evidencias y, de manera temporal, almacena dichas evidencias en un dispositivo externo de almacenamiento. De este modo se evita la sobreescritura de información en otras evidencias, como el disco duro local.
- **Gestión simultánea de incidentes**, puesto que COE está diseñado para permitir la concurrencia en el tratamiento de incidentes.
- **Tratamiento de todos los tipos de evidencias digitales volátiles** en entornos Windows, empleando para ello aplicaciones forenses.
- **Flexibilidad en la configuración de evidencias** necesarias por tipo de incidente, mediante la utilización de un fichero de configuración en el que se relacionan el tipo de incidente y las evidencias necesarias.
- **Almacenamiento centralizado de las evidencias** obtenidas en el servidor.
- **Incorporación de mecanismos de integridad de las evidencias** calculando el hash de cada uno de los ficheros de evidencias recibido, mediante el algoritmo MD5, y manteniendo el valor en un fichero específico.

D. *Resultados obtenidos con COE*

El objetivo de este apartado es mostrar el funcionamiento de COE cuando es invocado por un sistema de monitorización que ha detectado un incidente de seguridad.

En concreto, un sistema de monitorización que controla los puertos de una máquina determinada, detecta que se ha abierto un puerto no autorizado. Esta circunstancia podría ser síntoma de una infección por un virus o *malware*. En la Fig. 5, se muestra un esquema del entorno creado para la ejecución.

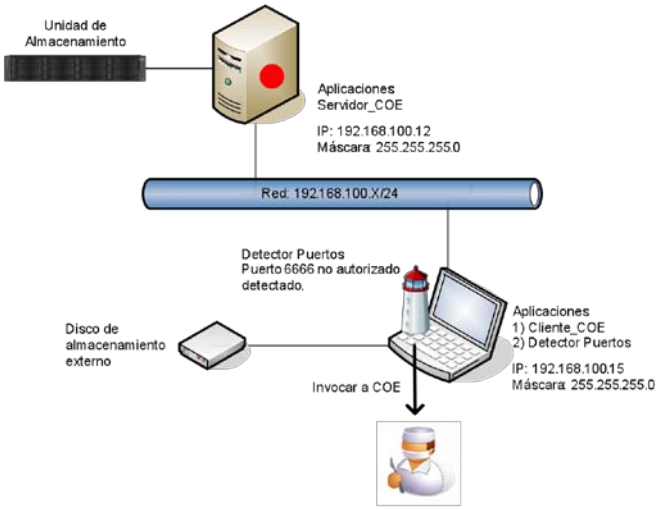


Fig. 5. Descripción del entorno de pruebas de COE

Es en este punto en el que COE comienza a capturar evidencias digitales volátiles que podrían resultar de utilidad en el posterior análisis ver Fig. 6. En concreto, puesto que se ha abierto un puerto de manera inesperada, COE inicia una captura de todo el tráfico de red que tenga como origen o destino este puerto durante un periodo de 5 minutos. De esta manera, no estaremos registrando todo el tráfico que sea enviado o recibido por el sistema que tenga instalada esta aplicación y que, a priori, no va a resultar de interés.

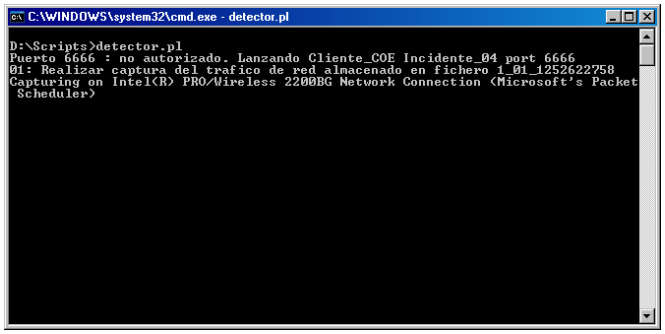


Fig. 6. Ejecución de COE y comienzo de obtención de evidencias

En este punto, sería interesante diseñar un cliente de COE que tuviera varios hilos de ejecución, permitiendo así la obtención de evidencias volátiles en paralelo.

En este caso, hemos recopilado información de todos los tipos de evidencias digitales volátiles compatibles con COE, incluyendo volcado de memoria, puertos abiertos, usuarios conectados o información de la tabla de NetBIOS. Cuando finalice la la obtención de evidencias, enviará los ficheros comprimidos al servidor.

Por otro lado, el servidor de COE, mientras se lleva a cabo la obtención de evidencias en el cliente, crea un proceso hijo para permitir de este modo la recepción de evidencias de varios clientes simultáneamente. Este proceso hijo crea la estructura de carpetas para almacenar las evidencias recibidas, estructura que contiene información de la fecha de la captura, cliente que envía la información, identificador y tipo de incidente. A continuación, queda a la espera de recibir las evidencias recopiladas. En las Fig. 7 y 8 se muestra un ejemplo de recepción de evidencias por parte del servidor y la estructura de carpetas creada con las evidencias recibidas.

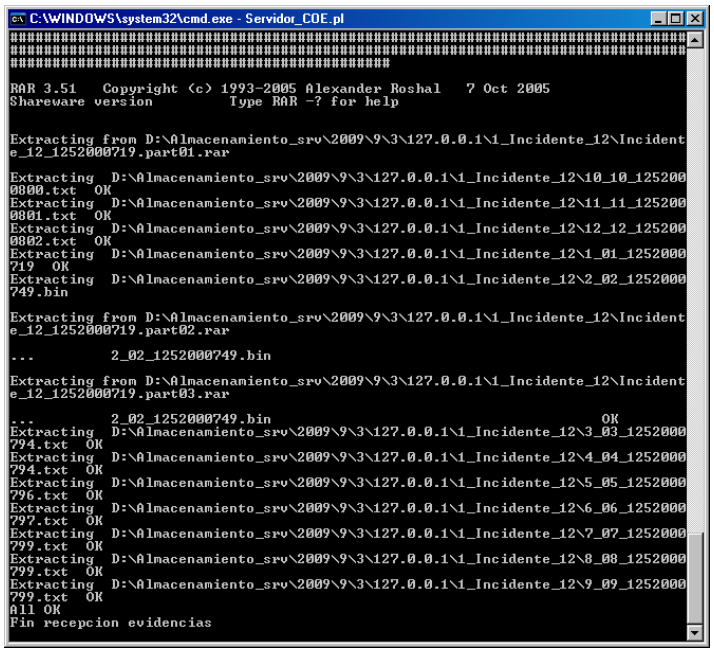


Fig. 7. Servidor de COE

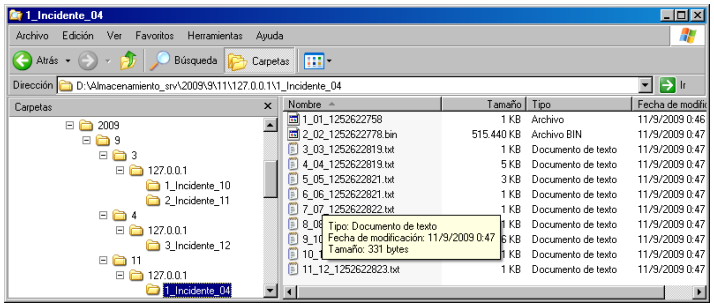


Fig. 8. Evidencias recibidas en el servidor de COE

Por último, el servidor COE calcula el hash de las evidencias recibidas y las almacena en un fichero de texto siguiendo el formato empleado por la aplicación md5sum, con objeto de facilitar los procedimientos de comprobación de integridad.

Como resultado de nuestra prueba, obtuvimos todas las evidencias digitales volátiles relacionadas con el evento de seguridad detectado de manera inmediata y sin necesidad de intervención de un analista forense.

Sin embargo, con esto sólo se ha cubierto la primera de las fases de un análisis forense. A continuación, habrá que trabajar sobre las evidencias obtenidas para tratar de averiguar qué ha sucedido, cómo ha sucedido y quién lo ha realizado.

V. CONCLUSIONES

Por todo lo anteriormente expuesto concluimos que COE es una solución que, combinando aplicaciones ya existentes, obtiene evidencias digitales volátiles relacionada con un incidente. En un entorno que utilice COE, los analistas

forenses dispondrán de gran parte de la información volátil necesaria para llevar a cabo los procedimientos de investigación de manera centralizada, minimizando la cantidad de información que no sea útil; y proporcionando mecanismos de verificación de la integridad de las evidencias.

Con respecto de otras soluciones existentes en el mercado, COE presenta ventajas como las que se detallan a continuación:

- Es integrable con otras aplicaciones de detección de incidentes, no dependiendo exclusivamente de un único motor de monitorización. Además, esta integración reduce el tiempo de respuesta ante incidentes invertido puesto que se lanza la ejecución del programa de manera automática.
- Combina la obtención de evidencias digitales volátiles de dos tipos: tráfico de red y elementos volátiles del sistema operativo. En un análisis forense probablemente necesitaremos ambos elementos para poder realizar un diagnóstico fiable de lo que ha sucedido. Además, es posible incorporar a COE la funcionalidad necesaria para la obtención de evidencias digitales no volátiles, como la imagen de un disco duro.
- Por último, incorpora mecanismos para la preservación de las evidencias de manera centralizada y calculando la huella digital de cada evidencia para verificar que no se ha alterado desde su obtención.

Sin embargo, COE no es una solución adecuada para todos los tipos de incidentes de seguridad. Una de sus características principales es que distribuye la carga de obtención de evidencias en clientes, pero en aquellos casos en los que el ataque afecte al rendimiento de la máquina o que lo reinicien de manera inesperada, no será posible recuperar las evidencias digitales volátiles necesarias.

Asimismo, es recomendable introducir ciertas mejoras en el diseño de COE. Uno de los aspectos principales de las evidencias digitales, es su preservación mediante mecanismos de cadena de custodia.

Para mejorar esta funcionalidad, actualmente limitada a verificar la integridad de las evidencias, sería recomendable proporcionar un entorno de acceso a las evidencias almacenadas en el servidor que registre de manera segura los usuarios que han accedido a las evidencias y las operaciones realizadas sobre ellas. Además, debería dotarse de mecanismos específicos de seguridad al fichero que contiene los *hashes* de las evidencias recibidas. Proponemos trabajar en una solución que firme el fichero de *hash* generado y que sea único por incidente.

Otro ejemplo de mejora propuesta consistiría en dotar a COE de mecanismos de aprendizaje automático en función de experiencias pasadas con objeto de optimizar las evidencias que se recopilen, filtrando aquellas que no vayan a ser útiles o añadiendo otras que en principio carecían de interés.

REFERENCIAS

[1] García Noguera, Noelia. *Delitos informáticos en el Código penal español*. Disponible en http://www.portaley.com/delitos-informaticos/codigo-penal.shtml.

[2] Convenio Sobre Ciberdelincuencia, Budapest, 23 nov. 2001. Disponible en https://www.gdt.guardiacivil.es/media/Convenio_Ciberdelincuencia.pdf

[3] Boletín Oficial del Estado (BOE) nº 281. Ley Orgánica 10/1995, 23 de nov. Disponible en http://www.boe.es/boe/dias/2004/11/22/pdfs/A38623-38627.pdf

[4] Barroso, D. *Informe sobre el Cibercrimen 2008*. Disponible en http://www.s21sec.com.

[5] Kent, K., Chevalier, S., Grance, T. y Dang, H. *Guide to Integrating Forensic Techniques into Incident Response*. Disponible en http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

[6] E Mandia, K., Prosise, C., Pepe, M. *Incident Response and Computer Forensics, 2nd Edition*, McGraw-Hill, 2003.

[7] Brezinski, D., Killalea, T. *RFC 3227: Guidelines for Evidence Collection and Archiving*, 2002. Disponible en http://www.rfc-editor.org/bcp/bcp55.txt.

[8] Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet 2nd Edition*. ElSevier Academic Press, 2004.

[9] Carrier, B. *File System Forensic Analysis*. Addison-Wesley, 2005.

[10] Consulta de características de Snort en la página web http://www.snort.org. Consultado en 2009.

[11] Roesch, M., Green, C. *Snort Users Manual 2.8.4*. Poner fecha y editorial.

[12] Jones, K, Bejtlich, R., Rose, C. *Real Digital Forensics: Computer Security and Incident Response.* Addison-Wesley, 2008.

[13] Nikkel, B. *A portable network forensic evidence collector*. Publicado por Elservier en Digital Investigation: The International Journal of Digital Forensics and Incident Response. Vol.3 No. 3. Octubre, 2006.

[14] Nagesh, A. *Distributed Network Forensics using JADE Mobile Agent Framework*. Universidad de Arizona.

[15] Guidance Software. *Encase Enterprise Edition v6.15 User's Guide*. 2009.

[16] Herramienta y características obtenidas en *http://www.wireshark.org*. Consultado en 2009.

[17] Herramienta y características obtenidas en *http://www.foundstone.org*. Consultado en 2009.

[18] Herramienta y características obtenidas en *http://www.sysinternals.org*. Consultado en 2009.

Anonimización de *payloads* para el desarrollo de AIDS basados en protocolos

Rolando Salazar-Hernández, Jesús E. Díaz-Verdejo
Departamento Teoría de la señal, telemática y comunicaciones
Universidad de Granada
ETS Ing. Informática y Telecomunicación – 18071 - Granada
rsalaza@ugr.es, jedv@ugr.es

***Resumen*- La adquisición de tráfico de red plantea diversos problemas de índole legal relacionados con la privacidad de las comunicaciones. Sin embargo, la disponibilidad de este tipo de datos resulta imprescindible para el desarrollo de sistemas de detección de intrusiones (IDS) basados en anomalías. Para preservar la privacidad y evitar el problema se pueden utilizar técnicas de anonimización del tráfico. Las técnicas existentes se centran en la ocultación de la información contenida en las diferentes cabeceras, lo que resulta inadecuado en algunos casos. En este trabajo se presenta y evalúa una técnica de anonimización que actúa sobre los contenidos de los mensajes intercambiados y que resulta válida para el desarrollo y evaluación de AIDS que operen en base a las cargas útiles del tráfico monitorizado.**

***Palabras Clave*- sistemas de detección de intrusiones, anonimización**

I. INTRODUCCIÓN

El desarrollo y evaluación de sistemas de detección de intrusiones basados en anomalías (AIDS, del inglés *Anomaly-based Intrusion Detection System*) requiere de la disponibilidad de conjuntos de datos que contengan la información necesaria para realizar la detección. Estos datos se usan tanto durante la fase de entrenamiento (estimación de los modelos o determinación de parámetros de los métodos de detección), como durante la evaluación de su rendimiento. A fin de que tanto el AIDS resultante como su evaluación sean válidos y representativos de cara a la detección de intrusiones, los datos deben haber sido obtenidos en entornos reales en explotación [1] [2] [3]. En caso contrario, el IDS no incorporará un modelo adecuado del comportamiento normal del sistema, por lo que su rendimiento no sería el esperado. Adicionalmente, se introducirán sesgos significativos durante la evaluación del rendimiento y, en consecuencia, en la comparación entre las diferentes técnicas desarrolladas o existentes, al falsearse la relación entre la tasas de detección (ataques correctamente detectados) y de falsos positivos (eventos normales detectados como ataques).

En el ámbito de los AIDS basados en red [4], contexto en el que se sitúa el presente trabajo, los datos necesarios corresponden a tráfico circulante en la red. Tal como se ha indicado anteriormente, en esta situación será necesario, por tanto, capturar el tráfico circulante en redes reales en explotación. Sin embargo, uno de los principales problemas que se plantean cuando se manejan bases de datos con tráfico real es que pueden contener datos sensibles en cuanto a la seguridad y privacidad de las comunicaciones. En este sentido, si estos datos sensibles son manejados sin una autorización expresa de los implicados, se puede incurrir en acciones tipificadas como delito de acuerdo las legislaciones vigentes en cada país. En particular, la Ley de Protección de Datos vigente en la Unión Europea tipifica este tipo de actividades. Por otra parte, además de las cuestiones relacionadas con la privacidad de los usuarios, también se plantean problemas desde el punto de vista de la seguridad de la infraestructura de la red, ya que permiten inferir información que puede ser utilizada para atacar dicha infraestructura [5] [6].

Para solventar estos problemas se suele plantear una aproximación basada en la anonimización de la información sensible contenida en la base de datos de tráfico. De esta forma, se posibilita, además, el uso de las mismas bases de datos por diferentes equipos investigadores, lo que permite comparar los rendimientos de las técnicas desarrolladas. Evidentemente, estas técnicas deben preservar la información relevante, de cara a la aplicación perseguida, sin que sea posible inferir ningún tipo de información sensible a partir de la misma.

Sin embargo, las técnicas descritas en la bibliografía, y que serán comentadas brevemente en el apartado siguiente, se centran en la anonimización de la información relativa a las cabeceras, como pueden ser las direcciones IP, los números de puertos, etc. Esto es debido a que en el escenario habitual las cargas útiles (*payloads*) de los paquetes son directamente eliminados o sólo se incluyen los primeros bytes. Consecuentemente, estas técnicas no serán de aplicación cuando la información sensible se encuentre en dichas cargas útiles, como es el caso que nos ocupa.

En consecuencia, en el presente trabajo se presenta y evalúa una técnica para la anonimización de la información contenida en las cargas útiles asociadas a protocolos basados en el intercambio de mensajes de texto, como es el caso de HTTP o DNS. En particular, la técnica propuesta se aplica al caso de peticiones GET del protocolo HTTP, dado que se está trabajando en el desarrollo de AIDS basados en esta información [7]. En esencia, el proceso de anonimización se basa en el mapeo y sustitución, una a una, de las diferentes cadenas de texto que aparezcan en la carga útil, a la vez que se obtienen algunos datos relativos a propiedades genéricas de las cadenas sustituidas y que pueden ser relevantes en el proceso de detección, como puede ser la frecuencia de aparición de la cadena. Esta técnica presenta dos características importantes: es de fácil implementación y bajo

coste computacional y, adicionalmente, preserva la información en la que se basan las técnicas de detección asociadas a la identificación de cadenas en las cargas útiles.

A continuación (Apartado II) se presentarán algunas de las técnicas básicas de anonimización así como las características de las mismas, estudiándose su aplicabilidad a la anonimización de las cargas útiles. En la Sección III se describirá la técnica propuesta, que será aplicada en un escenario concreto en la Sección IV. Finalmente, se presentarán las conclusiones.

II. TÉCNICAS DE ANONIMIZACIÓN DEL TRÁFICO DE RED

Como se ha mencionado con anterioridad, la anonimización del tráfico de red tiene como objetivo fundamental preservar la seguridad y la privacidad de las comunicaciones en lo que respecta a los datos sensibles implicados. Estos datos sensibles pueden corresponder tanto a datos relativos a los individuos implicados (por ejemplo el DNI, los números de cuenta, las páginas web accedidas, los perfiles y preferencias, etc.), como a datos relativos a la infraestructura de red (direcciones y máscaras de red, ubicación de cortafuegos, etc.). De esta forma, es necesario ocultar cualquier tipo de dato que permita inferir información de dicha naturaleza, pero sin alterar la información asociada al proceso que se realizará seguidamente. Es decir, se trata de ocultar la información sensible sin alterar las características que serán analizadas en las fases de tratamiento posterior. Por ello, en la aplicación de las técnicas de anonimización resulta extremadamente relevante la finalidad a la que se destinan los datos. Así, por ejemplo, si se pretende caracterizar los flujos de tráfico entre diferentes subredes será necesario que la transformación a aplicar a los datos (IPs en este caso) no altere las relaciones entre los diferentes equipos en cuanto a su pertenencia a la misma subred.

Las técnicas habituales de anonimización se pueden agrupar en las siguientes categorías [6]:

- Filtrado: el valor de los campos con información sensible es borrado.
- Reemplazo: se cambian los valores de los campos sensibles bien mediante la permutación con otros valores contenidos en los datos (pseudo-anonimato) o por valores diferentes (anonimato total).
- Reducción de exactitud: se sustituyen los valores de los datos por una aproximación de mismos o se realiza un mapeo de los valores de los datos por grupos.
- Agregación de ruido: se agrega ruido para perturbar los valores de los campos.
- Agregación: se sustituye el valor de los campos con estadísticas acumulativas de dichos valores.

Estas técnicas proveen diferentes niveles de protección, dependiendo la necesidad de utilizar unas u otras de las políticas de privacidad que cada entidad tenga. Por otra parte, en función de la finalidad de los datos, será necesario aplicar transformaciones con propiedades diferentes.

En el presente trabajo se pretende ofuscar la información contenida en las cargas útiles de los paquetes asociados a los protocolos de aplicación a analizar sin perder la información referente a la estructura y composición de los mismos. En particular, se pretende ocultar la información relativa a las páginas accedidas, los nombres de las variables y sus valores en el caso de URIs contenidos en peticiones GET. La información relativa a direcciones IP, puertos y restantes cabeceras resulta irrelevante y, por tanto, pueden ser anonimizadas mediante borrado o reemplazo.

A. Herramientas de anonimización

Existen varias herramientas disponibles para realizar la anonimización, entre las que cabe mencionar SCRUB-tcpdump [8], TCPdpriv [9] y Anonymizer API [10].

SCRUB-tcpdump permite la anonimización de las trazas de red en formato *tcpdump*, en campos que puedan contener datos sensibles. La herramienta trabaja en diferentes formas eliminando la información, añadiendo ruido, reemplazando o realizando permutaciones de los datos en los campos seleccionados. Sin embargo, trabaja únicamente hasta el nivel de transporte, por lo que la única operación posible para ofuscar las cargas útiles transportadas en los paquetes TCP o UDP consiste en el borrado de las mismas.

TCPdpriv es una de las herramientas disponibles en Internet con mayor difusión. Su operación es análoga a SCRUB-tcpdump, eliminando información sensible de las cabeceras de las trazas de red. En capas inferiores a TCP, dispone de una amplia gama de posibilidades de parametrización. De igual manera que ocurría con SCRUB-tcpdump, permite borrar toda la carga útil de los protocolos TCP y UDP. Provee diferentes niveles de anonimización, desde dejar los campos sin cambios hasta conseguir el más estricto anonimato, como el cambio completo de rangos de direcciones IP.

Anonymizer API es una herramienta desarrollada en C por Koukis y otros autores, presentando como principal ventaja su rapidez de procesamiento de las trazas. Utiliza funciones de las cuales depende del nivel de anonimato a aplicar a las trazas. AAPI provee una variedad de funciones de anonimización como el uso de compendios (*hashing*) con diferentes algoritmos (MD5, SHA, CRC32, etc.), aleatorización (*random*) para campos genéricos, mapeo de nombres de archivos y URI (*mapping*) para valores secuenciales sobre algún tipo de distribución (uniforme, gausiana, etc.), reemplazo (*replacing*) con constantes enteras o cadenas de caracteres, preservación (*prefix-preserving*) para direcciones IP, sustitución de expresiones regulares y borrado de campos. Esta herramienta permite anonimizar parte de las cabeceras en los protocolos de la capa de aplicación como son HTTP y FTP, si bien esta se realiza reemplazando el contenido de la cabecera por la que se indique.

Las tres herramientas mencionadas han sido analizadas y evaluadas con la finalidad de determinar su aplicabilidad en el contexto considerado. Sin embargo, únicamente AAPI permite operaciones diferentes del borrado sobre los campos de la capa de aplicación. Además, la única operación disponible es la sustitución por cadenas seleccionadas, lo que resulta inadecuado.

En consecuencia, se ha desarrollado una metodología que permita el anonimato de los campos con datos sensibles de las cabeceras del protocolo HTTP que será descrita a continuación. La metodología propuesta es aplicable a otros protocolos basados en el paso de mensajes de texto.

III. ANTECEDENTES Y ESPECIFICACIÓN DE REQUISITOS

La técnica de anonimización a utilizar debe reunir un conjunto de requisitos relacionados con las técnicas de detección a utilizar y la naturaleza de los mensajes. A fin de determinarlos, consideraremos la estructura típica de los mensajes intercambiados, particularizándolo al caso de URIs del protocolo HTTP, así como la técnica de detección desarrollada por nuestro equipo, denominada SSM [7].

A. Detección basada en modelado de los mensajes

La sintaxis y semántica de los mensajes intercambiados por un protocolo puede ser utilizada para construir un detector de anomalías. En [11] se describe detalladamente el uso del modelado de Markov para este fin. La idea clave es la clara existencia de estructura en los mensajes intercambiados por la mayoría de los protocolos, especialmente en los de la capa de aplicación. Esta estructura, definida en las especificaciones del protocolo, permite el uso de gramáticas y/o autómatas de estados finitos para describir la forma en la que se compone el mensaje. De esta forma, las cargas útiles de los paquetes que transportan los mensajes del protocolo presentarán una clara estructura que puede ser utilizada para estimar su probabilidad y, en consecuencia, para detectar anomalías en el uso del protocolo.

Así, a partir del modelo λ se puede definir un índice de normalidad, $N_s(p)$, para la carga útil p

$$N_s(p) = P(p \mid \lambda)$$

que permite la clasificación de dicha carga útil como normal o anómala sin más que establecer un umbral, θ,

$$clase(p) = \begin{cases} anómalo & N_s(p) < \theta \\ normal & N_s(p) \geq \theta \end{cases}$$

Sin entrar en excesivo detalle, la evaluación de la probabilidad asociada al modelo considera dos elementos relevantes: los estados y los símbolos observables. Los estados, $\underline{S}$, están asociados a los diferentes bloques o elementos que pueden constituir la carga útil de acuerdo a las especificaciones (sintaxis). Por otra parte, los símbolos observables, o_k, corresponden a los posibles valores de las cadenas que pueden ser observadas en los diferentes elementos o bloques constitutivos (estados) de la carga útil.

El conjunto formado por todos los símbolos observables, constituye el denominado *vocabulario*, V,

$$V=\{o_k,\ 1\leq k \leq M\}$$

También resulta relevante la probabilidad de observación (frecuencia de aparición) de cada uno de estos símbolos en cada uno de los estados, definida como el conjunto de probabilidades de observación, B,

$$B=\{b_{ik},\ 1\leq i\leq N,\ 1\leq k\leq M\}$$

donde b_{ik} es la probabilidad de observación del símbolo o_k en el estado s_i.

El desarrollo de IDS basados en esta aproximación requiere, básicamente, de la determinación de los estados, el vocabulario y las probabilidades asociadas a las transiciones entre estados y las de observación. La estructura en estados y las transiciones entre los mismos pueden inferirse habitualmente a partir de la especificación del protocolo. Sin embargo, la estimación del vocabulario y de las probabilidades requiere un proceso de estimación o entrenamiento a partir de la observación de instancias del protocolo a modelar. Es en este punto donde se requiere el uso de técnicas de anonimización.

Aunque esta técnica de detección puede ser aplicada a cualquier protocolo para el que el contenido de la carga útil presente estructura, a los efectos de este artículo nos centraremos en los URI de HTTP.

B. Estructura de los URI

La estructura de los URI contenidos en los mensajes intercambiados de acuerdo al protocolo HTTP viene definida en los RFC 1945 [12], 2068 [13], 2616 [14] y 2396 [15]. En estos se definen los diferentes campos constitutivos así como las reglas que rigen la composición de los mensajes a partir de dichos campos. Aunque el nombre de cada uno de los campos difiere en función del RFC considerado, se pueden considerar los siguientes tipos de campos, de acuerdo al RFC 2396:

- *Protocolo* (esquema en el RFC2396): protocolo a utilizar. En el caso consideraro, siempre será *´http'*.
- *Host*: nombre (recomendado) o dirección del equipo en el que se encuentra el recurso solicitado. El puerto, si existe (*:port*), se puede considerar incluido en este campo para los fines de este trabajo.
- *Segmento del path*: cada uno de los elementos del path que espcifica la ubicación del recurso solicitado en el equipo. La secuencia de todos los segmentos del path también se denomina referencia del URI en el RFC. Si existe, el fragmento ('#') se considerará incluido en este campo para los fines de este trabajo.
- *Consulta* (*Query)*: una cadena con información que debe ser interpretada por el recurso. De acuerdo a la sintaxis habitual, se considera compuesta por la secuencia de dos tipos de campos:
  Atributo: nombre de una variable o cadena.
  Valor: valor asignado a la variable.

Un URI consta de un protocolo (opcional), un equipo (opcional), una secuencia de uno o más segmentos de path, que constituyen el path absoluto de acuerdo a la terminología usada en el RFC2616, y, opcionalmente, una consulta compuesta por una secuencia de atributos cada uno de los cuales con un valor opcional. De esta forma, de acuerdo al RFC2616, un URI de HTTP o URL presenta la forma general:

"http:" "//" host [":" puerto] [abs_path ["?" consulta]]

Cualquier URI puede ser fácilmente segmentado en una secuencia de campos con sus valores asociados. A modo de ejemplo, considérese el URI

`host.nombre.dominio/dir1/dir2/script`

que puede ser segmentado en 4 valores

{"host.nombre.dominio", "dir1", "dir2", "script"}

sin más que considerar la sintaxis establecida.

Por tanto, en el contexto del modelado de protocolos descrito previamente, cada uno de los campos estará asociado a un estado del modelo, mientras que el vocabulario estará compuesto por cada una de las cadenas que pueden aparecer en el URI.

C. Requisitos de la técnica de anonimización

Por tanto, la técnica de anonimización a aplicar debe preservar la información asociada a los diferentes valores (cadenas) que pueden aparecer en los campos de los

mensajes. Esta información presenta dos facetas diferenciadas desde el punto de vista del detector. Por una parte, debe preservarse la información relativa a la posibilidad de aparición de una cadena concreta (pertenencia al vocabulario) en cada uno de los campos y, por otra parte, resulta relevante la frecuencia de aparición de cada uno de estos valores a fin de determinar su probabilidad. Adicionalmente, y en función de las variantes de la técnica de detección considerada, puede resultar de interés disponer de información relativa a la naturaleza de las cadenas (numérica, alfanumérica, alfabética) y algunas de sus características más relevantes, como por ejemplo la longitud en número de caracteres de dichos valores.

La información sensible se encontrará, obviamente, en los valores de los parámetros, como por ejemplo, el valor del campo DNI de una consulta, el nombre de un usuario o la página accedida. Por tanto, la ofuscación necesaria debe eliminar los valores de las cadenas, no siendo válidas, en consecuencia, las técnicas de reemplazo basadas en permutaciones. La única técnica viable en este contexto será la de reemplazo en base a un conjunto de valores diferente del conjunto original.

Finalmente, otro de los requisitos de la técnica de anonimización a emplear es que debe permitir la reposición de los valores originales. A pesar de que esto pueda parecer contradictorio, hemos de reseñar que el objetivo de la anonimización es disponer de trazas de tráfico susceptibles de ser utilizadas durante el desarrollo y evaluación de los detectores. Es evidente que la puesta en explotación de los mismos requerirá que la transformación realizada pueda ser invertida en los modelos resultantes a fin de que puedan operar en la red real. Si se realiza adecuadamente, esta reposición puede ser realizada por el administrador de la red, de forma análoga a la anonimización inicial, por lo que los investigadores o desarrolladores no tendrán acceso en ningún momento a la información sensible. Esta restricción puede relajarse sin más que considerar la aplicación de la transformación a todo el tráfico entrante cuando el detector se encuentre en operación, aunque de esta forma se introduciría una sobrecarga computacional innecesaria.

IV. Metodología propuesta

La metodología propuesta se basa en reemplazar cada uno de los valores de cada uno de los campos que constituyen el mensaje a partir de un diccionario de equivalencias. Para ello se considera como punto de partida la traza de red capturada en bruto, es decir, tal como se obtiene a partir de la red en explotación. A continuación detallaremos el proceso y metodología a seguir que consta de varias fases (Fig. 1):

- *Preparación y acondicionamiento*: durante esta fase se extrae la información relevante de cada uno de los paquetes de la traza de red. También se consideran procedimientos adicionales relacionados con la calidad de los datos obtenidos.
- *Obtención de vocabulario*: se obtiene el vocabulario asociado al tráfico monitorizado.
- *Caracterización del vocabulario*: opcionalmente, si el método de detección así lo requiere, se caracterizan cada uno de los elementos del vocabulario.

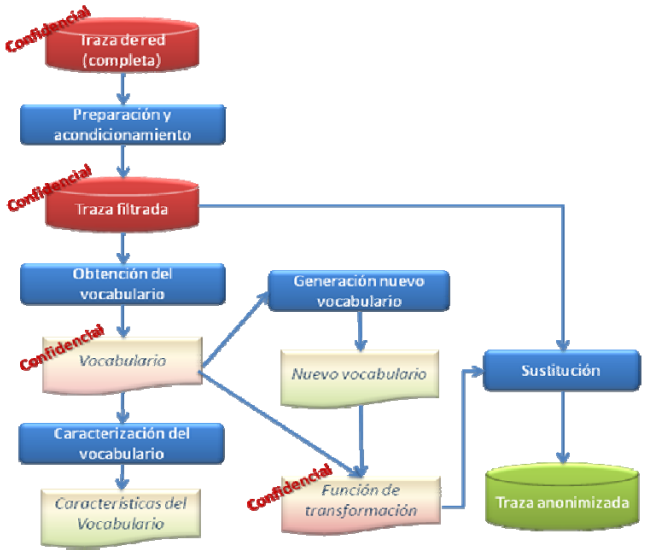


Fig. 1. Fases y elementos del proceso de anonimización propuesto.

- *Generación del nuevo vocabulario*: se genera un nuevo vocabulario con el mismo número de elementos que el original para reemplazarlo. No debe existir ningún tipo de relación entre los elementos del nuevo vocabulario y los del original.
- *Sustitución*: se genera una función de transformación que asocie a cada elemento del vocabulario original un elemento del nuevo vocabulario. Usando esta función, se reemplazan todas las cadenas correspondientes al vocabulario original en la traza de red por su correspondiente elemento del nuevo vocabulario.

Como resultado de estas fases, que serán detalladas a continuación, se obtiene un conjunto de datos que preserva la información útil de la traza de red y que se encuentra convenientemente anonimizada. La información confidencial se encuentra en el vocabulario original y en la función de transformación, por lo que para preservar la privacidad únicamente se requiere la ocultación de esta información. Adicionalmente, es posible revertir la operación sin más que aplicar la función de transformación inversa.

A. Preparación y acondicionamiento

La metodología propuesta se inicia sobre el conjunto de datos capturados de la red, es decir, sobre la traza de tráfico,

$$T_{orig}=\{t_{orig,i},\ 1<i<L_{orig}\},$$

que debe haber sido adquirida en función de las características a analizar. Se considera, por tanto, el uso de los filtros que se estimen oportunos sobre los datos durante el proceso de captura. Evidentemente, esta traza contendrá la información sensible que se pretende anonimizar, por lo que deberá haber sido adquirida y procesada por personal autorizado. Adicionalmente, es posible que incluyan cabeceras con información relativa a direcciones IP, puertos, etc. Esta información también puede resultar sensible, por lo que habrá que considerar la aplicación de técnicas de anonimización también a estos elementos. Dado que únicamente estamos analizando la ofuscación de la información contenida en las cargas útiles, este aspecto no será considerado. Por tanto, en lo que sigue consideraremos que dicha información de cabecera ha sido convenientemente

anonimizada mediante la técnica que se estime oportuna y de acuerdo a la política de privacidad que sea de aplicación.

Dada la finalidad del tráfico capturado, puede resultar necesario comprobar la ausencia de tráfico de ataques en la traza obtenida. Para ello pueden utilizarse detectores de intrusiones basados en firmas (p.e. Snort [16] o Bro [17]), que permitirán la detección de los paquetes inadecuados y, por tanto, posibilitarán su posterior eliminación mediante filtrado.

Otro aspecto a considerar en esta fase es la extracción de la información que se considera relevante para las fases posteriores, lo que puede requerir un filtrado adicional de la traza T_{orig}. En nuestro caso particular, únicamente resulta de interés el URI contenido en las peticiones GET del protocolo HTTP, por lo que se descartarán los paquetes que no incluyan peticiones GET y se extraerá dicho URI.

Como resultado del proceso de preparación y acondicionamiento se obtendrá, a partir de la traza original, T_{orig}, una nueva traza,

$$T_{fil}=\{t_i,\ 1<i<L_f\};\ T_{fil}\subseteq T_{orig}$$

únicamente con los datos a considerar en las fases posteriores. Típicamente, estos serán cargas útiles, o segmentos de la misma, de los protocolos considerados. Evidentemente, la información contenida en esta traza continuará siendo sensible, por lo que todo el proceso anterior debe haber sido realizado por personal autorizado al que se habrán suministrado las especificaciones de captura y los filtros a aplicar, en su caso.

B. Obtención del vocabulario

La siguiente fase consiste en la obtención del vocabulario original, V_{orig}, a partir de T_{fil}. Para ello se requiere la segmentación de las cargas útiles contenidas en T_{fil} de acuerdo a las especificaciones correspondientes.

Sean *nseg(p)* y *segmento(p,i)* las funciones que obtienen, respectivamente, el número de segmentos de la carga útil *p* y el segmento *i*-ésimo de dicha carga útil. A partir de éstas, la obtención del vocabulario se puede realizar de acuerdo al siguiente procedimiento:

- Inicialización:

$$V_{orig}=\varnothing$$

- Recursión: $\forall\ t_i \in T_{fil}$

$$n_i = nseg(t_i)$$

$$S_i = \left\{ s_j = segmento(t_i, j),\ \forall j, 1 \le j \le n_i \right\}$$

$$V_{orig} = V_{orig} \cup S_i$$

Finalmente, se obtendrá el vocabulario compuesto por todos los valores diferentes de las cadenas en cada uno de los segmentos

$$V_{orig}=\{o_k,\ 1\le k \le M\}$$

siendo $M \ge L_f$. Este vocabulario contiene todas las cadenas de texto encontradas en la traza, por lo que contiene información sensible. Para su obtención será necesario suministrar al personal autorizado los programas correspondientes incluyendo las funciones *nseg()* y *segmento()*.

Por motivos meramente operativos puede resultar conveniente ordenar alfabéticamente los elementos del vocabulario, a fin de facilitar el proceso de búsqueda y sustitución. Esta ordenación no introduce ninguna modificación conceptual en el proceso de anonimización.

- $T_{\{orig \mid fil \mid anon\}}$: traza de tráfico (conjunto de cargas útiles) original, filtrada o anonimizada.
- t_i: elemento de una traza de tráfico
- $L_{\{orig \mid fil \mid anon\}}$: tamaño de una traza (núm. elementos)
- $V_{\{orig \mid nuevo\}}$: vocabulario
- M: tamaño del vocabulario
- o_k: elemento del vocabulario original (palabras)
- p_k: elemento del vocabulario anonimizado (pseudo-palabras)
- S: conjunto de segmentos de un elemento de la traza
- s_i: segmento i-ésimo de un elemento de la traza
- C: conjunto de vectores de características del vocabulario
- c: vector de características de un elemento del vocabulario

Tabla 1. Notación utilizada.

C. Caracterización del vocabulario

En algunos casos la técnica de detección puede incorporar información relativa a la propia estructura de las cadenas de texto que pueden aparecer en los diferentes elementos constitutivos de la carga útil. A modo de ejemplo, en el caso de los URI puede utilizarse la naturaleza de la cadena (texto, alfanumérica, numérica) y su longitud. Dado que se va a realizar una sustitución de dichas cadenas, será necesario preservar la información de estructura que se considere necesaria, siempre con las limitaciones que determine la política de privacidad en uso. Es decir, se podrían considerar características globales como las mencionadas, mientras que sería delicado incluir aspectos de mayor detalle como por ejemplo, el número de vocales que contiene.

En cualquier caso, para esta fase se considera el vocabulario previamente extraído, V_{orig}, para el que se obtiene el vector de características, C_k, asociado a cada elemento del vocabulario, o_k, a partir de la función que obtiene la característica i-ésima, como

$$C_k = [c_{ki}]_{1\le i\le D} \quad siendo\ c_{ki} = característica(o_k, i)$$

La información resultante carece de información sensible si las características extraídas son adecuadas, por lo que puede ser utilizada por personal no autorizado. Sin embargo, durante el proceso de extracción habrá que manejar el vocabulario original, por lo que su obtención deberá realizarse por parte de personal autorizado al que se suministrarán los programas necesarios.

D. Generación del nuevo vocabulario

El nuevo vocabulario será utilizado para sustituir al original, por lo que debe contener el mismo número de elementos (M). Dado que no debe existir ninguna relación entre cada uno de los elementos de ambos vocabularios, sin pérdida de generalidad, se propone la generación de elementos del vocabulario de acuerdo al esquema p*n* , con n un número en el rango [1,M]. Dado que no serán palabras válidas en el protocolo considerado, y a fin de clarificar la

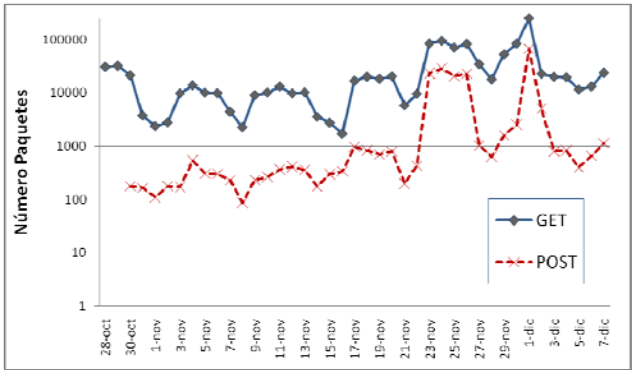


Fig. 2 Histograma de la captura de la base de datos PVHDB.

L	Host	URI
123	http://www.ugr.es	~biblio/bibl_electrónica/bases_datos/index.html

Fig. 3. Formato de los registros de la traza filtrada.

nomenclatura, denominaremos en lo que sigue a estos elementos como pseudo-palabras.

Por tanto, el nuevo vocabulario V_{nuevo} estará compuesto por

$$V_{nuevo}=\{p_k=\text{“p}k\text{”}, 1\leq k \leq M\}$$

Evidentemente, no existe ningún tipo de información sensible en este vocabulario.

E. Sustitución

La sustitución constituye el núcleo de la técnica de anonimización que, como se ha comentado, consiste en el reemplazo de cada una de las apariciones de las palabras en el vocabulario por pseudo-palabras. Para ello se define una función de reemplazo,

$$\Re : V_{orig} \rightarrow V_{nuevo}$$
$$\Re(o_k) = p_k$$

La función de reemplazo debe ser biyectiva para no alterar las frecuencias de aparición de cada palabra ni sus posiciones relativas dentro de las cargas útiles. La obtención de la traza anonimizada, T_{anon}, se realizará mediante la aplicación de la función de reemplazo a cada uno de los segmentos de cada uno de los elementos de la traza filtrada, T_{fil}, de tal forma que

$$segmento(t'_i, j) = \Re(segmento(t_i, j)) \quad 1 \leq j \leq nseg(t_i)$$

siendo

$$T_{anon}=\{t'_i, 1<i<L_f\};\ card(T_{fil})=card(T_{anon})$$

En el caso de que se hubiesen ordenado alfabéticamente los elementos de V_{orig} resulta conveniente realizar una reordenación aleatoria de los elementos de V_{nuevo} o asignar el número de secuencia incluido en la pseudo-palabra al azar a fin de ocultar la información de orden en el resultado. En caso contrario, de la relación $p_k<p_{k+1}$ podría extraerse información, especialmente en el caso de grandes vocabularios. Consecuentemente, habrá que aplicar la misma reordenación a las características C_k.

Dado que se utilizan tanto T_{fil} como V_{orig}, ambos conteniendo información sensible, el proceso de reemplazo debe ser realizado por personal autorizado. El resultado, T_{anon}, carece de información sensible.

Finalmente, tanto la traza anonimizada, T_{anon}, como los vectores de características, C_k, pueden ser distribuidos sin restricciones.

Paq. GET	Alertas	GET “limpio”	Err. Cab.	URIs	Palabras Vocab.
1.176.781	16	1.176.765	208	1.176.557	28.025

Tabla 2. Características de la traza de red capturada.

F. Restitución

La aplicación de la técnica de detección desarrollada, en su caso, puede realizarse sin más que considerar la función de reemplazo en todos los paquetes a analizar de forma análoga a la realizada durante el proceso de anonimización. Sin embargo, esto supone una carga computacional que resulta conveniente eliminar. Dado que la función de reemplazo es biyectiva, existirá la función inversa que puede ser aplicada al modelo obtenido, si este incluye información sobre las pseudo-palabras, recuperándose el vocabulario original en dicho modelo.

Evidentemente, también puede recuperarse la traza filtrada original a partir de la traza anonimizada y de la función de reemplazo inversa, si fuese necesario.

V. EJEMPLO DE APLICACIÓN

La eficacia de la metodología ha sido probada con una base de datos de tráfico real denominada PVHDB. Esta base de datos ha sido adquirida en una institución académica que ha permitido la colocación de un sensor para adquirir el tráfico asociado a un servidor web en producción. A continuación se describe el proceso seguido.

A. Preparación y acondicionamiento

La traza se ha capturado mediante la herramienta *tcpdump* [18] del 28 de noviembre al 7 de diciembre del 2009. En la Fig. 2 se muestra el volumen de tráfico diario obtenido. Por las características del sistema de detección desarrollado, únicamente se hará uso de las peticiones GET y POST del protocolo HTTP. De los datos adquiridos, 1.176.781 paquetes contienen peticiones GET, habiéndose filtrado el tráfico restante en primera aproximación.

A continuación se utiliza un sistema de detección de intrusos basados en firmas (Snort) para descartar el tráfico anómalo y/o ataques que la base de datos pudiera contener. Snort se ha configurado y parametrizado con las reglas VRT del 18 de septiembre del 2009 que afectan el contenido del URI. Después de evaluar la traza, se han detectado 16 paquetes con instancias de ataque, que han sido descartados. En consecuencia, la traza original consta de 1.176.765 paquetes de tráfico GET “limpio”. Las características más relevantes de la traza se resumen en la Tabla 2.

La anonimización de las cabeceras se ha realizado mediante borrado, ya que la información a utilizar se encuentra únicamente en las cargas útiles. Mediante los programas adecuados, se ha extraído el URI de cada uno de los paquetes, que ha sido almacenado en un archivo de traza filtrada, T_{fil}, en el que también se incluye la longitud del URI a fin de facilitar el procesamiento de los datos. El formato

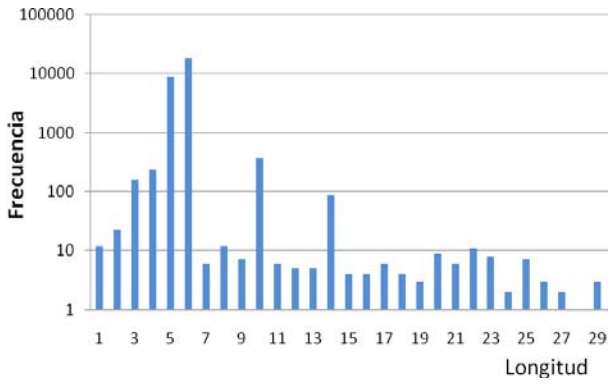


Fig. 4. Distribución de longitudes de las palabras en el vocabulario.

Pseudopalabra	Palabra
p0	bases_datos
p1	bibl_electronica
p2	index.html
p3	www.ugr.es
p4	~biblio

Fig. 5. Función de reemplazo: asociación entre palabras y pseudo-palabras de los vocabularios.

resultante de cada uno de los registros del archivo de traza filtrada se muestra en la Fig. 3.

B. *Obtención del vocabulario*

A partir del archivo de traza se ha extraído el vocabulario tras la segmentación de cada uno de los URI. Para ello se ha utilizado la librería *URIparser* [19], que responde a las especificaciones del RFC2396.

El tamaño del vocabulario resultante, V_{orig}, es de 28.025 palabras diferentes.

C. *Caracterización del vocabulario*

Dicho vocabulario ha sido analizado para obtener el tipo de cadena correspondiente a cada una de las palabras así como la longitud de las mismas.

En cuanto a la clasificación, se han etiquetado 30 palabras como alfabéticas, 481 palabras como numéricas y 27.014 palabras como alfanuméricas. En la Fig. 4 se muestra el histograma correspondiente a la distribución de las longitudes de las palabras analizadas.

D. *Generación del nuevo vocabulario*

De acuerdo al tamaño del vocabulario original, se ha generado un nuevo vocabulario compuesto por 28.025 pseudo-palabras con el formato *p[n]*, siendo *n* un número de 0 a 28.024.

E. *Sustitución*

Para realizar la sustitución de las cadenas en la traza filtrada se ha definido una función de reemplazo (Fig. 5) que asocia cada palabra del vocabulario original, V_{orig}, con una pseudo-palabra de V_{nuevo}.

Obsérvese que, a fin de facilitar la búsqueda de las palabras a reemplazar durante la sustitución, se han ordenado alfabéticamente las palabras del vocabulario original. En consecuencia, también se ha realizado la reordenación

Pseudopalabra	Longitud y tipo
p0	11 A
p1	16 X
p2	10 A
p3	10 A
p4	6 A

Fig. 6. Índice de características.

L	Host	URI
123	http://www.ugr.es/	~biblio/bibl_electrónica/bases_datos/index.html
21	http://p3/	p4/p1/p0/p3

Fig. 7. URI antes y después de la anonimización.

correspondiente en el conjunto de características. Por ello, se ha considerado la generación de un archivo de características indexado en el que se detallan las características de cada una de las pseudo-palabras (Fig. 6).

Finalmente, se realiza la sustitución de todas las palabras contenidas en los URI de la traza filtrada (Fig. 7). En este proceso se respetan las posiciones relativas de las cadenas en el URI, por lo que la información de estructura (sintaxis) se mantiene. Por otra parte, dado que la sustitución es uno a uno, se preserva el número de veces que aparece cada cadena, por lo que no se introducirán cambios en las frecuencias relativas de aparición. Se consiguen cumplir, por tanto, los requisitos asociados a la técnica de detección. La traza resultante, así como la relación de características de los elementos del vocabulario, carecen de información sensible.

F. *Restitución*

Una vez estimado el modelo a utilizar para la detección de anomalías se puede revertir la anonimización sin más que usar la transformación inversa sobre el modelo resultante, si este incluye la información relativa al vocabulario.

En nuestro caso particular, el modelado considerado se basa en el modelado de Markov, en el cual se incluye un vocabulario con las cadenas que pueden ser observadas en el proceso a modelar. Evidentemente, durante la experimentación, este vocabulario estará asociado con las pseudo-palabras del nuevo vocabulario. Sin embargo, una vez obtenido el modelo y estimadas las probabilidades de las pseudo-palabras, se puede obtener el modelo correspondiente a la traza original por parte del personal autorizado sin más que aplicar la función de reemplazo en el sentido inverso (Fig. 5) al vocabulario asociado al modelo. Evidentemente, tras esta restitución, el modelado resultante será idéntico al que se hubiese obtenido sin realizar el proceso de anonimización.

VI. Conclusiones

Difícilmente las empresas, operadores o instituciones pueden autorizar la colocación de un sensor a fin de obtener tráfico real por motivos de privacidad y seguridad. Sin embargo, en el contexto de la ingeniería de tráfico en general y de la detección de intrusiones en particular, resulta imprescindible contar con trazas de tráfico obtenidas de

entornos reales. Las técnicas de anonimización pueden utilizarse para preservar la privacidad de los datos, si bien las técnicas existentes se centran en la ocultación de los datos de las cabeceras. En este trabajo se ha descrito una técnica de anonimización orientada a la ocultación de la información contenida en las cargas útiles de determinados procotolos que, a su vez, permita deducir y analizar propiedades de dichas cargas útiles en relación a su posible uso en sistemas de detección de anomalías. La técnica descrita se basa en la sustitución de los elementos constitutivos de las cargas útiles que pueden contener información sensible por cadenas genéricas. De esta forma, siempre que la función de reemplazo permanezca confidencial, se pueden proporcionar las trazas de tráfico anonimizadas a los investigadores. Adicionalmente, en algunos casos es posible aplicar los resultados de los desarrollos que se realicen al poderse invertir la transformación.

AGRADECIMIENTOS

Este proyecto ha sido parcialmente financiado por el MICINN, a través del proyecto TEC2008-06663-C03-02.

Los autores desean expresar su agradecimiento a la Escuela de Estudios Profesionales Valle Hermoso dependiente de la Universidad Autónoma de Tamaulipas (Mexico) y, en particular, a Oscar Damián Gámez Maldonado por su colaboración en la adquisición de trazas de tráfico.

REFERENCIAS

[1] McHugh, J.; The 1998 Lincoln Laboratory IDS Evaluation. A critique; *Proc. RAID 2000*, LNCS vol. 1907, pp. 145-161, 2000.

[2] N. Athanasiades y otros; Intrusion detection testing and benchmarking methodologies; Proc. First IEEE International Workshop on Information Assurance, pp. 63-72, 2003.

[3] M. Bermúdez-Edo, R. Salazar-Hernández, J. Díaz-Verdejo, and P. García-Teodoro, "Proposals on Assessment Environments for Anomaly-Based Network Intrusion Detection Systems", *Proc. CRITIS 2006*, LNCS 4347, pp. 210 – 221, 2006.

[4] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", *Computers & Security*, vol. 28, pp. 18-28, 2009.

[5] J. Biskup, U. Flegel, On Pseudonymization of Audit Data for Intrusion Detection, *Proc. Int. workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability*, pp. 161-180, 2001.

[6] W. Yurcik y otros; Privacy/Analysis Tradeoffs in Sharing Anonymized Packet Traces: Single-Field Case; *Proc. of the 2008 Third Int. Conf. on Availability, Reliability and Security*, págs. 237-244, 2008.

[7] J. Estévez-Tapiador, P. García-Teodoro, J. Díaz-Verdejo; Detection Of Web-Based Attacks Through Markovian Protocol Parsing; *Proc. of the 10th IEEE Symposium on Computers and Communications (ISCC 2005);* pp. 457-462, 2005.

[8] W. Yurcik, C. Woolam, G. Hellings, L. Khan, B. Thuraisingham; Privacy/Analysis Tradeoffs in Sharing Anonymized Packet Traces: Single-Field Case; Proc. Third International Conference on Availability, Reliability and Security, pp. 237-244, 2008.

[9] G. Minshall; TCPdpriv Command Manual; http://ita.ee.lbl.gov/html/contrib/tcpdpriv.0.txt; 1996.

[10] D. Koukis , S. Antonatos , D. Antoniades , E. P. Markatos , P. Trimintzios; A Generic Anonymization Framework for Network Traffic; Proc. of the IEEE International Conference on Communications (ICC 2006), pp. 2302-2309, 2006.

[11] J. Estévez; Detección de intrusiones en redes basada en anomalías mediante técnicas de modelado de protocolos; Tesis Doctoral, Universidad de Granada, 2004.

[12] T. Berners-Lee, R. Fielding, H. Frystyk; "Hypertext Transfer Protocol -- HTTP/1.0", http://www.rfc.net/rfc1945.html

[13] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee, "Hypertext Transfer Protocol - HTTP/1.1", RFC 2068. January, 1997.

[14] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee; "Hypertext Transfer Protocol -- HTTP/1.1", http://www.ietf.org/rfc/rfc2616.txt

[15] T. Berners-Lee, R. Fielding, and L. Masinter, "Uniform Resource Identifiers". RFC 2396. August, 1998.

[16] M. Roesch; Snort – lightweight intrusion detection for networks; *Proc. 13th Conference on Systems Administration (LISA-99)*, 1999.

[17] V. Paxson; Bro: A System for Detecting Network Intruders in Real-Time; Comput. Networks, 1999.

[18] Leres y McCanne; tcpdump, Lawrence Berkeley National Laboratory; www.tcpdump.org.

VulneraNET: Técnicas para la resolución cooperativa de vulnerabilidades

David del Pozo*, Alberto Pastor*, Francisco J. Blanco† and Ana M. Vázquez‡
*División I+D+i
Germinus XXI (Grupo Gesfor)
Avenida Manoteras, 32
28050 Madrid
{dpozog,apastorm}@grupogesfor.com
†Departamento de Ingeniería de Servicios Telemáticos
Universidad Politécnica de Madrid
Avenida Complutense nº 30
28040 Madrid
fcojavibr@dit.upm.es
‡Departamento de informática
Universidad Carlos III de Madrid
Avenida Universidad, 30
28911 Leganés
amvazque@inf.uc3m.es

***Resumen*—Este artículo presenta el proyecto VulneraNET, que propone mejorar la seguridad de las aplicaciones web proporcionando herramientas a los desarroladores que les faciliten (i) comprobar la seguridad de las aplicaciones desarrolladas, (ii) corregir las vulnerabilidades detectadas de forma cooperativa y (iii) compartir el conocimiento de de seguridad de aplicaciones web. Con este fin, la plataforma VulneraNET emplea técnicas web 2.0 y semánticas para facilitar la detección, gestión y resolución de vulnerabilidades, con el fin de reducir el esfuerzo y tiempo de corrección de vulnerabilidades.**

Las herramientas de VulneraNET pueden ser utilizadas a diferentes niveles, de acuerdo a las personas involucradas en el proceso de desarrollo y pruebas de un proyecto (desarrolladores, jefes de proyecto y auditores de seguridad) y sin necesidad de tener amplios conocimientos en el área de la seguridad.

***Palabras Clave*—seguridad, vulnerabilidad, wiki semántico, google wave, wapiti, lapse**

I. Introducción

La seguridad es uno de los principios más importantes en las aplicaciones web, ya que están expuestas a los ataques de cualquier usuario malintencionado. En caso de producirse un ataque con éxito contra la aplicación web, la empresa propietaria de la misma puede perder información o ésta puede ser sustraída, comprometiendo gravemente la información de la empresa y de sus clientes. Todo esto desencadenaría numerosas pérdidas económicas, a la vez que un grave desprestigio y perdida de confianza por parte de sus clientes y del sector empresarial.

Un estudio del Instituto Nacional de Estándares y Tecnología de Estados Unidos estima que los errores informáticos causan unas pérdidas de 59,5 billones de dólares anualmente [1]. No todos los fallos pueden ser detectados, pero el mismo estudio afirma que una infraestructura de pruebas que asegure la identificación efectiva y temprana de los defectos del software podría ahorrar casi un tercio de dichas perdidas.

La seguridad, pese a todo, es deliberadamente descuidada por muchos desarrolladores. Se piensa que realizar pruebas de seguridad es un esfuerzo innecesario en un proyecto, ya que el cliente final no puede ver los resultados de una forma tangible. Además, las pruebas de seguridad resultan tediosas, se deben tener grandes conocimientos sobre la materia y se pierde demasiado tiempo para los ajustados plazos a los que se suelen comprometer los fabricantes de software.

La mayoría de herramientas actuales están centradas en realizar pruebas específicas de algún aspecto de seguridad en concreto, requieren la interacción humana para realizar las pruebas y el usuario debe tener conocimientos tanto de la herramienta como de seguridad para llevar las pruebas a cabo.

Basándose en estas premisas, el proyecto VulneraNET [3] innova en la seguridad mediante la creación de una herramienta colaborativa que facilita la predicción, detección y corrección de vulnerabilidades de aplicaciones y servicios web, abarcando todo el ciclo de vida, desde su desarrollo hasta su auditoría y corrección de fallos. La herramienta será desarrollada y distribuida como Software Abierto. La Internet del futuro abre nuevos horizontes, pero también nuevas amenazas si no se disponen de medidas de seguridad adecuadas. Hoy en día se puede ya hablar ciber-terroristas, por lo que es necesario investigar en técnicas y herramientas para que los ciber-policías puedan detectar, predecir y corregir dichas vulnerabilidades en tiempos muy cortos. Precisamente éste es el objetivo del proyecto, orientado a la prevención de la seguridad de sistemas de clientes por auditores de seguridad, y a comunidades de software abierto que se auto-protegen en un entorno hostil y lleno de atacantes potenciales como Internet. Un estudio reciente de vulnerabilidades arrojaba algunas cifras inquietantes [2]:

- una vulnerabilidad de un navegador web es explotada después de un día de que sea conocida en el 94 % de las veces en 2008, frente a un 79 % de 2007.
- en vulnerabilidades publicadas para un sistema operativo, se explota en el mismo día en el 80 % de las

publicadas en 2008, frente a un 70 % de 2007.

El proyecto VulneraNET automatiza las pruebas de seguridad con el objetivo de reducir el esfuerzo y el tiempo de corrección de una vulnerabilidad, ofreciendo un panel de control que aglutine las vulnerabilidades encontradas por las diferentes herramientas de seguridad que se integran en VulneraNET y muestre los resultados de una forma clara para un desarrollador que no tenga conocimientos de seguridad, de forma que sea posible identificar dónde se encuentra la vulnerabilidad para poder tomar las medidas necesarias para solventarla.

Para centralizar toda esta información VulneraNET hace uso de Google Wave [4], pudiendo tener un control de las vulnerabilidades y realizar una gestión y seguimiento de las mismas. La plataforma Google Wave además permite su comunicación con otros servicios y aplicaciones externas. Para que sea posible la intercomunicación de las herramientas el proyecto define un formato de intercambio mediante el cual se pueden comunicar las diferentes herramientas de seguridad que están integradas en el proyecto.

Además se pretende innovar mediante el uso de tecnologías web 2.0 y semánticas en el ámbito de la seguridad para poder obtener procedimientos de corrección de vulnerabilidades que faciliten al desarrollador su tarea. Para que el uso de estas tecnologías sea posible, el proyecto plantea la construcción de un wiki de seguridad y una red social en la que los desarrolladores podrán aportar el conocimiento a la aplicación. La red social podrá ser privada (empleados de la misma empresa auditando o desarrollando una aplicación) o pública (empleada por voluntarios que contribuyen a la detección y predicción de vulnerabilidades en software abierto). De esta forma, se aprovecha el conocimiento de los expertos en seguridad para que éste sea compartido entre los demás desarrolladores y se realiza una retroalimentación de los procesos de solución propuestos por el sistema para ir perfeccionando las soluciones a las distintas vulnerabilidades. VulneraNET además investigará el uso de un modelo reputacional para evaluar y calificar los diferentes componentes existentes a lo largo del proceso de resolución de vulnerabilidades mediante información obtenida de la red social e Internet, para ello se investigará en técnicas de extracción de datos y minería de opiniones.

II. Arquitectura de VulneraNET

VuneraNET provee un entorno colaborativo para la detección y resolución de vulnerabilidades de seguridad. Con este propósito, la arquitectura de VulneraNET (ver Fig. 1) se ha diseñado como un conjunto de herramientas que se comunican mediante un formato de intercambio de vulnerabilidades. Actualmente, VulneraNET investiga en herramientas para la detección de vulnerabilidades, tanto de caja negra (sección V) como de caja blanca (sección VI), y en herramientas de gestión del conocimiento de resolución de vulnerabilidades, como un wiki semántico (sección III). La interacción entre las diferentes personas involucradas en las pruebas y corrección de vulnerabilidades, se realiza mediante la plataforma colaborativa Google Wave (sección IV), que permite la colaboración tanto en la notificación de vulnerabilidades, ejecución de pruebas, asignación social de vulnerabilidades pendientes y gestión del conocimiento corporativo.

El formato definido para el intercambio de información en VulneraNET posibilita la integración sencilla de nuevas herramientas en la plataforma. Este formato contiene información detallada sobre una vulnerabilidad como puede ser el tipo, fecha de detección, persona o aplicación que la encontró, posibles soluciones, gravedad, estado, etc. VulneraNET integra las diferentes herramientas a través de dicho formato, pudiendo generar a partir de él informes de vulnerabilidades y trasferir información a las demás herramientas de plataforma.

Dentro del proyecto VulneraNET se está investigando en los dos principales enfoques de detección de vulnerabilidades en aplicaciones web, las pruebas de caja blanca y las pruebas de caja negra, los estudios realizados sobre estas técnicas se están materializado en herramientas de seguridad que están siendo evolucionadas para la inclusión de las técnicas de detección estudiadas y que finalmente serán integradas en la plataforma (la herramienta Wapiti (sección V-A) en el caso de caja negra y LAPSE+ (sección VI-A) en el caso de caja blanca).

Por otra parte, VulneraNET también reúne diferentes herramientas de resolución de vulnerabilidades como la red social de profesionales de seguridad, el wiki semántico (sección III) que recoge información sobre vulnerabilidades, incluyendo procesos de resolución de vulnerabilidades y Google Wave (sección IV), que permite la comunicación de diferentes participantes en un proyecto para hacer más sencillo el proceso de resolución de vulnerabilidades. Google Wave además contiene el panel de control que permite ver de forma clara las vulnerabilidades encontradas en una aplicación web sobre la que se hagan las pruebas, generar informes y realizar el seguimiento de las vulnerabilidades. La integración con Google Wave para facilitar la cooperación entre usuarios se detalla en la sección IV-A.

Como se comentó anteriormente el proyecto está enfocado a las diferentes personas que trabajan en la seguridad informática, tanto los auditores de seguridad como los desarrolladores que se encargan de corregir los bugs. Las herramientas pueden ser utilizadas conjuntamente o por separado, con lo que hace más flexible su uso. Sin embargo, la ventaja diferencial de este proyecto radica en usar las herramientas en conjunto para la perfecta gestión de conocimiento de los diferentes profesionales que desarrollan las actividades de seguridad de una aplicación web.

III. Wiki semántico

Un objetivo principal del proyecto VulneraNET es la investigación de mejoras en la gestión del conocimiento de consultoría de seguridad mediante la aplicación de técnicas de etiquetado social para procesos y vulnerabilidades. Para llevar a cabo esta investigación se ha definido una herramienta colaborativa de resolución de incidencias, donde se tratará de validar el uso de redes sociales para facilitar la auditoría de seguridad de un equipo de auditores y mejorar la comunicación con el equipo de desarrollo [31]. La capacidad organizativa de los portales que implementan los conceptos wiki y wiki semántico, así como su facilidad de creación de comunidades muy activas y abiertas con una enorme capacidad de generación y edición de contenidos, unido a su gran impacto en la red de redes, los convierten en una aplicación idónea para el objeto de estudio [27].

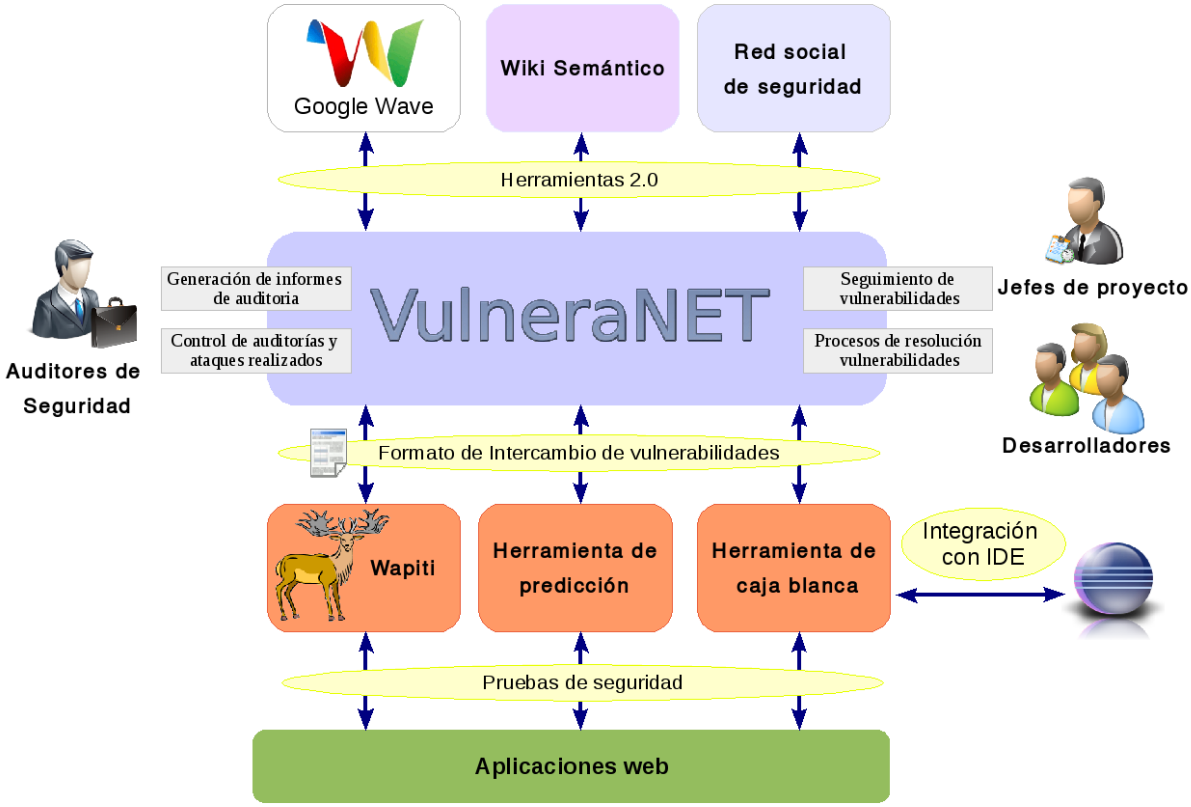


Figura 1. Visión general de VulneraNET

Así, wiki podría definirse como un concepto de aplicación Web cuyas páginas pueden ser editadas por múltiples voluntarios a través de un navegador, permitiendo a los diferentes usuarios de la aplicación crear, modificar o borrar información compartida. Cada página de un wiki se identifica por un título unívoco, al señalar dicho título con dos corchetes en cualquier lugar del wiki se crea automáticamente un enlace a dicha página, creando una estructura global de páginas que permite a los usuarios saltar de unas a otras a través de tales referencias [28]. Con estas sencillas reglas se construye un portal con gran capacidad organizativa, permitiendo a la comunidad compartir grandes cantidades de información, depurarla y enriquecerla continuamente. La principal utilidad de un wiki es que permite crear y mejorar las páginas de forma instantánea, dando gran libertad al usuario con una interfaz muy simple. Con un clic, un usuario puede empezar a editar una página y con otro clic, guardarla para que el resto de usuarios puedan cargarla de forma inmediata con los cambios realizados. Esto hace que un número considerable de usuarios participe en su edición, a diferencia de los sistemas tradicionales donde resulta más difícil que los usuarios del sitio contribuyan a mejorarlo.

El wiki software es un programa que permite ejecutar una aplicación Web basada en el concepto wiki. Existen diferentes versiones de software wiki, la mayoría de ellos son software libre y de código abierto. Es común que estos sean modulares, proporcionando APIs que permiten a los programadores desarrollar nuevas mejoras para la aplicación sin necesidad de familiarizarse con el código base. De los software wiki más populares se pueden destacar los siguientes Foswiki, MoinMoin, TikiWiki, XWiki, DokuWiki y MediaWiki, este último es el que se ha usado.

Existe una visión innovadora del concepto wiki que explota su capacidad organizativa por medio de conceptos de la Web semántica, llamado wiki semántico [29]. Un wiki semántico nace de la implementación de un modelo de conocimiento en el concepto wiki. Los wikis semánticos, a diferencia de las aplicaciones wiki, proporcionan la capacidad de formalizar la información acerca de los datos almacenados en sus páginas Web y establecer una jerarquía de relaciones entre estas, de forma que la información contenida en la aplicación puede ser exportada o consultada como una base de datos, aplicando el modelo de Entidad-Relación [22] [24].

Las tecnologías semánticas permiten proveer de una nueva dimensión de conocimiento a la información, posibilitando la integración y estandarización de conocimiento sobre las aplicaciones o recursos a aplicar la seguridad modelando el significado a los términos y conceptos necesarios [30]. Por lo tanto, esta nueva visión constituye una mejora notable a la hora de trabajar con la información contenida en la aplicación Web por medio de agentes software externos, facilitando la automatización del procesado de la información añadida al wiki y el intercambio de dicha información. La formalización de los términos incluidos en el wiki permite a estos agentes procesar la información de forma automática, evitando los tediosos procesos de parseado, minería e identificación del texto plano extraído de una página Web. Los usuarios que colaboran en un wiki suelen ser muy heterogéneos debido a las características del wiki de apertura y facilidad formándose grandes comunidades donde los contenidos aportados se van enriqueciendo debido a la diversidad de tales usuarios.

El problema radica en que tal heterogeneidad hace que

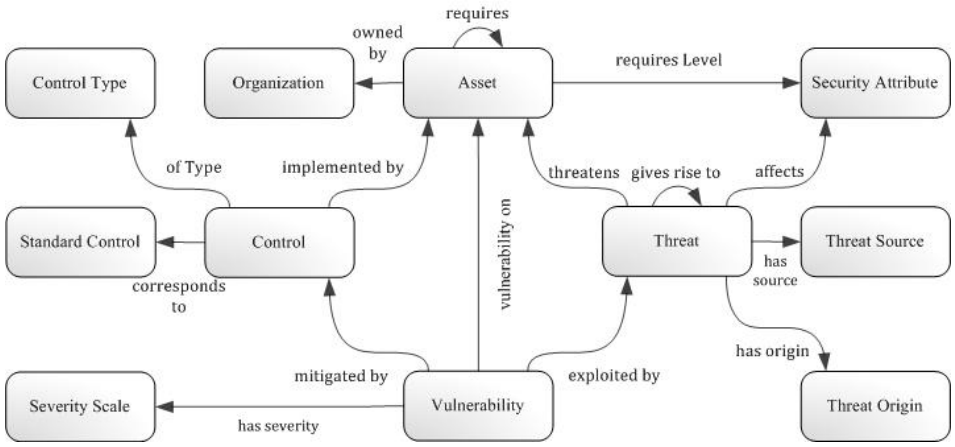


Figura 2. Ontología utilizada en VulneraNET

cada contenido difiera en demasía con los otros, incluso los más similares, ya que los usuarios no siguen ningún patrón, ni terminología, ni estructura en común. Esto es una de las cuestiones principales que intenta abordar la aplicación de wikis semánticos, añadiendo el uso de una estructura que formalice la creación y edición de contenidos en todo el wiki. El principal método por el que se genera una estructura formalizada es la inclusión de ontologías. En el área de la seguridad informática, el uso de ontologías de seguridad [26] [20] [23] provee de las siguientes capacidades:

- **Expresividad.** Una ontología y la cantidad de tecnologías subyacentes son capaces de describir cualquier clase de concepto y las relaciones entre ellos. Estos conceptos y sus propiedades quedarán jerarquizados formando una taxonomía y se les podrá asociar restricciones a éstos y a sus relaciones.
- **Organización.** Permite organizar el conocimiento, separa los requisitos de seguridad de su implementación técnica facilitando la gestión de la seguridad y el desarrollo y posterior acceso al modelo de seguridad ya que el sistema se realiza en dos fases: desarrollo del modelo sin tener en cuenta los elementos específicos y después la instanciación de dichos elementos. La ontología organiza y sistematiza cualquier tipo de fenómeno a cualquier nivel de detalle, reduciendo la lista de items a una lista de propiedades.
- **Mecanismos de formalización y compartición del conocimiento.** La falta de conocimiento explícito compartido en general en toda la ingeniería del software presenta una gran dificultad que repercute en gasto innecesario de tiempo y esfuerzo. La integración del conocimiento, su soporte automático y la posibilidad de su comunicación entre los agentes (humanos o software) disminuye la ambigüedad del lenguaje que frecuentemente lleva a errores, falta de entendimiento y realización de esfuerzos improductivos. Gracias a esta compartición y transmisión de la información se mitiga completamente la posible diferencia de conocimiento entre los miembros sobre el dominio del problema.
- **Inferencia lógica.** El procesamiento y análisis de las ontologías hace posible una capa lógica donde por ejemplo se pueden dibujar conclusiones o conseguir nueva información por la combinación de toda la información. La información implícita es hecha explícita gracias a la capacidad de las ontologías de razonar a través de un motor de inferencias.
- **Extensibilidad y reutilización.** Una ontología es siempre reutilizable pues se abstrae de los elementos específicos del sistema definiéndolos a través de conceptos y propiedades, esto supone escalabilidad pues con la misma ontología se pueden definir diez que cien elementos, lo único que se necesita es una instancia para cada uno. La idea es no empezar nunca de cero sino usar ontologías completas ya publicadas conteniendo la mayoría de los conceptos que se manejan en esa área específica. Una ontología es fácilmente modificable y ampliable de forma dinámica.
- **Interoperabilidad.** La capacidad que tienen las ontologías para especificar comportamientos sobre los objetos que representan los recursos y el manejo de conceptos comunes hace muy sencillo el intercambio de información entre entornos y aplicaciones heterogéneas. Gracias a la integración semántica y a la definición del comportamiento de los diferentes agentes mediante ontologías puede lograrse una capacidad de operar conjuntamente.

Concretamente, el empleo de ontologías en el proyecto VulneraNET está enfocado en la gestión de seguridad por medio de agentes inteligentes especificando el modo en que dichos agentes cooperan entre sí. La coordinación de estos agentes con la información especificada y compartida por parte de los diferentes usuarios que conforman el grupo de trabajo (auditores, analistas de seguridad, equipo de desarrollo, usuarios de la Web) lleva a emplear técnicas semánticas que permiten automatizar el proceso, disminuyendo la necesidad del componente humano en un proceso complicado y tedioso como es la monitorización de las incidencias de seguridad en tiempo real y el seguimiento de su resolución a lo largo de su ciclo para cada vulnerabilidad detectada. Además la utilización de ontologías permite la formalización del vocabulario de ataques, vulnerabilidades y demás componentes que toman parte en el seguimiento de incidencias en el campo de la seguridad de una aplicación Web, permitiendo también formalizar el proceso mismo del seguimiento de la incidencia

(ver figura 2).

La formalización de los términos anteriormente citados (Vulnerabilidades, amenazas, activos, procesos, etc.) permiten facilitar la gestión de la información de vulnerabilidades y amenazas que afectan a una aplicación Web dada. En este caso el uso de técnicas semánticas facilita a los agentes software la traducción de la información compartida por los usuarios de la aplicación, detectada por cualquiera de los módulos de detección de seguridad (análisis de código, análisis de trafico, etc.) y/o exportada a la base de datos desde un sitio externo a un formato de intercambio de vulnerabilidades de seguridad. La información puesta en este formato podrá ser entonces intercambiada entre los módulos del suit de seguridad o entre diferentes suites o programas de seguridad, así como entre diferentes aplicaciones Web dedicadas a la publicación de incidencias de seguridad.

Una última utilidad que cabe reseñar es el seguimiento en la edición de cada página y, por lo tanto, el seguimiento de cada concepto añadido al wiki. Así asociada a cada página existe otra página donde se puede discutir, criticar o realizar comentarios sobre los contenidos expuestos, las ediciones o actualizaciones realizadas, la adecuación o completitud de la información escrita o, por ejemplo, orientar sobre el contenido que queda por meter.

En la búsqueda de una herramienta colaborativa de resolución de incidencias esta perspectiva es idónea pues en las páginas de contenidos se tendrá toda la información de relevancia, con los datos técnicos, que se irán modificando, enriqueciendo y actualizando en un ambiente colaborativo a medida que los usuarios vayan accediendo y el proceso de resolución de la incidencia vaya avanzando. Al mismo tiempo en las páginas de discusión se realizarán los comentarios y críticas pertinentes a los contenidos, pudiendo especificar a los usuarios responsables que realizaron tales cambios o que serán los encargados de realizar las modificaciones. Para ello, la discusión será dividida en una lista organizada de entradas, cada una de las cuales expone una actividad a realizar sobre los contenidos y exponiendo las tareas hechas para llevar a cabo dicha actividad, especificando el usuario responsable de la tarea. Esta forma de gestionar los contenidos permite tener las dos áreas perfectamente separadas: la exposición del contenido técnico frente a las posibles discusiones, adecuándose ambas a un ambiente colaborativo.

IV. Google Wave

VulneraNET utiliza Google Wave [4] como herramienta colaborativa para la participación de los diferentes usuarios en la visualización de las vulnerabilidades de forma centralizada utilizando todas las ventajas que la plataforma provee.

Google Wave es una herramienta on-line de comunicación y colaboración en tiempo real. Cada conversación se conoce como *wave* u *ola* y se compone de diferentes mensajes que puede ser tanto una conversación como un documento, y en ellos los usuarios pueden participar y trabajar juntos usando texto formateado, fotos, vídeos, mapas, *widgets*, etc. Además, permite una participación activa por parte de los usuarios de la *ola*. Cualquier participante puede editar, responder o comentar algo en cualquier parte del mensaje, las respuestas se pueden publicar entre medias de otras, como respuesta concreta de una (creando subniveles de respuesta) o dentro de otra respuesta, además de poder privatizarla para elegir que usuarios pueden leerla. Google Wave permite a los usuarios acceder al historial de la ola, pudiendo ver de forma cronológica la evolución de la conversación.

Google Wave proporciona un API que permite utilizar y mejorar sus servicios a través de inserciones y extensiones. Las inserciones permiten introducir las olas de Google Wave en aplicaciones web externas. Las extensiones permiten mejorar las prestaciones y servicios que provee Google Wave mediante el uso de robots, que se comportan con un participante más de la ola y permiten automatizar ciertos comportamientos, y mediante el uso de *gadgets*, que están orientados a aumentar la experiencia de colaboración, permitiendo interactuar a los usuarios de nuevas formas a las que ya provee de forma básica Google Wave.

IV-A. Extensión de Google Wave para VulneraNET

En esta sección se mostrará un caso práctico de uso de VulneraNET. Dentro de el entorno de Google Wave se ha implementado una extensión en forma de robot [19]. Los robots dentro de Google Wave tienen el aspecto de un usuario normal y pueden participar en una conversación y modificar el contenido de la misma. Este robot permite al usuario obtener un informe con estadísticas e información que muestra de forma gráfica distintas vulnerabilidades, utilizando un fichero XML con vulnerabilidades generado por Wapiti como fichero de entrada.

Para poder ejecutar el robot en Google Wave lo primero que hay que hacer es añadirlo a la lista de contactos (su dirección es vulneranet@appspot.com). A continuación basta con incluirlo como participante en una *wave* para que se ejecute automáticamente, entonces aparecerá un formulario en el mensaje inicial de esa conversación con un campo de entrada de texto en el que indicar la URL del fichero con el informe de Wapiti en XML y una casilla de verificación que permite al usuario presentar el informe en un solo mensaje dentro del *wave* o en varios (modo múltiple, una vulnerabilidad por mensaje).

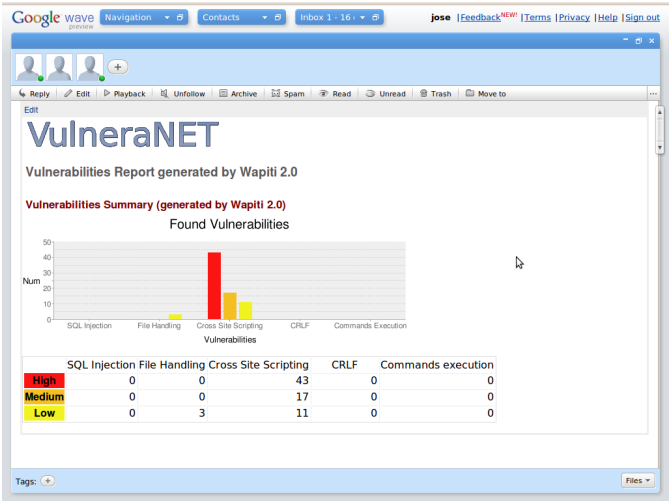


Figura 3. Informe dentro de Google Wave

En este ejemplo el informe aparece en el modo múltiple, con un mensaje introductorio y uno por cada riesgo que

incluye el fichero de entrada. El usuario podrá interactuar sobre cada vulnerabilidad usando directamente las opciones que Google Wave proporciona, por ejemplo, el usuario podrá: responder directamente sobre el mensaje en el que esté descrita esa vulnerabilidad para poner un comentario, crear una nueva wave con esa vulnerabilidad para poder interactuar de forma independiente al *wave* actual, editar la información que aparece sobre la vulnerabilidad, etc.

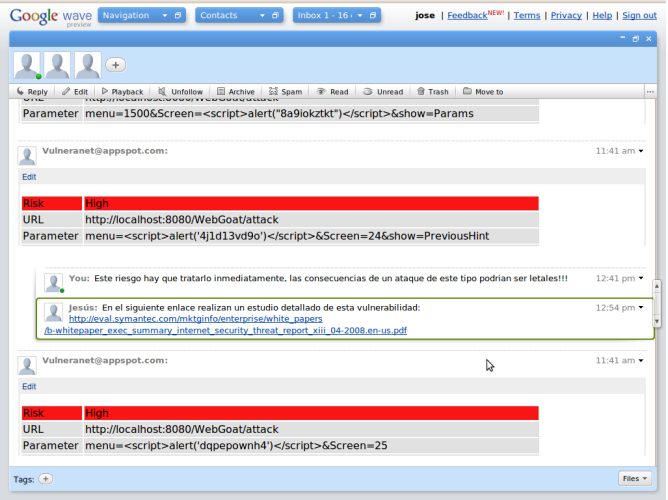


Figura 4. Usuarios interactuando con el informe

V. Enfoque de detección de vulnerabilidades de caja negra

Las técnicas de detección de vulnerabilidades de caja negra se basan en realizar ataques de la misma forma que un atacante real para poder descubrir las vulnerabilidades de una aplicación.

Existen diferentes técnicas basadas en este principio, el enfoque más utilizado, por ser el más eficiente, es el de la auditoría manual utilizando un *proxy* entre el servidor donde se encuentra la aplicación a evaluar y el navegador del auditor. Éste intercepta las peticiones y las respuestas del servidor y las manipula de forma manual con el fin de encontrar vulnerabilidades. Este enfoque permite descubrir todo tipo de vulnerabilidades, pero su éxito se basa en la pericia del auditor ya que para poder realizar este tipo de pruebas, son necesarios unos amplios conocimientos de seguridad [5].

Una de las herramientas más destacables que siguen este enfoque es WebScarab [6]. Esta herramienta desarrollada por la Fundación OWASP [8], permite realizar análisis de seguridad sobre aplicaciones que se comunican a través de los protocolos HTTP. Es una herramienta modular y puede ser extendida añadiendo *plugins*. Dispone de varios modos de operación, pero el más común es el de *proxy* entre la conexión y el navegador. Un auditor de seguridad puede revisar y modificar las respuestas desde el servidor hasta el navegador. Esta aplicación está orientada a personas que están familiarizadas con el protocolo HTTP y que tienen conocimientos amplios en el área de seguridad. La principal forma de trabajo con esta herramienta es prácticamente manual, requiere la intervención del usuario, aunque también dispone de funcionalidades automatizadas.

Otro enfoque muy utilizado es el *fuzzing*, técnica que consiste en inyectar una colección de cadenas maliciosas en las entradas de la aplicación que se desea probar, evaluando la respuesta obtenida. La gran ventaja de esta técnica es que puede detectar la mayoría de las vulnerabilidades relacionadas con inyecciones de código (XSS, inyecciones SQL, etc.), siendo éstas las más comunes según el Top 10 de vulnerabilidades de OWASP [7]. A diferencia de la anterior, esta técnica se puede automatizar. Lo normal es integrarla dentro de un proceso de auditoría manual puesto que evita realizar tareas muy repetitivas. Sin embargo, la evaluación de las respuestas de forma manual es mucho más exhaustiva que la automatizada, ya que ésta no es capaz de detectar muchas respuestas como vulnerables [5].

V-A. *OWASP Wapiti*

En este apartado se muestra la herramienta OWASP Wapiti,la cual se ha integrado dentro de VulneraNET. OWASP Wapiti [9] es un proyecto de código abierto liderado por Nicolas Surribas y Grupo Gesfor. La herramienta Wapiti utiliza técnicas de *fuzzing* para realizar los ataques y descubrir las vulnerabilidades. Wapiti no inyecta un grupo predefinido de cadenas maliciosas, sino cadenas generadas dinámicamente, de esta forma se evitan muchos falsos positivos. Permite auditar la seguridad de aplicaciones web de una forma automática y sencilla. La ventaja que tiene Wapiti respecto a otras herramientas del mismo estilo es que realiza el escaneo del sitio web sin la necesidad de la intervención del usuario. Las vulnerabilidades que es capaz de detectar son errores de manejo de ficheros, inyecciones de bases de datos, inyecciones XSS, inyecciones LDAP, inyecciones CRLF y de ejecución de comandos.

Wapiti puede ser fácilmente extendido para incluir nuevos tipos de ataque gracias a su arquitectura modular, cada ataque es implementado como un módulo independiente del resto. Wapiti también permite la configuración de *cadenas de texto maliciosas* que puede ser insertadas en los ataques existentes para expandirlos. Wapiti además genera informes con las vulnerabilidades encontradas que pueden ser exportados a diferentes formatos: HTML, XML y texto plano. Los informes están orientados a programadores y desarrolladores, un público que normalmente no tiene grandes conocimientos de seguridad, ya que proporcionan información sencilla y concisa sobre las vulnerabilidades para que éstas puedan ser resueltas.

OWASP (Open Web Application Security Project), una de las organizaciones sin animo de lucro más importante en el ámbito de la seguridad informática, ha reconocido la utilidad de esta herramienta incluyéndola como proyecto OWASP Alpha y distribuyendo Wapiti en la distribución GNU/Linux de seguridad OWASP Live CD [10]. Además, la herramienta OWASP Wapiti ha sido recientemente incluida en la distribución Backtrack [11]. BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general que goza de gran popularidad y aceptación.

Wapiti será evolucionado dentro de VulneraNET para la detección de errores de seguridad con AJAX y posteriormente integrado en VulneraNET gracias al formato de intercambio. La tecnología AJAX (Asynchronous JavaScript and XML),

está siendo usada cada vez más para crear aplicaciones web pues ofrece enormes beneficios de usabilidad para el usuario fin. Sin embargo, desde un punto de vista de seguridad estas aplicaciones tienen más problemas que una aplicación web convencional debido a que poseen una superficie de ataque mayor que las aplicaciones web normales (el número de entradas a la aplicación crece), tienen funciones internas expuestas como servicio y en ocasiones acceden desde la parte cliente a recursos sin mecanismos de codificación o seguridad.

VI. Enfoque de detección de vulnerabilidades de caja blanca

Las técnicas de detección de vulnerabilidades de caja blanca se basan en el análisis de código fuente. La aplicación de estas técnicas forma parte del desarrollo software donde los propios programadores someten a revisión el código que han generado para descubrir los problemas e inconsistencias que este contiene antes de su compilación. Aunque estas comprobaciones pueden ser realizadas por una persona, es habitual que esta tarea se automatice utilizando herramientas específicas que son capaces de analizar el programa completo. Las herramientas de análisis estático de código recorren el código fuente de un programa y automáticamente detectan errores y vulnerabilidades que no son advertidos normalmente por los compiladores y que posteriormente pueden suponer grandes problemas. Este tipo de procesos permiten resultados más exhaustivos que los realizados mediante pruebas de caja negra aunque ello también conlleva que, en proyectos de elevado tamaño, la dimensión del análisis puede suponer una labor ingente.

En la actualidad es posible encontrar diferentes propuestas orientadas al análisis estático. Algunas de ellas simplemente hacen un análisis semántico del código, comparando partes de éste con una biblioteca de vulnerabilidades conocidas como Flawfinder [12] o ITS4 [13]. Con diferencia, las propuestas más potentes para detección y localización de vulnerabilidades pasan por el análisis de flujo de datos. La técnica de análisis estático basado en el flujo de datos, construye un grafo de control del flujo que sirve para determinar las posibles propagaciones de datos manipulados de forma malintencionada hasta los puntos vulnerables del programa. Un ejemplo de este tipo de análisis es el propuesto por la Universidad Tecnológica de Viena denominado Pixy [14]. Una estrategia similar emplea la propuesta de la Universidad de Stanford, el llamado análisis de punteros (Points-to analysis) [15], en el que se obtienen los caminos por los que los datos manipulados pueden llegar hasta partes vulnerables del programa. Los esquemas basados en análisis de flujos y punteros pueden presentar la aparición de falsos positivos, sentencias de código identificadas por el proceso como potencialmente peligrosas, que en realidad no lo son. Por ello, son cada vez más habituales el empleo de técnicas sensibles al contexto que reducen el número de falsos positivos con respecto a otros esquemas.

VI-A. LAPSE+

LAPSE (Lightweight Analysis for Program Security in Eclipse) [16] es una herramienta para realizar la auditoría de seguridad en las aplicaciones Java y forma parte del proyecto *Griffin Software Security Project* [17] de la Universidad de Stanford. El analizador se distribuye como un plug-in de Eclipse [18] permitiendo mostrar, mediante vistas específicas, en qué parte del programa se da la vulnerabilidad de seguridad. LAPSE tiene como objetivo encontrar las vulnerabilidades de seguridad en las aplicaciones Web causadas por inadecuada o nula validación de las entradas del usuario. La implementación actual de LAPSE no constituye una de las herramientas más eficientes, los resultados documentados por sus desarrolladores muestran que algunos errores no se llegan a detectar y aparecen falsos positivos como resultado del análisis. Sin embargo, los autores de LAPSE proponen un análisis más completo, basado en punteros y al contexto como una futura mejora. Este análisis utiliza el lenguaje PQL para las vulnerabilidades en una sintaxis parecida a Java. Posteriormente las vulnerabilidades así definidas se traducen a un lenguaje lógico Datalog y se resuelven en una base de datos especifica. Este análisis a pesar de ser mucho más completo, es difícil de utilizar ya que no se integra bien en el entorno de desarrollo Eclipse.

Dadas las deficiencias presentes en el desarrollo LAPSE y basándose en la mejoras propuestas por los propios creadores se pretende la implementación de una nueva versión del plug-in de Eclipse, LAPSE+. Esta nueva herramienta tendrá en cuenta las vulnerabilidades en aplicaciones web cuyo origen se basa en la entrada de datos de usuario que no se valida de forma adecuada antes de ser utilizada por la aplicación, problema definido por el grupo SUIF como *tainted object propagation problem* (propagación de objetos envenenados). Como resultado, LAPSE+ constituirá una herramienta para la detección de las vulnerabilidades de seguridad en el código Java, teniendo en cuenta las vulnerabilidades más recientes en las aplicaciones web.

VII. Conclusiones

En este trabajo de investigación se ha presentado el proyecto VuneraNET, basado en herramientas y procesos colaborativos de detección, predicción y corrección de vulnerabilidades de aplicaciones web para desarrolladores y auditores de seguridad. Esta combinación e integración de herramientas de detección y resolución produce una sinergia que disminuye radicalmente el tiempo de corrección de vulnerabilidades.

VulneraNET permite aumentar la productividad, mediante la reducción del tiempo de detección y corrección de vulnerabilidades gracias a las herramientas de detección de vulnerabilidades y al entorno colaborativo de trabajo en el cual se enmarca este proyecto, que permite gestionar de forma eficiente el conocimiento de seguridad de todas la personas involucradas en el desarrollo y pruebas de un proyecto informático.

Agradecimientos

Este proyecto ha sido cofinanciado por el Ministerio de Industria, Turismo y Comercio, dentro de la convocatoria del subprograma Avanza I+D, dentro de la prioridad temática de Internet del futuro y como Proyecto Tractor de Investigación Industrial y Desarrollo Experimental en Cooperación (TSI-020302-2009-64).

Referencias

[1] Chen, H., Zou, T., and Wang, D. Data-flow based vulnerability analysis and java bytecode. In 7th Conference on 7th WSEAS international Conference on Applied Computer, 2007

[2] Internet Security Systems X-Force support. Disponible en http://www.usatoday.com/tech/news/computersecurity/2008-07-29-internet-threats-f aster_N.htm
[3] Sitio web de VulneraNET, http://vulneranet.grupogesfor.com
[4] Google Wave, http://wave.google.com/about.html
[5] Guia de test de OWASP v.3, http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
[6] Sitio web del proyecto OWASP WebScarab, http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
[7] OWASP Top 10, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[8] Sitio del proyecto OWASP, http://owasp.org
[9] Sitio web de Wapiti, http://www.ict-romulus.eu/web/wapiti
[10] Distribucion GNU/Linux OWASP Live CD: http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project
[11] Distribución Linux de seguridad Backtrack, http://www.backtrack-linux.org
[12] Sitio web de Flawfinder, http://www.dwheeler.com/flawfinder
[13] Sitio web de ITS4, http://www.cigital.com/its4/
[14] Jovanovic, N., Kruegel, C., and Kirda, E. Pixy: a static analysis tool for detecting Web application vulnerabilities. Security and Privacy, IEEE 2006
[15] Livshits, V. B. and Lam, M. S. Finding security vulnerabilities in java applications with static analysis. USENIX Security Symposium, 2005
[16] Sitio Web LAPSE, http://suif.stanford.edu/ livshits/work/lapse/
[17] Sitio Web Griffin Software Security Project, http://suif.stanford.edu/ livshits/work/griffin/
[18] SitioWeb Eclipse, http://www.eclipse.org/
[19] Robot de Google Wave de VulneraNET, http://vulneranet.grupogesfor.com/google-wave
[20] Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A., & Piattini, M. (2007). Revisión sistemática y comparación de ontologías en el marco de la seguridad Paper presented at the IV Congreso Iberoamericano de Seguridad Informática (CIBSI 07), Mar Del Plata. Argentina.
[21] Eyal Oren. SemperWiki: a semantic personal Wiki. In Proceedings of the Workshop on Semantic Desktop. Workshop at 4th International Semantic Web Conference (ISWC 2005), Galway, Ireland, 2005.
[22] Eyal Oren, Max Völkel, John Breslin, Stefan Decker. Semantic Wikis for Personal Knowledge Management. In Proceedings of the 17th International Conference on Database and Expert Systems Applications Krakow, Poland, 2006
[23] Bill TSOUMAS, Dimitris GRITZALIS, "Towards an Ontology-based Security Management,.Advanced Information Networking and Applications, International Conference on, pp. 985-992, 20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06), 2006
[24] Max Völkel, Eyal Oren. Towards a Wiki Interchange Format (WIF) -Opening Semantic Wiki Content and Metadata. In Proceedings of the Workshop on SemWiki. Workshop at ESWC, 2006.
[25] Artem Vorobiev and Jun Han, "Security Attack Ontology for Web Services", in Proceedings of the Second International Conference on Semantics, Knowledge, and Grid (SKG'06), IEEE Computer Society, 2006.
[26] J. Undercoffer, A. Joshi and J. Pinkston. Modeling Computer Attacks: An Ontology for Intrusion Detection. University of Maryland, Baltimore County. Department of Computer Science and Electrical Engineering, 2003.
[27] Buffa, M., Gandon, F., Ereteo, G., Sander, P., and Faron, C: SweetWiki: A semantic wiki. Web Semant., vol 6, no. 3, pages 84-97, year 2008.
[28] Ye, Shiren and Chua, Tat-Seng and Lu, Jie: Summarizing definition from Wikipedia. ACL-IJCNLP '09: Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP, vol 1, pages 199-207, year 2009.
[29] Schaffert, S., Bry, F., Baumeister, J. and Kiesel, M.: Semantic Wikis. IEEE Softw., vol. 25, no. 4, pages 8-11, year 2008.
[30] Panagiotou, D. and Mentzas, G.: Exploiting Semantics in Collaborative Software Development Tasks. Proceeding of the 2008 conference on Knowledge-Based Software Engineering, pages 385-394, year 2008.
[31] Xiao, WenPeng and Chi, ChangYan and Yang, Min: On-line collaborative software development via wiki. WikiSym '07: Proceedings of the 2007 international symposium on Wikis, pages 177-183, year 2007.

Estudio del impacto energético del códec en aplicaciones VoIP en entornos WiFi

Jorge López Gallardo, Juan M. Vozmediano Torres, Antonio Estepa Alonso, Rafael Estepa Alonso.
Área de Ingeniería Telemática
Universidad de Sevilla
C/ Camino de los Descubrimientos s/n
jorge.lopez@descalzos.es, {jvt,aestepa,rafa}@trajano.us.es.

***Abstract*—En las aplicaciones de VoIP es común que el usuario seleccione el códec de audio que mejor se adapte a sus necesidades y ello puede tener implicaciones en el consumo de energía cuando se utilizan dispositivos móviles.**

En este artículo se presentan los resultados de un estudio realizado para caracterizar el consumo energético en las aplicaciones de VoIP. En particular se analiza cómo el códec seleccionado influye en el consumo energético del dispositivo móvil. Los resultados muestran que, en caso de usar el modo de ahorro de energía en el interfaz WiFi, el códec seleccionado influye significativamente en el consumo de energía y que, por lo tanto, el aspecto energético debería ser tenido en cuenta junto a otros como el caudal mínimo o la calidad a la hora de seleccionar un códec.

***Index Terms*—Energía, códecs, VoIP, 802.11**

I. Introducción

Los dispositivos móviles orientados al mercado residencial capaces de conectarse a redes WiFi (teléfonos móviles, ordenadores portátiles y agendas electrónicas) han experiementado un fuerte crecimiento en los últimos años. Los factores que han contribuido a este éxito son tanto tecnológicos (cada vez más recursos en menos espacio) como económicos (abaratamiento de los precios).

Los dispositivos citados ven limitada su autonomía por la duración de su batería. El consumo energético de los dispositivos móviles depende tanto de los circuitos que los componen como del uso que de éstos hacen los diferentes procesos de aplicación en ejecución. Así, parece haber consenso en cuanto al reparto del gasto de batería imputable a los diferentes componentes de la circuitería, tal y como refleja la Figura 1.

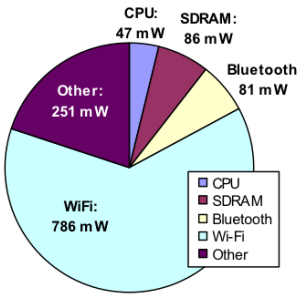


Fig. 1. Componentes del consumo energético en dispositivos móviles [1]

La fracción dominante del gasto energético corresponde a la interfaz WiFi, por lo que habitualmente se ignora el consumo debido a las aplicaciones en el gasto total. Estudios recientes sobre el consumo de la interfaz WiFi [2]–[4] indican que el uso del modo de ahorro de energía o PSM (*Power Saving Mode*), que reemplaza la mayor parte de la permanencia en estado ocioso (*idle*) por el estado durmiente (*sleep*), permitiría considerables economías en el consumo. Esta situación modifica el balance energético, obligando a revisar la importancia relativa del gasto en las citadas aplicaciones frente a la interfaz WiFi.

Por otra parte, el uso cada vez más habitual de los dispositivos móviles para la ejecución de aplicaciones multimedia aconseja estudiar la influencia de este tipo de aplicaciones en el consumo energético del dispositivo. Aunque existen medidas sobre el consumo de aplicaciones de *streaming* de audio/vídeo [5], [6], son escasos los estudios sobre el consumo de las aplicacionesde VoIP [2], [7]. Además, las aplicaciones de VoIP suelen dejar a la libre elección del usuario ciertos parámetros de configuración, entre ellos el códec a utilizar. Por ello parece igualmente interesante la realización de un estudio que caracterice la influencia del códec en el consumo de energía.

El objetivo de este trabajo es presentar un estudio del impacto energético de las aplicaciones de VoIP en los dispositivos móviles. Más específicamente, el objetivo de este artículo es comparar el consumo atribuible a cada uno de los códecs de uso común en las aplicaciones de VoIP, tanto en situaciones normales como ante el uso del modo *PSM*. Esto permitirá valorar el impacto energético como un parámetro más al seleccionar códec adecuado para cada situación.

La organización del resto del artículo es la siguiente. En la sección II se ofrece un breve resumen sobre las principales características de los códecs bajo estudio en el presente trabajo. La sección III introduce las características más relevantes del modo de ahorro de energía, así como la relación entre el estado de la interfaz WiFi y el del códec VoIP. La sección IV realiza un breve análisis sobre la influencia que tienen los códecs en los diferentes componentes con impacto en el consumo. La sección V explica el experimento realizado para la medición de los recursos consumidos por los códecs bajo estudio. Las secciones VI y VII presentan los resultados obtenidos y, finalmente, la sección VIII ofrece las conclusiones principales y las futuras líneas de avance.

II. Resumen de códecs de VoIP

Este apartado resume las características más relevantes de los distintos códecs objeto del estudio. Todos ellos toman a su entrada una señal PCM de 16 bits muestreada a 8kHz y generan palabras código o *tramas* a intervalos periódicos. De esta forma cada trama permite reconstruir el discurso original correspondiente a un periodo de dicha duración. Si

las tramas son enviadas inmediatamente a la red[1], el retardo de empaquetado es igual a dicho intervalo. El retraso total o latencia resulta del anterior incrementado en un retardo de anticipación, que no es más que el retraso correspondiente al acopio de un número de muestras de entrada suficientes para que el codificador empiece a trabajar sobre ellas.

Algunos códecs, capaces de supresión de silencios o transmisión discontinua, ahorran capacidad interrumpiendo el envío periódico de las tramas citadas en los instantes en los que no hay actividad vocal según indique un algoritmo detector de actividad vocal (*Voice Activity Detector o VAD)*. Los más avanzados las sustituyen incluso por el envío más esporádico de tramas mucho menores (tramas SID, o de descripción de silencios) que describen el nivel de potencia del ruido detectado en el lado del hablante. Estas tramas permiten que, con un coste de transmisión reducido, en el destino pueda generarse ruido de confort fiel al que ocurre en el lado del hablante.

A. G.711

El códec G.711 [8] es el decano de los mecanismos de codificación de voz. Aunque originario de las redes de telefonía basadas en conmutación de circuitos, se usa también en redes de VoIP.

Dado que este códec no hace uso de técnicas de compresión, su latencia es de sólo 125 μs, siendo el retardo de anticipación despreciable. La sobrecarga computacional de la fase de codificación es también mínima, correspondiente a una cuantificación logarítmica que busca reducir la distorsión en señales de baja amplitud. Existen dos variantes de dicho mecanismo, denominadas Leyes A y μ, respectivamente. En este estudio se ha utilizado exclusivamente la Ley A. Su único inconveniente es una tasa elevada, de 64 Kbit/s[2]. Su alta calidad hace que se use para marcar el nivel de referencia del servicio de telefonía.

B. G.729

El G.729 [9] es un códec que incorpora un algoritmo de compresión mediante predicción lineal con excitación por código algebraico de estructura conjugada (CS-ACELP). Es uno de los más utilizados en VoIP debido a su buen compromiso entre baja tasa, alta calidad y robustez, a costa de una alta complejidad. Incurre en un retardo de 15 ms, repartidos en 5 ms de retardo de anticipación y 10 ms de empaquetado. Cada trama consiste en 80 bits, lo que resulta en una tasa nominal de 8 Kbit/s que puede variar en diferentes extensiones de la norma. Las características de éstas, que pueden modificar la calidad de la señal decodificada, son las siguientes:

G.729A: Variante simplificada que requiere una potencia de cálculo menor a cambio de una degradación en la calidad de la voz.

G.729B: Variante que reduce el ancho de banda utilizado mediante un esquema de compresión de silencios con transmisión discontinua (DTX), detección de actividad vocal (VAD) y generación de ruido de confort (CNG).

G.729AB: Mezcla de los dos anteriores: variante simplificada (G.729A) pero añadiendo el esquema de compresión de silencios.

C. G.723.1

Al igual que los dos anteriores, el G.723.1 es otro códec normalizado por la ITU-T [10]. Es muy popular en aplicaciones VoIP porque ofrece una tasa razonablemente baja.

Su latencia comprende un retardo de anticipación de 7.5 ms y un retardo de empaquetado de 30 ms. Incorpora dos algoritmos de codificación diferentes, que resultan en diferentes longitudes de trama y, por tanto, diferentes tasas:

- Algoritmo MPC-MLQ, con tramas de 24 octetos, que resultan en 6.4 Kbit/s de tasa.
- Algoritmo de codificación ACELP, con tramas de 20 octetos, que se traducen en una tasa de 5.3 Kbit/s.

Este códec también proporciona un esquema de compresión de silencios basado en transmisión discontinua (DTX), detección de actividad vocal (VAD) y generación de ruido de confort (CNG), lo que permite ahorros adicionales sobre las tasas mencionadas.

D. iLBC

El iLBC (Internet Low Britrate Codec) es un códec de tipo predictivo lineal, recogido en [11], que ofrece una calidad comparable con la obtenida con el G.711 aunque con la cuarta parte del consumo de ancho de banda. Esto, unido a que se trata de un códec muy robusto frente a pérdida de paquetes, lo hacen indicado para comunicaciones en tiempo real: telefonía, videoconferencia, flujos de audio, etc.

El iLBC trabaja con dos tamaños de trama diferentes:

- Tramas de 303 bits con un retardo de empaquetado de 20 ms, correspondientes a una tasa de 15.2 Kbit/s.
- Tramas de 399 bits con un retardo de empaquetado de 30 ms, que resultan en una tasa de 13.33 Kbit/s.

Aunque el iLBC carece de un mecanismo específico que mitigue los efectos de la pérdida de paquetes (o mecanismo de *Packet Loss Concealment*), sí que permite una fácil implementación, por ejemplo interpolando los paquetes inmediatamente anterior y posterior al perdido para suministrar un paquete sustituto. La robustez frente a pérdidas del códec iLBC es muy superior a la del resto, ya que las tramas generadas son independientes.

E. AMR

El códec AMR, (*Adaptative Multi-Rate*), normalizado por el 3GPP [12], se utiliza ampliamente en redes de telefonía móvil.

Como su nombre indica, es un códec multitasa que permite funcionar a 12,2, 10,2, 7,95, 7,40, 6,70, 5,90, 5,15 y 4,75 Kbit/s con tramas de 244, 204, 159, 148, 134, 118, 103 y 95 bits respectivamente, correspondientes a un retardo constante de empaquetado de 20 ms de duración.

El codificador usado es de tipo híbrido, con un algoritmo de predicción lineal con excitación por código algebraico de

[1] En algunas aplicaciones de VoIP se permite que el usuario agrupe un conjunto de tramas - normalmente 2 ó 4 - antes de ser enviadas a la red. Con ello se consigue un transporte más eficiente ya que se comparten las cabeceras RTP, UDP, IP y 802.11 necesarias para hacer llegar las tramas a su destino.

[2] El códec G.711 cuenta con un algoritmo VAD definido en su anexo II utilizado tradicionalmente en comunicaciones de larga distancia. En este trabajo no se ha incluido para este códec dicho algoritmo VAD.

estructura conjugada (ACELP) para realizar el proceso de codificación de la señal de entrada. El retraso de codificación es de 20 ms, al que hay que sumar un retardo de anticipación de 5 ms, salvo para la tasa de 12.2 Kbit/s.

Al igual que el G.723.1 o el G.729B, el AMR usa un esquema de compresión de silencios basado en transmisión discontinua (DTX), detección de actividad vocal (VAD) y generación de ruido de confort (CNG) para reducir el ancho de banda durante los periodos de silencio.

La tabla I resume las características principales de los códecs estudiados. La columna MOS ha sido calculada utilizando el método de evaluación de la calidad vocal por percepción, PESQ, normalizado en la Recomendación P.862 de la ITU-T. Por tanto, se asume un escenario sin pérdidas de paquetes ni retrasos entre el transmisor (codificador) y el receptor (decodificador).

III. Funcionamiento de la interfaz WiFi

Para este estudio se considerará un escenario en el que un terminal VoIP accede en solitario a una red 802.11g gestionada por un punto de acceso (PA). En esta situación no existen colisiones, por lo que refleja el mínimo consumo energético. Dada la baja tasa de los códecs comparados con el régimen binario del canal puede asumirse que las escuchas previas a las transmisiones detectan siempre un canal vacío, así que el retardo de acceso al canal será mínimo e igual al correspondiente intervalo entre tramas (SIFS, PIFS o DIFS), sin ventanas de contienda adicionales.

La Figura 2 sintetiza el funcionamiento de la interfaz WiFi en el escenario considerado. Tras la generación de una trama por parte del códec, el protocolo de acceso CSMA-CA impone una espera DIFS con auscultación del canal previa al envío. Efectuada la transmisión, el punto de acceso esperará un intervalo SIFS, de más corta duración, y responderá con un asentimiento. Este ciclo se repetirá a la tasa de generación de tramas del códec, suprimiéndose cuando proceda en el caso de códecs con transmisión discontinua. En el sentido opuesto, el punto de acceso enviará las tramas procedentes del extremo distante tras una espera algo más corta (PIFS), siendo asentidas por el terminal tras la espera mínima (SIFS).

Los tiempos de propagación a las distancias propias de los entornos locales pueden considerarse despreciables con respecto al resto, tal y como se muestra en la Tabla II.

La misma Figura 2 representa los estados de consumo correspondientes al terminal. En ausencia de mecanismos de ahorro de energía, la interfaz transmisora se encontrará en estado activo durante el envío de las tramas y de los asentimientos correspondientes al sentido opuesto, y otro tanto en estado de recepción. El resto del tiempo quedará en estado ocioso. Por tanto, si se tienen en cuenta los tamaños habituales de las tramas generadas por los códecs, se observa que la mayor parte del tiempo la interfaz WiFi estará en estado ocioso, y los ahorros de energía en dicho estado serán los más significativos.

El modo de ahorro de energía (PSM) permite a un terminal pasar a estado durmiente cuando no se está transmitiendo, recibiendo o auscultando el canal [2], [3]. Para minimizar la pérdida de paquetes en recepción el punto de acceso los almacena hasta que el terminal despierte. La necesaria

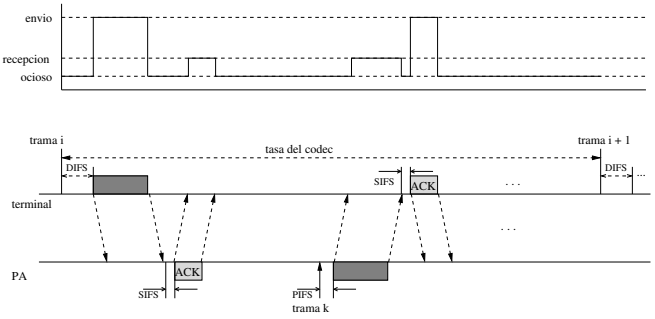


Fig. 2. Funcionamiento de las interfaces WiFi en aplicaciones VoIP

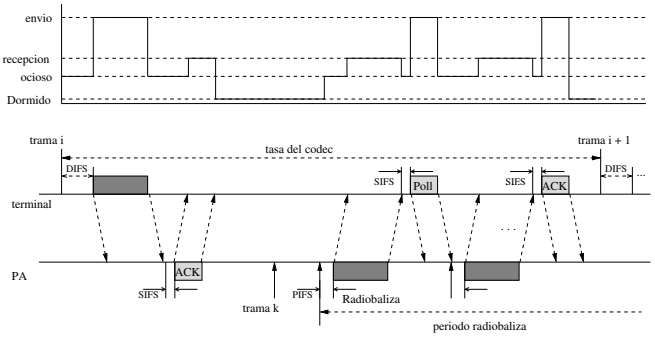


Fig. 3. Funcionamiento de las interfaces WiFi en aplicaciones VoIP con modo de ahorro de energía (PSM)

sincronización se resume en la Figura 3. Previamente el terminal indica su intención de pasar a estado durmiente durante el lapso correspondiente a un determinado número de radiobalizas. La periodicidad de la radiobaliza enviada por el punto de acceso es negociable, y puede acordarse a un valor igual a la tasa del códec, lo que permitirá un ciclo de paso de estado durmiente a recepción para cada trama recibida sin que haya pérdidas. Cuando el terminal despierte esperará a recibir la radiobaliza, que porta una indicación de la existencia de datos destinados al mismo, y responderá con una trama de sondeo. El punto de acceso enviará la trama al terminal ya ocioso y esperará el asentimiento con el mismo esquema de esperas que se realiza en el modo normal. Si no hubiera datos con destino al terminal, éste omitirá el sondeo y podrá pasar a estado durmiente hasta la siguiente radiobaliza.

En esta situación, el estado ocioso quedará reservado para las esperas DIFS, PIFS y SIFS, como se muestra en la Figura 3. Para cada ciclo de radiobaliza habrá que contar con la transmisión de un sondeo adicional por parte del terminal. El resto del tiempo que antes era ocioso pasará ahora a estado durmiente.

IV. Modelado del Consumo de Energía de un códec de VoIP

Estudios sobre el consumo de energía en los dispositivos móviles [1], [6], [13] parecen coincidir en el hecho de que la CPU, la memoria y la tarjeta WiFi consumen la mayor parte de la energía de un dispositivo móvil. Aunque existen algunos estudios que afinan el consumo energético, realizando un estudio particularizado para diferentes tipos de aplicaciones comunes tales como descarga de ficheros o streaming de audio o vídeo [5], [6], son escasos los estudios existentes sobre el consumo de las aplicaciones de VoIP [2], [7]. Además, las

Códec	Tasa de muestreo (kHz)	Tasa de bits (Kbit/s)	Tamaño de trama (ms)	Bits por trama de voz	Bits por trama SID	Algoritmos de codificación	DTX	MOS	Código fuente C descargable de
G.711	8	64	-	640	-	PCM	No	4.39	http://www.itu.int/rec/T-REC-G.711/es [8]
G.723.1	8	6.3 5.3	30	192 160	32	MP-MLQ ACELP	Yes	3.69 3.49	http://www.itu.int/rec/T-REC-G.723.1/es [10]
G.729	8	8	10	80	-	CS-ACELP	No	3.75	http://www.itu.int/rec/T-REC-G.729/es [9]
G.729A	8	8	10	80	-	CS-ACELP	No	3.67	http://www.itu.int/rec/T-REC-G.729/es [9]
G.729B	8	8	10	80	10	CS-ACELP	Yes	3.51	http://www.itu.int/rec/T-REC-G.729/es [9]
G.729AB	8	8	10	80	10	CS-ACELP	Yes	3.55	http://www.itu.int/rec/T-REC-G.729/es [9]
AMR	8	12.2 10.2 7.95 7.4 6.7 5.9 5.15 4.75	20	244 204 159 148 134 118 103 95	39	MR-ACELP	Yes	3.97 3.93 3.69 3.71 3.64 3.55 3.44 3.39	http://www.3gpp.org/ftp/Specs/html-info/26073.htm [12]
iLBC	8	15.2 13.3	20 30	303 399	-	iLBC	No	3.86 3.82	http://www.ietf.org/rfc/rfc3951.txt [11]

TABLA I
PRINCIPALES CARACTERÍSTICAS DE LOS CÓDECS DE VOIP.

Intervalo	Duración (μs)
SIFS	10.0
PIFS	19.0
DIFS	28.0
Radiobaliza (típ.)	40.29
Tara MAC	36.07
ACK	30.0
Sondeo (*PS-Poll*)	31.70
Propagación 100 m	0.30
Periodo códec	2000-8000.

TABLA II
TIEMPOS DE TRANSMISIÓN Y ESPERA2.

aplicaciones de VoIP suelen tener ciertos parámetros de funcionamiento configurables por el usuario entre los que destaca el códec a utilizar junto a sus características tales como VAD o DTX. Es previsible que la elección de estos parámetros tenga influencia en el consumo finalmente obtenido.

En una aplicación de VoIP los componentes del consumo directamente afectados por el códec son los siguientes:

- La CPU, usada en los procesos de codificación y decodificación de cada trama de una conversación. Además del algoritmo de cifrado, también el algoritmo de VAD consumirá ciclos de CPU en los códecs que presenten esta característica. El tiempo de CPU necesario para generar una trama dependerá básicamente del algoritmo de compresión del códec, debiendo ser siempre significativamente menor que el tiempo entre tramas.
- La interfaz WiFi, usada para transmitir las tramas generadas y recibir las tramas procedentes del otro extremo de la conversación [3]. Aunque la generación y consumo de tramas se pueden considerar periódicas, los códecs con DTX suspenden el envío durante los períodos de inactividad vocal, a excepción de las esporádicas tramas de descripción de ruido de fondo (tramas SID) que se usan en el generador de ruido de confort.
- Otros componentes como la memoria o la tarjeta de sonido pueden influir en el consumo de energía. Para el resto de este artículo no se tendrán en cuenta estos componentes.

Para estimar el consumo de energía se medirá el tiempo de uso de cada tipo de recurso (esto es, cada posible estado de la CPU e interfaz WiFi) durante las fases de transmisión y recepción de una conversación. El tiempo de uso de cada tipo recurso puede relacionarse directamente con la energía consumida utilizando datos de potencia de la circuitería del dispositivo en particular. Por ello, más que en términos absolutos (que dependería de cada dispositivo), nuestro objetivo es realizar un estudio comparativo entre códecs que permita inferir los beneficios de unos frente a los otros en términos relativos. Los datos utilizados para el cálculo de la potencia serán, por lo tanto, seleccionados de la literatura tanto en el caso de WiFi [14], [15] como en el caso de la CPU, donde se utiliza la proporción de gasto de CPU (un 4%) frente al consumo total expuesta en [1].

V. EXPERIMENTO

Se ha diseñado un experimento para medir el consumo de recursos de cada códec estudiado[4] en un escenario ideal sin colisiones, en la que un terminal hace uso exclusivo de una red de infraestructura 802.11g. Se ha escogido esta variante dado que es la más popular en entornos residenciales [16]. La elección de un escenario sin colisiones permitirá comparar sin distorsiones los distintos códecs. Es evidente que si hubiera colisiones se incrementaría el gasto energético de la interfaz WiFi, pero no el de la CPU.

Los pasos seguidos para el análisis de cada códec son los siguientes:

1) Obtención del código fuente de referencia (véase la tabla I).
2) Modificación del código fuente del códec en dos aspectos:

[3]El uso de la interfaz WiFi también requiere de una mínima atención de la CPU que será despreciada en nuestro estudio.

[4]Existen implementaciones comerciales de bajo consumo para varios de estos códecs, pero ante las dificultades para obtenerlas este estudio considerará sólo la implementación referencia, asumiendo que todos los códecs pueden ser objeto de mejoras similares.

- Para generar un archivo de texto de salida que contenga una secuencia con cada tipo de trama generado en el proceso de codificación (es decir, trama activa (0) y para aquellos códecs con VAD/DTX, trama SID (1), o sin trama (2)). Este archivo de salida (archivo *ftype*) permitirá identificar los periodos activos y los periodos de silencio, diferenciando así la energía consumida por la generación y envío de cada tipo de trama.
- Para indicar al sistema operativo que tome medidas del uso de recursos del sistema tales como ciclos de CPU o memoria usada por el proceso. Este paso se ha realizado con la utilización de la función `getrusage`, de la biblioteca GNU C, que se invoca cada vez que se procesa una trama.

3) Codificación de una conversación de referencia en PCM de 16 bits de 16.6 s de duración y con un factor de actividad del 50%.
   Como resultado se obtendrán 3 salidas:
   - el archivo codificado,
   - el archivo *ftype*, y
   - un archivo que muestra los recursos utilizados en el proceso de codificación (es decir, número de ciclos de CPU y memoria).
4) Decodificación del archivo codificado previamente, midiendo nuevamente los recursos utilizados en este proceso.

Para los códecs multitasa, tales como el AMR, el G.723.1 o el iLBC, los procesos de codificación y decodificación se han ejecutado para cada modo posible. El equipo utilizado en este estudio ha sido un Macbook con CPU tipo Intel Core Duo T2500 (2.0 GHz) y 2GB de RAM.

Las medidas para los procesos de codificación y decodificación se han realizado 300 veces (puesto que el uso de recursos de la CPU puede presentar pequeñas variaciones entre las mediciones). Los resultados presentados en este trabajo muestran el valor promedio.

VI. Resultados

A. Consumo de CPU

La CPU es utilizada tanto para la codificación de las tramas que se generan como para la descodificación de aquellas tramas que se reciben[5].

1) Codificación: En la Figura 4 se muestra, sobre el fondo de los primeros 8 s de la conversación, la evolución del consumo acumulado de tiempo de CPU (tiempo de sistema y tiempo de usuario) empleado en la codificación[6]. Los códecs que muestran mayor pendiente se corresponden con un mayor tiempo de procesado y por tanto un mayor consumo energético. Igualmente se observa cómo disminuye este consumo en los periodos de silencio para los códecs capaces de transmisión discontinua.

Del mismo modo, en la Figura 5 se puede observar la fracción de tiempo acumulado de CPU consumido por cada

[5]En el escenario del experimento no se pierden tramas y por lo tanto no se utilizan mecanismos de mitigación de pérdidas (PLC).

[6]En aras de la claridad, sólo presentaremos en los resultados tres de los ocho modos del códec AMR (los de mayor y menor tasa y una tasa intermedia)

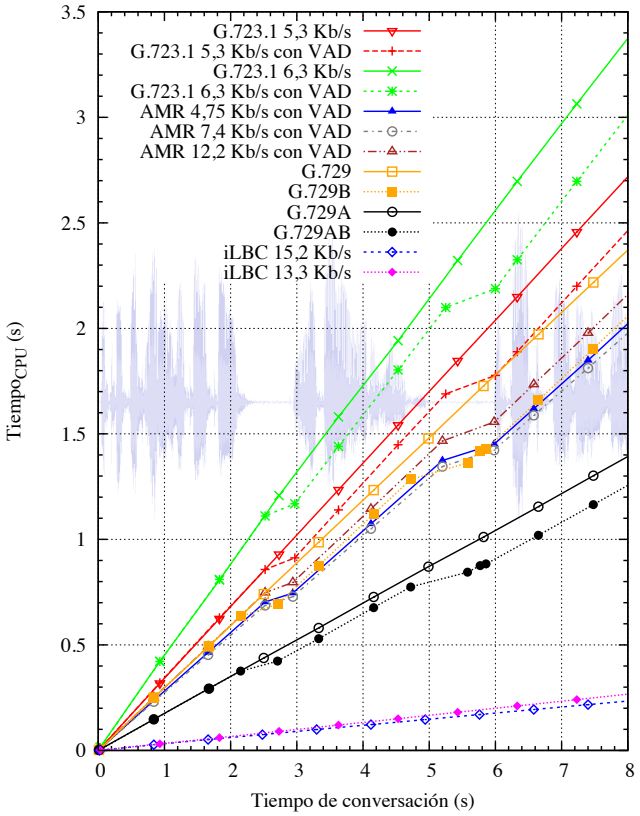


Fig. 4. Tiempo de CPU consumido en el proceso de codificación de los diferentes códecs.

códec y segundo de conversación en el proceso de codificación tanto para tramas activas como SID.

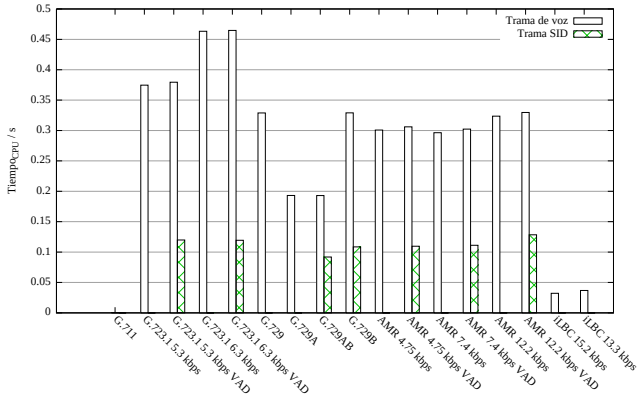


Fig. 5. Tasa de uso de la CPU en la codificación de tramas.

En [1] se indica que el consumo energético de la interfaz WiFi, en nuestro caso de 1.3 W·s, es de 15 a 16 veces superior al de la CPU, por lo que se ha estimado en 8.25 mW·s el gasto energético de ésta. Con esa cifra puede representarse el consumo energético de la CPU para la conversación anterior tal y como refleja la Figura 6.

2) Decodificación: En las Figuras 7, 8 y 9 se representan los datos descritos en el epígrafe anterior en el caso de la decodificación de tramas.

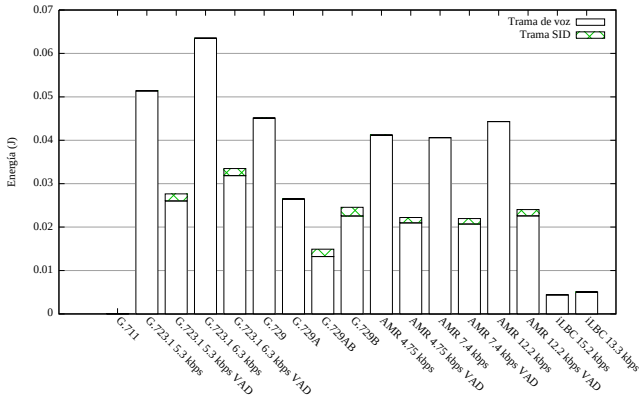


Fig. 6. Energía total consumida por la CPU en la codificación de tramas de la conversación

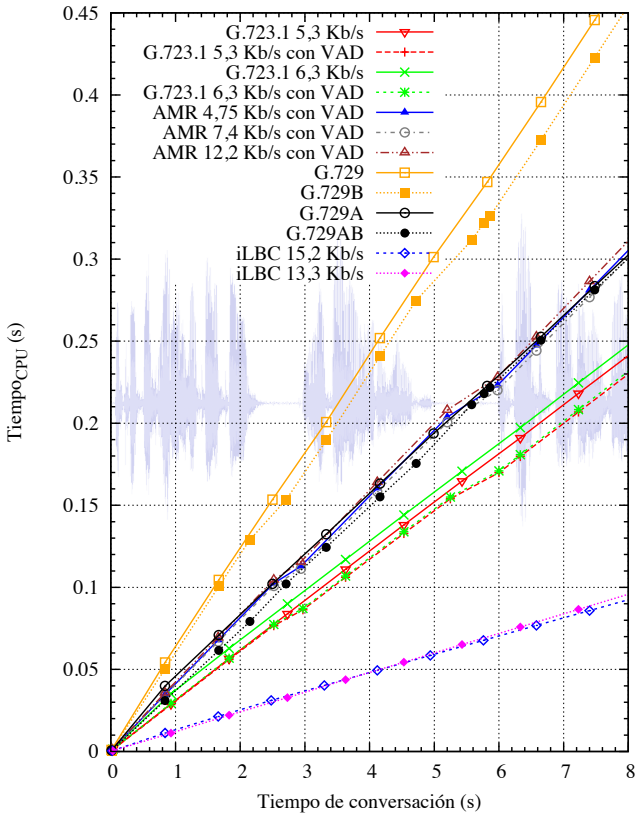


Fig. 7. Tiempo acumulado de CPU consumido en el proceso de decodificación de los diferentes códecs.

B. *Energía consumida por la interfaz WiFi*

Para el cálculo del ahorro energético en la interfaz WiFi se ha tenido en cuenta lo expuesto en la sección III. Dado que el número medio de tramas de cada tipo generadas será igual al de recibidas durante la conversación[7], puede computarse el consumo en ausencia de modo de ahorro de la siguiente forma:

- El tiempo en estado de envío será igual al tiempo de envío de las tramas más un asentimiento por cada una de ellas.

[7]Supondremos la conversación simétrica; es decir, que ambos extremos generan las mismas tramas.

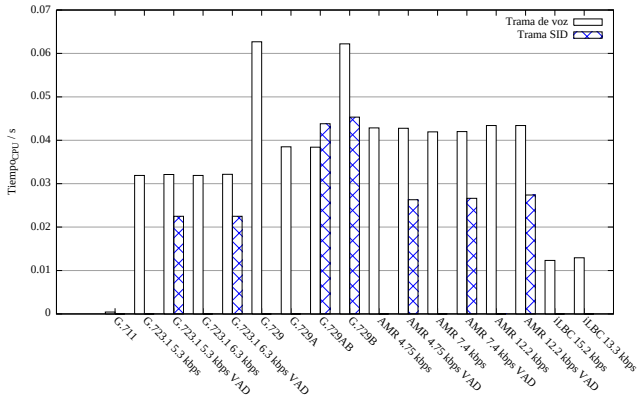


Fig. 8. Tasa de uso de la CPU en la decodificación de tramas.

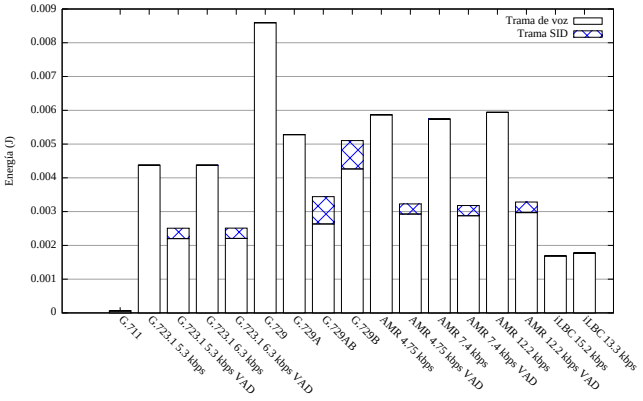


Fig. 9. Energía total consumida por la CPU en la codificación de tramas de la conversación.

- El tiempo en estado de recepción será mayor al anterior en el número de radiobalizas recibidas por la duración de la misma.
- El resto del tiempo hasta alcanzar el total de la conversación se computará como estado ocioso.

Con el modo de ahorro de energía (PSM) el cómputo queda así:

- El tiempo en estado de envío será igual al tiempo en el caso anterior incrementado en el número de tramas activas o SID multiplicadas por el tiempo de envío de un sondeo.
- El tiempo en estado de recepción será igual al del caso anterior, puesto que se reciben el mismo número de tramas y de radiobalizas.
- El tiempo en estado ocioso se determinará multiplicando $1 \times DIFS + 2 \times PIFS + 3 \times SIFS$ por cada trama activa o SID transmitida (recuérdese que en media se reciben las mismas que se transmiten), más una espera de PIFS por cada periodo sin trama en recepción.
- El resto del tiempo hasta alcanzar el total de la conversación se computará como estado durmiente.

Las tasas de potencia atribuibles a cada estado se encuentran descritas en [14] (para los estados de transmisión ($\rho_{tx} = 0.3W$), recepción ($\rho_{rx} = 0.185W$) y ocioso ($\rho_{\sigma} = 0.066W$) y en [15](para el estado durmiente).

Las Figuras 10 y 11 representan la energía total consumida por la interfaz WiFi tanto en la transmisión como en la

recepción de todas las tramas de nuestra conversación de 16,6 s sin y con modo ahorro de energía PSM respectivamente. En este caso puede apreciarse cómo al utilizar el modo PSM las diferencias entre códecs se hacen más patentes.

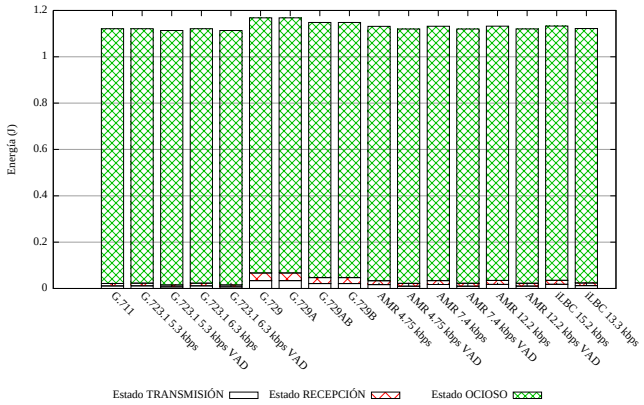


Fig. 10. Energía consumida por la interfaz WiFi en la transmisión y recepción de todas las tramas de la conversación sin modo PSM.

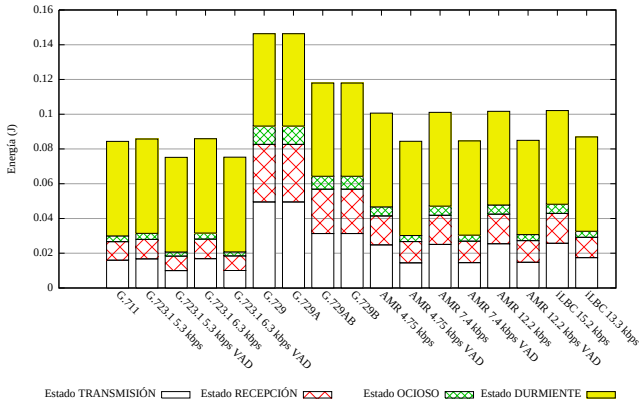


Fig. 11. Energía consumida por la interfaz WiFi en la transmisión y recepción de todas las tramas de la conversación con el modo PSM.

C. Estimación de la energía total

Las Figuras 12 y 13 muestran el total de energía consumida en la conversación de referencia sin y con el modo PSM respectivamente. En nuestro modelo simplificado, el total de Energía es calculado como la suma de la energía atribuible a la CPU mostrada en el epígrafe anterior (suma de codificación y decodificación), más la energía atribuible a la interfaz WiFi teniendo en cuenta el uso o no del modo PSM.

VII. Discusión de los resultados

De los resultados obtenidos en la sección VI relativos al uso de la CPU pueden obtenerse varias conclusiones:

- El códec iLBC muestra un consumo de CPU significativamente menor del resto, seguido por el códec G.729AB. En el otro extremo, el códec G.723.1 es el que registra mayor consumo seguido de los modos de mayor tasa del códec AMR.
- Tal y como cabía esperar, en aquellos códecs multimodo, los modos con mayor compresión (menor tasa) realizan un mayor esfuerzo computacional.

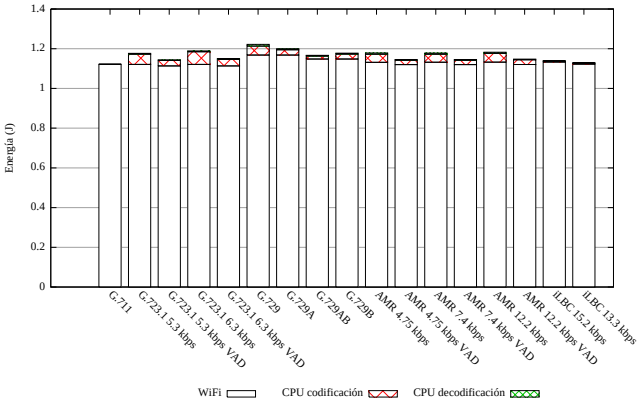


Fig. 12. Energía total consumida en una conversación de 16,6 segundos.

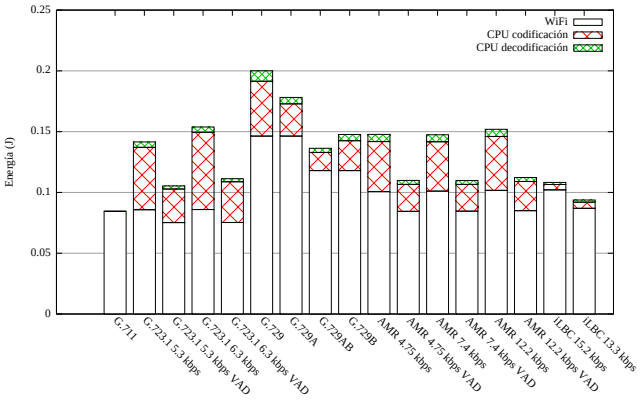


Fig. 13. Energía total consumida en una conversación de 16,6 segundos con Power Saving Mode activado.

- El funcionamiento del algoritmo VAD de los códecs reduce notablemente el consumo de CPU durante los periodos de inactividad vocal.
- El proceso de decodificación requiere de un esfuerzo computacional de casi un orden de magnitud menor que en el caso de la codificación.

En lo relativo al consumo del interfaz WiFi, puede concluirse que:

- En ausencia de modo PSM, la práctica totalidad del tiempo la ocupa el estado ocioso (cuando no se transmite ni recibe). Su consumo es significativo, por lo que apenas existen diferencias de consumo entre códecs.
- Cuando se utiliza el modo PSM, la mayoría del tiempo en estado ocioso pasa a ocuparse por el estado durmiente, donde el consumo sí es significativamente menor. Ello hace que afloren las diferencias de consumo entre distintos códecs. En particular, G.723.1 y AMR tienen un consumo significativamente menor que el resto, mientras que en el otro extremo el G.729, debido a su alta tasa de envío de tramas, presenta el mayor gasto.

Finalmente, debido al alto peso del consumo del interfaz WiFi sobre el consumo total, puede afirmarse que las diferencias entre códecs van a estar determinadas por el hecho de utilizar PSM o no. En ausencia de este modo apenas existen diferencias significativas entre códecs, ya que el tiempo en estado ocioso es claramente dominante frente a cualquier otra consideración. Cuando se usa el modo PSM se hacen más

evidentes las diferencias de consumo en CPU y WiFi de cada códec. En este modo en menor consumo es para G.723.1 y iLBC. El primero, pese a consumir más CPU que el resto, ahorra en el uso de la interfaz WiFi, ya que envía sus tramas cada 30ms y dispone de algoritmo VAD. El segundo es el que menos CPU consume, pero no dispone de algoritmo de actividad vocal, lo que se traduce en un mayor consumo en la interfaz WiFi.

VIII. Conclusiones y Líneas de Avance

Se ha llevado a cabo un estudio de la influencia de los diferentes códecs de VoIP en el consumo de recursos de los dispositivos móviles. Los resultados reflejan que el uso o no del modo de ahorro de energía o PSM en la interfaz WiFi es determinante para que se aprecien diferencias significativas entre códecs. Las diferencias encontradas entre códecs cuando se utiliza PSM colocan a los códecs iLBC, G.723.1 y AMR como los de menor consumo frente al resto.

En el futuro se pretende realizar un estudio con un modelo energético más complejo, que incluya otros componentes tales como la memoria o la pantalla, complementado con medidas de consumo realizadas con hardware específico en un laboratorio.

Referencias

[1] G. R. Pering T., Agarwal Y., "CoolSpots: redugin the power consumption of wireless mobile devices with multiple radio interfaces," in *4th International Conference on Mobile systems, applications and services*, june 2006, pp. 220 –232.

[2] V. Namboodiri and L. Gao, "Towards energy efficient VoIP over wireless LANs," in *MobiHoc '08: Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*. New York, NY, USA: ACM, 2008, pp. 169–178.

[3] T. Z. Madhani, S. Gurung, and E. P. van den Berg, "Reducing energy consumption on mobile devices with WiFi interfaces," in *IEEE Globecom 2005*. New York, NY, USA: IEEE, 2005.

[4] N. S. Ye Chan and S. Emeott, "Power management for VoIP over IEEE 802.11 WLAN," in *Wireless Communications and Networking Conference, IEEE WCNC*, March 2004, pp. 403 –408.

[5] D. W. MA Viredaz, "Power evaluation of a handheld computer," in *IEEE Micro*, 2003, pp. 66–74.

[6] V. Raghunathan, T. Pering, R. Want, A. Nguyen, and P. Jensen, "Experience with a low power wireless mobile computing platform," in *ISLPED '04: Proceedings of the 2004 international symposium on Low power electronics and design*. New York, NY, USA: ACM, 2004, pp. 363–368.

[7] P. M. A. Gupta, "Energy consumption and conservation in WiFi based phones: A measurement-based study," in *Conference SECON 2007*, 2007, pp. 66–74.

[8] "Pulse code modulation (PCM) of voice frequencies," ITU-T, Recommendation G.711, November 1988. [Online]. Available: http://www.itu.int/rec/T-REC-G.711-198811-I/en

[9] "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)," ITU-T, Recommendation G.729, January 2007. [Online]. Available: http://www.itu.int/rec/T-REC-G.729-200701-I/en

[10] "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s," ITU-T, Recommendation G.723.1, May 2006. [Online]. Available: http://www.itu.int/rec/T-REC-G.723.1-200605-I/en

[11] S. Andersen, A. Duric, H. Astrom, R. Hagen, W. Kleijn, and J. Linden, "Internet Low Bit Rate Codec (iLBC)," IETF, Recommendation RFC 3951, December 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3951.txt

[12] S. Andersen, H. Astrom, R. Hagen, R. Hagen, W. Kleijn, and J. Linden, "Adaptative Multi-Rate speech codec; C-source code," ETSI, Recommendation TS 126 073, December 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/26073.htm

[13] Y. L. SJ Ruan, "Development and analysis of power behavior for embedded system laboratory," in *Workshop on Embedded Systems Education*, 2006, pp. 363–368.

[14] M. Ergen and P. Varaiya, "Decomposition of energy consumption in IEEE 802.11," in *Communications, 2007. ICC '07. IEEE International Conference on*, june 2007, pp. 403 –408.

[15] "Power consumption and energy efficiency comparisions of WLAN products," in *Atheros Communication. White Paper*. Atheros, 2003.

[16] WiFi Alliance. [Online]. Available: http://www.wi-fi.org/files/kc_5_WFACertificationofIEEE802.11g-English_12-30-04.pdf

Distributed Management of Application Layer Multicast Trees for IPTV Services

D. Díez-Hernández*, J. García-Reinoso*, A. García-Martínez*, A. Bikfalvi*† and I. Vidal*
*Departamento de Ingeniería Telemática,
Universidad Carlos III de Madrid
Avda. de la Universidad 30, 28911. Leganés, Madrid.
Email: {ddhernan, jgr, alberto, ividal}@it.uc3m.es
†Institute IMDEA Networks,
Avda. del Mar Mediterraneo 22, 28918, Leganés - Madrid
Email: alex.bikfalvi@imdea.org

***Resumen*—IP multicast is an efficient mechanism to distribute IPTV content towards multiple users, but nowadays Internet Providers filter out this kind of traffic, mainly due to security and accounting issues. In order to overcome this filtering, the same idea of IP multicast can be implemented at the end user terminals, but implementing multicast trees at the application layer, also known as Application Layer Multicast (ALM). ALM has some drawbacks, mainly due to dynamic behavior of users, joining and leaving the trees. In order to minimize the impact of this behavior, this paper proposes a distributed management for ALM in IPTV, instead of a centralized one, where some nodes connected to a tree will be on charge of the management of that tree. Furthermore, all nodes are dynamically configured with the substitute of its parent node in order to accelerate the reconnection process. Results presented in this article show that this proposal provides fast reconstructions and low management load per node, while keeping a balanced tree topology.**

***Palabras Clave*—ALM, video streaming, churn**

I. Introducción

Hoy en día, para transmitir vídeo en tiempo real utilizando el protocolo IP, el método más eficaz es utilizar *IP multicast* debido a que la información sólo se replica en aquellos puntos (routers) donde haga falta, al contrario que en *unicast*, donde la propia fuente debe replicar el contenido tantas veces como receptores tenga. Sin embargo, el uso de IP multicast en entornos multi-proveedor está restringido debido a la dificultad de tarificar este tipo de tráfico, ya que un paquete en origen puede replicarse varias veces en la red, antes de llegar a sus posibles destinos. Esto, unido a problemas de seguridad y escalabilidad, han hecho que IP multicast no sea utilizado masivamente en Internet para transmitir vídeo, por ejemplo. Sin embargo, se puede utilizar una técnica en donde se crean árboles de distribución a nivel de aplicación en vez de hacerlo a nivel de red como lo hace IP multicast. A este tipo de técnicas se les llama *Multicast a Nivel de Aplicación* o *Application Layer Multicast (ALM)* en inglés. En los árboles ALM, los diferentes receptores del contenido pueden actuar a su vez como emisores para otros equipos si disponen de los recursos necesarios, creando un árbol de distribución, cuya raíz será el equipo generador de los contenidos (un Media Server, por ejemplo). El árbol tendrá también nodos *hoja* que recibirán el contenido pero no transmitirán dicho contenido a otros nodos y, quizás, nodos *interiores* que recibirán el contenido de otros nodos y, a su vez, transmitirán el contenido a uno o varios nodos receptores. Se dice que si un nodo U_i envía datos a otro U_j, el primero es *padre* del segundo (y, lógicamente, el segundo será *hijo* del primero).

El principal problema al usar cualquier técnica de ALM residen en el comportamiento dinámico de los usuarios. Si un nodo padre de uno o varios nodos, decide cambiar de canal (o salir del sistema) el sistema deberá reconstruir el árbol recolocando a los hijos que deja *huérfanos*. Esto puede provocar un corte en la reproducción del vídeo en los hijos que han quedado huérfanos, dependiendo del tiempo que se necesite para realizar la reconstrucción del árbol. Por lo tanto, el tiempo de reconstrucción es un parámetro que se debe intentar minimizar. Además, es importante distinguir entre las salidas ordenadas y desordenadas de los usuarios. En el primer caso el usuario que abandona el canal enviará un mensaje a las partes implicadas para notificar su salida, y en el segundo, el abandono se producirá de forma abrupta por algún problema en su funcionamiento. Evidentemente, el comportamiento y el tiempo de reacción del sistema ante una u otra situación será diferente.

El tiempo de reconstrucción depende de varios factores y de la técnica utilizada para realizar la reconstrucción. Normalmente, en las salidas ordenadas, los nodos envían un mensaje a un nodo central que se encarga a su vez de reconstruir el árbol si fuese necesario. El nodo central conoce la estructura completa del árbol y los recursos disponibles de cada uno de los nodos, por lo que puede decidir cómo recolocar a los nodos huérfanos, balanceando la estructura del árbol resultante. Una vez aplicado el algoritmo de reconstrucción, el nodo central envía la información a cada uno de los nodos huérfanos para asignarles nuevos padres. Uno de los mayores inconvenientes de este mecanismo es que un nodo central debe tener la información completa de todos los árboles de distribución para que el algoritmo proporcione un resultado óptimo en cuanto a la distribución de carga de los nodos. Además, el tiempo de reconstrucción del árbol depende del tiempo de ejecución de dicho algoritmo y del tiempo de transmisión y propagación hasta recibir la información con el nuevo padre al que se deben conectar.

En este artículo proponemos un sistema distribuido de administración de los árboles multicast a nivel de aplicación para distribuir contenido IPTV, en donde la información de la estructura del árbol se encuentre distribuida entre los

propios nodos que forman el árbol. Con esta información, algunos nodos del árbol, designados a tal fin, se encargaran de calcular y distribuir la información de los *padres adoptivos* para cada uno de los nodos. Es decir, cada nodo en el árbol estará recibiendo el vídeo de un padre y a su vez tendrá un padre adoptivo, es decir, un padre al que conectarse tan pronto se detecte un problema con su actual padre. Con esto pretendemos minimizar el tiempo de reconstrucción de los árboles y distribuir la carga de administración entre los propios nodos que forman el árbol.

El resto del artículo está organizado de la siguiente manera. La Sección II presenta algunos ejemplos de árboles multicast a nivel de aplicación. La Sección III explica detalladamente la propuesta de administración distribuida de gestión de los árboles multicast a nivel de aplicación, mientras que la sección IV presenta resultados obtenidos mediante simulación, que validan la solución propuesta. La Sección V presenta las conclusiones.

II. Árboles Multicast a Nivel de Aplicación

Para transmitir vídeo a través de la red tradicionalmente se ha usado una arquitectura cliente-servidor, en la que cada usuario se conecta a un servidor que es la fuente del vídeo. Una modificación sobre esta arquitectura es la denominada CDN (*Content Delivery Network*) en la que la fuente de vídeo se distribuye por un conjunto de servidores situados estratégicamente en la red. De esta manera, el cliente se conecta al servidor de contenido más cercano que tenga, distribuyendo la carga del servidor central. El problema de las arquitecturas cliente-servidor para la distribución de vídeo es la escalabilidad, ya que conforme el número de usuarios aumenta, se necesitan más servidores para balancear la carga. Pero desde hace relativamente poco tiempo se han empezado a utilizar redes P2P para solucionar los problemas que presentan las arquitecturas tradicionales para la distribución de vídeo. En este tipo de redes, los usuarios actúan como clientes y como servidores.

Existen dos tipos de servicios de vídeo para los que se pueden utilizar estas redes. El primero es el de vídeo bajo demanda, en el que el usuario elige reproducir un contenido para visualizarlo cuando quiera. Un ejemplo de este tipo de servicios sería *youtube*[1]. El segundo, que es el que nos ocupa en este documento, es el de vídeo en directo. En este tipo de servicio, todos los usuarios desean recibir un vídeo de una fuente determinada que está retransmitiendo en directo. Es decir, los usuarios están sincronizados en la reproducción.

Para la opción de reproducir vídeo en directo, existen actualmente dos soluciones basadas en arquitecturas P2P: las estructuras basadas en árbol (*tree-based*) y las basadas en malla (*mesh-based*).

Las distribuciones basadas en árbol pretenden emular los árboles multicast ideados para la distribución de vídeo y audio. Pero dado que el soporte de IP multicast se encuentra muy restringido por parte de los proveedores, se ha intentado emular el comportamiento de éstas mediante la utilización de los ALM (Multicast a Nivel del Aplicación).

Podemos diferenciar dos tipos de estructuras basadas en árbol. Las redes de un sólo árbol y las redes de múltiples árboles.

En las redes de un sólo árbol existe una fuente de vídeo que envía al resto de usuarios ([1], [2]). Pero a diferencia de la arquitectura cliente-servidor, los usuarios estarán organizados en forma de árbol de forma que cada usuario recibe el vídeo de un único nodo padre y es capaz de reenviarlo a uno o más nodos hijo, dependiendo de los recursos que tenga disponibles. En este tipo de arquitectura se reduce la carga que tenía el servidor, ya que el resto de usuarios que forman la red también actúan como retransmisores del vídeo. Existen principalmente tres aspectos que hay que tener en cuenta a la hora de diseñar un sistema de este tipo. El primero es que cada nivel añade un retardo a la retransmisión del vídeo. Por lo tanto un criterio de diseño es mantener el número de niveles de un árbol bajo un cierto límite que dependerá del número de nodos. Para ello cada usuario debe intentar atender al mayor número de hijos posible. Pero esto en la realidad está claramente limitado por el ancho de banda de subida que tiene cada usuario, que hace que no se pueda retransmitir nada más que a un número limitado de hijos, que en general es muy pequeño. Segundo, tampoco es recomendable conectar muchos nodos hijos a un nodo con gran número de recursos, ya que en caso de abandono del padre, se tendrá que reconectar un elevado número de nodos, lo que podría suponer una reestructuración compleja del árbol. El último aspecto importante se refiere al mantenimiento del árbol. Los usuarios pueden entrar y salir del árbol en cualquier momento, y cuando lo abandonan, sus hijos dejan de recibir vídeo. Para que no se produzcan cortes en la reproducción, el árbol tiene que reconstruirse lo antes posible. En las arquitecturas existentes hasta ahora la construcción y mantenimiento del árbol se realizan de forma centralizada. Es decir, existe un servidor central que controla la posición en la que ha de ubicarse un nuevo usuario y también controla la reconfiguración del árbol en caso de detectar abandonos, ya sea de manera ordenada, por avisos que se produzcan, o desordenada, mediante un soft-state. En cualquier caso, para árboles relativamente grandes, este tipo de sistemas presentan claramente un cuello de botella que puede repercutir en el rendimiento general del árbol, ya que tendría que atender a demasiadas peticiones en función del dinamismo de la red que administra. Con lo cuál, es posible que el árbol no se pueda recuperar suficientemente rápido cuando haya abandonos.

En las redes de múltiples árboles ([3], [4], [5]) se intenta aprovechar los recursos de los nodos que están en el extremo final de cada rama del árbol, ya que son nodos que sólo consumen recursos, pero no se utilizan para enviar vídeo a nadie más. Una red basada en múltiples árboles pretende solucionar este problema creando varios flujos diferentes del mismo vídeo y haciendo que cada uno se transmita por un árbol diferente. De esta manera, cada nodo puede tener un rol diferente en cada uno de los subárboles, pudiendo ser nodos hoja en un árbol e interiores en otros, cediendo así por lo menos parte de su ancho de banda de subida. En este tipo de sistemas, la utilización de varios árboles mejora notablemente el aprovechamiento del ancho de banda de salida de los nodos, pero la manera de buscar nodos con los que conectarse o reconectarse a la red es bastante compleja y requiere tiempos que en determinados entornos pueden ser demasiado largos.

[1] http://www.youtube.com

Aún así, eso puede no ser un problema, ya que al estar conectados a varios árboles, los árboles tienen cierta garantía de seguir recibiendo información en caso de abandonos en alguno de los árboles.

Por último, los sistemas basados en malla son arquitecturas en las que los usuarios intercambian la información del vídeo (o cualquier otro contenido) entre ellos, formando topologías lógicas independientes de la red en la que estén, y además con la característica de que cada nodo puede tener más de una fuente de la que recibir el vídeo, según sus necesidades, y enviar a diferentes nodos, dependiendo de sus recursos. Un ejemplo de un sistema de este tipo sería CoolStream ([6],[7],[8]). Estos sistemas introducen el concepto de *buffer map*, que sirve para representar la disponibilidad de los últimos bloques de diferentes sub-flujos que se quieran reproducir. Esta información se debe intercambiar entre los nodos periódicamente para determinar a qué sub-flujos suscribirse. Por esa razón, la gestión de miembros es muy importante para la construcción y mantenimiento de la red. En general, los sistemas basados en malla son arquitecturas bastante robustas en cuanto a la posibilidad de estar recibiendo vídeo, ya que cada nodo se asegura siempre de tener a un conjunto suficiente de usuarios que le estén proporcionando sus *buffer maps* y así siempre tener datos que mostrar. Pero por otro lado, son estructuras relativamente complejas que requieren un tratamiento complejo de los bufferes de recepción, y que además no deja de estar sujeta a discontinuidades en la reproducción, debido a la selección aleatoria de compañeros con los que asociarse, que puede crear incertidumbre sobre los datos a recibir.

III. Descripción de la propuesta

A continuación describiremos la solución planteada para distribuir la carga de construcción y reconstrucción de los árboles multicast que se utilizarán para la transmisión de vídeo IPTV. Se busca una arquitectura distribuida, descentralizada y uniforme: tal y como se ha diseñado la red en forma de árbol, los elementos de control de la red tienen una visibilidad fronteriza organizada en niveles. Cada elemento de control sólo tendrá información de lo que ocurra en su nivel y en el nivel inmediatamente inferior. Los cambios en una zona de control no afectan a cambios en otras zonas, distribuyendo por lo tanto la información por los niveles del árbol. Es una arquitectura uniforme ya que cualquier elemento que la compone es susceptible de asumir el rol de ser elemento de control.

Una consecuencia de este tipo de arquitectura es una reducción considerable del número de mensajes de control y un mejor aprovechamiento del ancho de banda de la red para la distribución de los contenidos, ya que en otro tipo de arquitecturas totalmente centralizadas hay que mantener comunicación con todos los nodos que forman la estructura para informar de cambios. Sin embargo, en este caso, al tratarse la información de control por niveles, los mensajes que hay que enviar cuando se produce un cambio sólo se producen entre niveles adyacentes. Además, al producirse los mensajes sólo en el entorno de su nivel, la recopilación de información es más sencilla y rápida, y la cantidad de información que hay que recopilar y almacenar en tablas también es mucho menor que en otras arquitecturas P2P.

Con el fin de introducir algunos conceptos y definiciones que son necesarias para desarrollar la propuesta, a continuación se describe la funcionalidad de algunos elementos importantes de la arquitectura propuesta y que se representan en la Fig. 1:

- Canal. Se refiere al árbol de distribución que se genera para reproducir un contenido determinado. Parte de una raíz y es accesible a través de los elementos que componen la red diseñada.
- Nodo. Un Nodo es un usuario que se quiere conectar a un canal para visualizarlo, y para ello tiene que entrar a formar parte del árbol de distribución de ese canal. Cualquier Nodo, cuando se conecta a un árbol, recibirá el vídeo de un único Nodo, que será su padre, y es susceptible de retransmitir ese vídeo a otros nodos, que serán sus hijos, y cuyo número dependerá de los recursos[2] que tenga disponibles. Además, el Nodo sólo enviará y recibirá vídeo relacionado con ese canal. Es decir, que mientras está en un árbol, sólo utilizará contenido manejado por ese árbol. Cada Nodo tienen un identificador único que lo identifica unívocamente dentro de la red. Un dato importante que deben tener todos los nodos es quién va a ser su siguiente padre, denominado padre adoptivo, y esta información se la comunica siempre el Big-Parent de su nivel superior. Así, cuando se pierda la comunicación de un Nodo con su padre actual (que es el que le está enviando el vídeo), el Nodo podrá reconectarse lo antes posible a otro padre.
- Big-Parent. Dentro de cada nivel i existe un único nodo denominado Big-Parent que contiene almacenada información sobre el resto de los nodos de ese nivel i, así como de sus recursos. El Big-Parent constituye el punto de entrada para un Nodo que se quiera conectar a un nodo del nivel i, ya que es el Big-Parent el que le asignará un padre de entre los nodos de su nivel. También se encarga de asignar el *padre adoptivo* a todos los nodos del nivel inferior y de decidir cuál va a ser el Big-Parent de entre ellos. El Big-Parent es un Nodo normal del árbol que recibe y envía vídeo como cualquier otro nodo, sólo que además tiene un papel organizativo dentro de la estructura. Cualquier nodo es candidato a ser Big-Parent cuando entra al árbol y además, cuando un Nodo pasa a ser Big-Parent, no abandona ese rol hasta que abandona el canal. Si abandonase el canal, sería necesario nombrar a otro Nodo para la administración del nivel.
- Generador. Es el nodo fuente y emisor del vídeo. Este nodo no puede desaparecer, ya que constituye el origen del vídeo y es la raíz del árbol para ese canal. A efectos de administración del canal, el comportamiento de este nodo es igual que el de un Big-Parent.
- Bootstrap. Es el nodo en el que están registrados los canales. Cada canal cuenta con un conjunto de nodos Big-Parents, con los que iniciar la comunicación y que se guardan en el Bootstrap de forma dinámica. Cualquier nodo que quiera conectarse a un canal debe comunicarse

[2]En este caso los recursos estarán en función del ancho de banda del nodo, aunque para la realización de las pruebas este parámetro no se ha tenido en cuenta.

antes con el Bootstrap. La manera en que el Bootstrap indica a un nodo con quién debe conectarse se explicará más adelante.

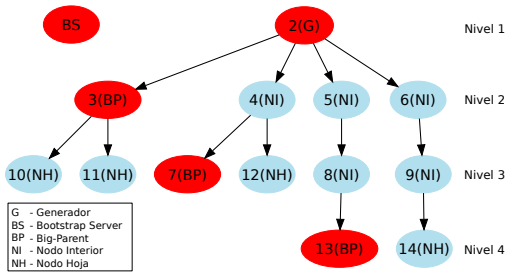


Figura 1. Tipos de Nodos

El concepto de padre adoptivo será también muy importante ya que es el que nos va a permitir reducir los tiempos de reconexión de los nodos. Esto hará que la disminución del buffer de reproducción de cada nodo sea lo menor posible y no se necesiten grandes esfuerzos para recuperarse de las reconexiones (mediante incrementos puntuales del ancho de banda, por ejemplo).

III-A. Estructura de los árboles

La estructura de la red (Fig. 1) está formada por un nodo Generador que es el origen del vídeo y raíz del árbol, y el resto de nodos se organizan por niveles. Cada Nodo puede tener un sólo padre y cero, uno o varios hijos, dependiendo del nivel, del tiempo que lleve conectado y de los recursos disponibles en dicho Nodo. La dimensión vertical del árbol está organizada en niveles, entendiendo que el nivel 2 estará formado por los nodos que tienen como padre directamente al nodo Generador, y el siguiente nivel será el formado por los nodos que tengan como padres a los nodos del nivel anterior y así sucesivamente. Cada nivel tendrá su propio nodo Big-Parent, que se se encargará de administrar los recursos de los nodos de su nivel y también de asignar siguiente padre y Big-Parent entre los nodos del nivel inferior. A nivel de nomenclatura, el nodo Generador será el nivel 1, y los siguientes niveles serán 2, 3, 4, etc. a medida que vayan apareciendo en el árbol. Se dirá que el nivel superior a un nodo que está en el nivel i será el nivel de su padre $(i-1)$, y el nivel inferior el de sus hijos $(i+1)$.

III-B. Mecanismo de conexión

Para conectarse a un canal, el nuevo Nodo envía al Bootstrap server un mensaje con el identificador del canal al cual quiere conectarse (mensaje 1 en Fig. 2). El Bootstrap tiene que seleccionar un Big-Parent del árbol de ese canal y comunicárselo al nuevo Nodo (mensaje 2), indicándole la dirección IP y el puerto del mismo. Cuando el nuevo Nodo recibe la respuesta del Bootstrap, envía un mensaje de *join request* (mensaje 3) al Big-Parent asignado, para indicarle que quiere conectarse. El Big-Parent solicitado puede hacer tres cosas: asignarle un nodo de su mismo nivel (si es que hay recursos) decirle al nodo que se conecte a él mismo si tiene recursos o reenviar la petición a otro Big-Parent de otro nivel. Si el Big-Parent ha decidido que se conecte a él mismo, le añade a su lista de hijos y de nodos del nivel inferior. Si no es así, la selección del padre se hace escogiendo el nodo de su propio nivel que menos recursos ocupados tenga, es decir, el que menos nodos hijos tenga. En el caso en el que el Big-Parent detecte que no hay recursos disponibles en su nivel, devolverá al nodo el identificador de otro Big-Parent[3]. En el caso de tener recursos en su nivel, en el mensaje *join reply* que le devuelve al Nodo, el Big-Parent le especifica cuál va a ser su siguiente padre, su nivel i y también el Big-Parent del nivel i. Una vez que el Nodo se ha conectado en el nivel i, el Big-Parent del nivel superior $(i-1)$ puede convertir al nuevo Nodo en Big-Parent de su nivel (i), si éste es el primer nodo de dicho nivel. Cuando el Nodo recibe la respuesta del Big-Parent (mensaje 4), si su padre va a ser el propio Big-Parent (nivel $i-1$), el nodo se considera conectado y manda un mensaje al Big-Parent de su nivel i para informarle de su existencia y de sus recursos. Con esta información, el Big-Parent de nivel i añadirá al nuevo Nodo a su tabla de nodos en el nivel i.

En el caso de que la conexión se haga con un nodo normal, el Nodo *padre* que recibe este mensaje (5) de *join* acepta la conexión del nuevo Nodo *hijo* y lo añade a su lista de hijos. Además, el nodo *padre* envía un mensaje (7) al Big-Parent de su nivel para decirle que tiene un hijo más (un recurso menos), por lo que el Big-Parent lo añade en su tabla de nodos del nivel inferior $(i+1)$. Finalmente, el nuevo nodo envía un mensaje (8) al Big-Parent de su nivel para que lo añada a su tabla.

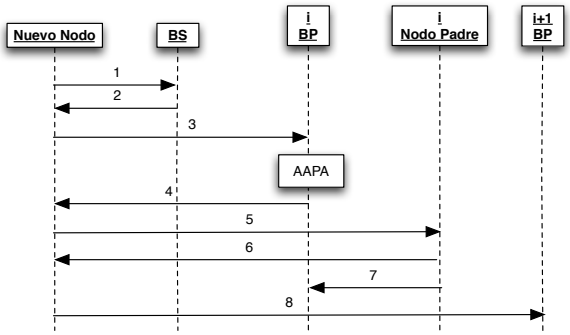


Figura 2. Mecanismo de Conexión a un Nodo normal

III-C. Eliminación de Nodos de un Árbol

Un Nodo se elimina del árbol cuando el usuario abandona el canal o el sistema (mensajes 1 a 5 de la Fig. 3). Antes de abandonar el árbol, el Nodo avisa a su padre para que no le siga enviando vídeo (mensaje 1) y a sus hijos para que se reconecten a otro padre (mensaje 2) y, si el nodo que abandona es Big-Parent, avisa al Bootstrap para que marque el nivel y no asignarle temporalmente nodos. En todo este proceso, tanto el padre como los hijos mandan mensajes y utilizan mecanismos para hacer saber a sus Big-Parents el abandono del nodo. Estos mecanismos se verán a continuación.

El nodo padre del que abandona el canal envía un mensaje (mensaje 3 de la Fig. 3) al Big-Parent de su nivel para comunicarle que tiene un recurso más. A su vez, este Big-Parent avisa (mensaje 4) al Big-Parent del nivel i que un nodo

[3]Una solución similar sería que el Bootstrap server le devuelva al nodo una lista de Big-Parents, por lo que el propio nodo podría elegir otro Big-Parent en caso de que el anterior no devuelva un nodo al que conectarse.

de su nivel ha abandonado el canal[4] por lo que éste ejecuta el algoritmo de asignación de padres adoptivos (AAPA), ya que pudo haber asignado como padre adoptivo al nodo que ha abandonado el canal. Si fuese así, asignaría nuevos padres adoptivos a los nodos correspondientes (mensaje 5).

III-D. Mecanismo de reconexión

Al recibir un mensaje *leave* de su Nodo padre, los *hijos huérfanos* de dicho nodo deberán reconectarse enviando un mensaje (mensaje 6 de la Fig. 3) *reconnect* al nodo que cada uno de ellos tienen asignado como *padre adoptivo*. En el mensaje de *reconnect* un nodo pide reconectarse indicando además a qué nodo estaban conectados, que será el nodo que ha abandonado el canal.

El nodo que recibe el *reconnect* añade a su nuevo hijo a la tabla e informa (mensaje 8) al Big-Parent de su nivel que un nodo de su nivel se ha ido (el que le ha dicho su nuevo hijo) y también los datos de su nuevo hijo. Con esta información, el Big-Parent de nivel i ejecutará el algoritmo de asignación de padres adoptivos y enviará dicha información a los nodos correspondientes (mensaje 9).

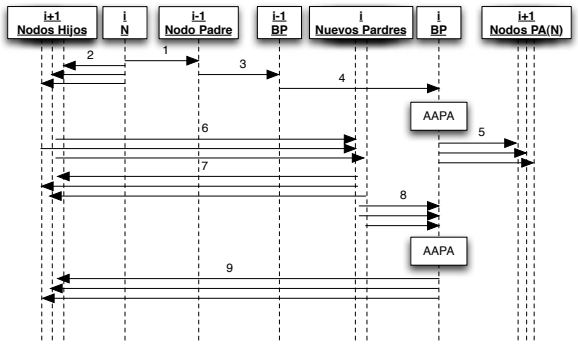


Figura 3. Abandono de Nodos normales y reconexión

III-E. Mecanismo de elección de Big-Parent

El Big-Parent de un nivel i lo elige el Big-Parent del nivel superior $i-1$. El Big-Parent tiene una tabla en la que, aparte de aparecer el identificador de cada nodo, el tiempo que llevan conectados y el padre y siguiente padre que tienen asignados, también aparece el Big-Parent que conoce cada nodo y por supuesto si un nodo es Big-Parent. Para elegir un nuevo Big-Parent en el nivel $i+1$, el Big-Parent de nivel i busca de entre los nodos de nivel inferior aquél que lleve más tiempo conectado, ya que ese Nodo es el que tiene más probabilidad de seguir en el canal ([9]), disminuyendo, en media, el número de mensajes necesarios para la elección y posterior notificación de los Big-Parents.

Con esa información, el Big-Parent de nivel i envía un mensaje a todos los nodos del nivel inferior indicándoles cuál ha sido el Nodo elegido para ser Big-Parent del nivel $i+1$. Cuando cada nodo del nivel inferior reciba el mensaje deberán enviar un mensaje al nuevo Big-Parent con sus tablas de hijos, para que éste conozca toda la información de su nivel y del nivel inferior, incluido el Big-Parent del siguiente nivel. El nuevo Big-Parent también debe enviar un mensaje al Bootstrap para sustituir al que ya había en su nivel e indicarle que ya puede aceptar peticiones de conexión.

[4]Con esto se puede reaccionar ante salidas desordenadas de los nodos. Aunque no se han contemplado las salidas desordenadas en las pruebas, los mecanismos se han diseñado pensando también en ello

III-F. Mecanismo de asignación de Big-Parent en el Bootstrap

Cuando un Nodo se conecta al Bootstrap para obtener un punto de conexión al árbol de un canal, el Bootstrap busca un Big-Parent de forma pseudo-aleatoria de entre los niveles que estén disponibles (que serán todos aquellos cuyo Big-Parent no se haya ido del canal y el nivel se esté reconfigurando todavía), y se lo asignará al nuevo Nodo. Decimos que el algoritmo de búsqueda de Big-Parent es pseudo-aleatoria porque se tiene en cuenta cuántos nodos se han conectado desde el último Big-Parent asignado, no utilizando este último hasta que el número de nodos nuevos haya sobrepasado un cierto límite. Este mecanismo permite controlar la altura de los árboles, ya que se elimina la posibilidad de que nodos consecutivos que entren al canal se aniden formando una rama, sin más nodos en sus niveles correspondientes.

III-G. Mecanismo de abandono de canal y reestructuración del árbol

Cuando un Nodo abandona el canal, lo único que tiene que hacer es enviar un mensaje *leave* a su padre y a cada uno de sus hijos. Además, si el nodo es Big-Parent, envía un mensaje al Bootstrap, para que éste sepa que provisionalmente no hay Big-Parent en el nivel y no asigne nodos ahí hasta que se haya reestructurado. A partir de ese momento, el nodo es libre de abandonar ese canal.

El problema puede surgir, evidentemente, en los nodos que se quedan. Los hijos, al recibir el mensaje *leave*, se reconectan a otro padre siguiendo el mecanismo de reconexión descrito anteriormente.

Cuando el padre recibe el *leave*, envía un mensaje al Big-Parent de su nivel indicándole el nodo que se ha ido. El Big-Parent, de esta manera sabe que el nodo tiene un hijo menos, y además si el que se ha ido fuera Big-Parent, tendría que buscar un nuevo Big-Parent y enviar mensajes según el mecanismo de elección de Big-Parent visto anteriormente. Si el que se ha ido no es Big-Parent, envía un mensaje al Big-Parent del nivel inferior para que éste actualice la tabla de nodos en su nivel.

IV. VALIDACIÓN

Para realizar la validación de la arquitectura diseñada se ha implementado un simulador basado en eventos que es capaz de simular una red con los mensajes que se envían entre los nodos y permite estudiar el comportamiento de éstos frente a cambios que se produzcan en el árbol, en especial las conexiones y reconexiones que se produzcan, y que son las que van a centrar las mediciones realizadas.

Gracias a la implementación de este simulador se podrán obtener datos de árboles de un tamaño considerable y que se podrán procesar más fácilmente. Por ello, al simulador se le ha dotado de un sistema de monitorización que permite obtener casi cualquier dato del estado del árbol o de los nodos.

Para que este simulador sea válido, debe reproducir lo más fielmente posible las condiciones de una red real y el comportamiento de los usuarios para los que se ha diseñado

la arquitectura. Para conseguir las condiciones de una red real, los mensajes que envíen los nodos deben estar sujetos a retardos parecidos a los que se encontrarían en Internet. Es decir, que para cada par de nodos debería existir un retardo diferente que estará en función de la localización de cada nodo en la red. Evidentemente, la red más real que tenemos es Internet, y para intentar reproducir las condiciones completas se necesitaría una simulación muy compleja. Por lo tanto se ha optado por hacer una aproximación basada en datos empíricos obtenidos a través del proyecto PingER[5], el cual realiza estadísticas de retardos entre diferentes puntos de Internet, y que permite elegir varios parámetros para sacar las medidas. En concreto, nosotros nos hemos basado en la tabla resumen del RTT medio para nodos localizados en Europa, y para un tamaño de paquete de 100 bytes. Hemos decidido utilizar datos de un sólo continente porque la probabilidad de que los usuarios que estén viendo una retransmisión en directo sean de una zona concreta es bastante alta. En base a estos datos se ha generado una variable aleatoria normal con media 19.8ms y desviación típica de 16ms para cada enlace entre cada par de nodos. La elección del tipo de variable aleatoria se ha hecho por aproximación a partir de histograma realizado con los datos extraídos del mes de marzo de 2010 del citado proyecto.

Otro dato de entrada importante es el tiempo de estancia de cada usuario en un canal cualquiera. Este dato lo hemos extraído de [10] en donde se obtuvieron diferentes parámetros de un servicio desplegado de IPTV. Aunque el sistema analizado en dicho artículo está basado en una infraestructura dedicada para IPTV desplegada utilizando multicast IP, nosotros tomamos el valor de tiempo de estancia en el canal como referencia, ya que nuestro objetivo es brindar la misma experiencia a los usuarios del sistema P2P propuesto que la que perciben los usuarios de un sistema dedicado. Ya que la información proporcionada en [10] es agregada entre todos los canales ofertados, hemos decidido simplificar el análisis y aplicar la misma distribución de tiempo de estancia a todos los canales simulados. Por este mismo motivo, todos los canales y usuarios tendrán el mismo comportamiento, por lo que los usuarios tendrán un tiempo de estancia en el canal siguiendo la misma distribución y, una vez abandonen su canal actual, elegirán con la misma probabilidad (siguiendo una distribución uniforme) otro canal.

Con todos estos datos que intentan aproximar una red con condiciones reales, se ha creado una simulación en la que existe un Bootstrap server en el que están registrados 4 canales, y que cuenta con un número total de 400 usuarios en el sistema (ya que se utiliza una distribución uniforme para seleccionar el siguiente canal, se espera un número medio de 100 usuarios por canal).

Aunque existen otras condiciones y variables importantes como son el número de recursos (ancho de banda disponible en uplink) y tamaño de buffers en cada equipo, en estas simulaciones se supone que esto no es problema, asumiendo un número infinito de recursos.

[5]http://www-iepm.slac.stanford.edu/pinger/

IV-A. Estructura de los árboles

Una parte importante de la validación es comprobar que los árboles de distribución se crean y reconstruyen de manera adecuada. Para ello hemos obtenido los parámetros típicos de un árbol de distribución para comprobar la morfología media resultante. En la Fig. 4 se representan los valores medios y desviación típica del porcentaje de nodos por cada uno de los niveles. Un resultado interesante es que, aún teniendo número ilimitado de recursos en cada nodo, los nodos padre no tienen muchos nodos hijos conectados ya que la relación entre nodos de cada nivel no es muy grande. Además, aunque el número de nodos por nivel no es constante, sí se puede observar que se distribuye entre los diferentes niveles. Lógicamente, por el orden de conexión, el porcentaje de nodos de los niveles inferiores comienza a decrecer a partir de un cierto punto.

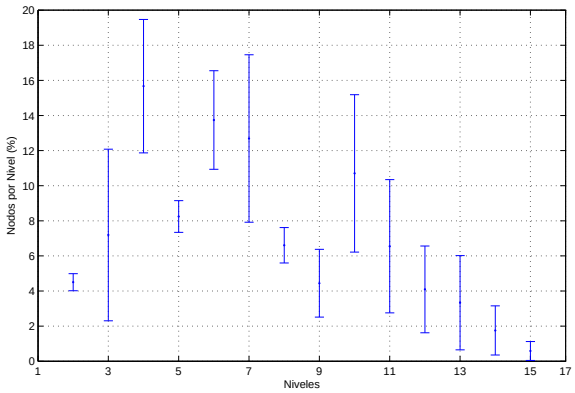


Figura 4. Porcentaje de nodos por nivel

Otro parámetro interesante es el del número de nodos hoja en el árbol. Tras realizar varias simulaciones, hemos obtenido que el número medio de nodos hoja es de $33{,}5\,\%$ del total de nodos y una desviación típica de $1{,}75$. Además, hemos estimado que el número medio de niveles es de $13{,}1$ con una desviación típica de $1{,}25$. Estos valores nos demuestran que el árbol se encuentra acotado tanto en altura como en el número de nodos hijo de cada nodo, y además concuerdan con lo esperado en el diseño descrito en III-F.

IV-B. Tiempos de conexión y reconexión

Uno de los valores más importantes, y motivo por el cual hemos realizado esta propuesta, es el tiempo que necesita un nodo para reconectarse una vez detecta que su padre actual se ha desconectado. Para estimar dicho valor, se han realizado 30 ejecuciones diferentes de 1 día de duración[6] cada una de ellas, obteniendo los resultados que se muestran en la Fig. 5. En esa figura se puede ver la función de distribución (Cumulative Distribution Function o CDF en inglés) para los tiempos de conexión (tiempo necesario para que un nodo se conecte o cambie a otro canal) y de reconexión (tiempo necesario para que un nodo hijo se reconecte a otro nodo padre). De estos resultados, se desprenden las siguientes conclusiones:

- Para el tiempo de conexión, el valor máximo obtenido es de $234ms$ y el mínimo de $35ms$. El valor medio

[6]Se refiere a 24 horas en tiempo de simulación, no en tiempo real.

obtenido entre todas las realizaciones es de $115ms$ con una desviación típica de $38{,}5ms$.

- Para el tiempo de reconexión, el valor máximo obtenido es de $107ms$ y el mínimo de $10ms$. El valor medio de todas las reconexiones es $48ms$ con una desviación típica de $17{,}3ms$

Lo más importante es que el tiempo medio de reconexión de un nodo es muy pequeño, e incluso el valor máximo es aceptable para que un nodo no agote su buffer de recepción durante esta fase de reconexión. Analizando detalladamente los resultados, hemos podido comprobar que no se han producido errores en las reconexiones de los nodos con sus *padres adoptivos*. Esto quiere decir que los nodos que se han quedado huérfanos siempre han podido reconectarse al padre adoptivo asignado.

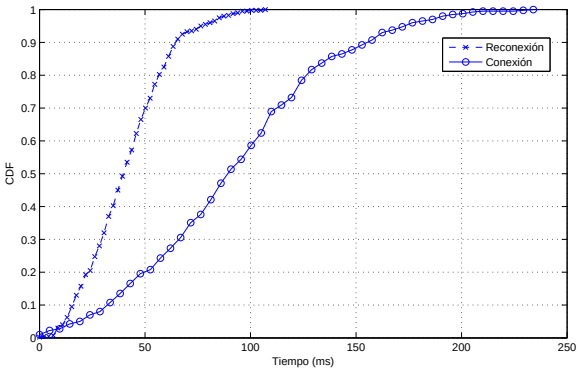


Figura 5. CDF de los tiempos de conexión y reconexión

V. Conclusiones

En este artículo hemos presentado una idea novedosa que pretende mejorar las prestaciones de los árboles multicast a nivel de aplicación. El objetivo principal es el de distribuir la carga de administración entre todos los equipos que forman parte del árbol multicast y, a su vez, minimizar el tiempo de reconexión de un nodo cuando su nodo padre abandona el canal. Mediante simulación, hemos obtenido valores del tiempo de reconexión muy buenos y que harían que el buffer de los clientes disminuyera de manera casi despreciable, por lo que se valida la propuesta. Es también interesante recalcar que se ha comprobado que en los casos peores, los tiempos siguen siendo muy bajos, y esto es debido a que la información de padre adoptivo que tiene cada uno de los nodos es siempre válido, ya que en caso de reconexión, siempre se pueden conectar a dichos nodos padre.

Como se ha comentado en la parte de validación, las simulaciones han sido realizadas suponiendo unas condiciones óptimas en la red, en donde todos los nodos tienen suficiente ancho de banda en subida y el tamaño de los bufferes no representa ningún problema. Este es un aspecto en el que se quiere seguir trabajando y se deja como trabajo futuro la inclusión de restricciones del número de recursos en los diferentes nodos.

Agradecimientos

Este artículo está financiado parcialmente por el proyecto MEDIANET (S-2009/TIC-1468) de la Comunidad de Madrid y por la Cátedra Telefónica en Internet del Futuro para la Productividad de la Universidad Carlos III de Madrid.

Referencias

[1] Y. Chu, S. Rao, S. Seshan, and H. Zhang, "A case for end system multicast," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 8, pp. 1456–1471, 2002.

[2] S. Banerjee, B. Bhattacharjee, and C. Kommareddy, "Scalable application layer multicast," in *Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2002, p. 217.

[3] M. Castro, P. Druschel, A. Kermarrec, A. Nandi, A. Rowstron, and A. Singh, "SplitStream: high-bandwidth multicast in cooperative environments," in *Proceedings of the nineteenth ACM symposium on Operating systems principles*. ACM, 2003, p. 313.

[4] D. Kostić, A. Rodriguez, J. Albrecht, and A. Vahdat, "Bullet: High bandwidth data dissemination using an overlay mesh," *ACM SIGOPS Operating Systems Review*, vol. 37, no. 5, p. 297, 2003.

[5] A. Nicolosi and S. Annapureddy, "P2PCAST: A peer-to-peer multicast scheme for streaming data," in *1st IRIS Student Workshop (ISW3). Available at: http://www. cs. nyu. edu/nicolosi/P2PCast. ps*. Citeseer, 2003.

[6] B. Li, Y. Qu, Y. Keung, S. Xie, C. Lin, J. Liu, and X. Zhang, "Inside the new coolstreaming: Principles, measurements and performance implications," in *Proc. of IEEE Infocom*. Citeseer, 2008.

[7] S. Xie, B. Li, G. Keung, and X. Zhang, "Coolstreaming: Design, Theory and Practice," *IEEE Transactions on Multimedia*, vol. 9, no. 8, p. 1661, 2007.

[8] X. Zhang, J. Liu, and B. Li, "On large-scale peer-to-peer live video distribution: Coolstreaming and its preliminary experimental results," in *Proc. MMSP*. Citeseer, 2005.

[9] Z. Liu, C. Wu, B. Li, and S. Zhao, "Distilling superior peers in large-scale P2P streaming systems," *Proc. of IEEE INFOCOM, Rio de Janeiro, Brazil*, 2009.

[10] M. Cha, P. Rodriguez, J. Crowcroft, S. Moon, and X. Amatriain, "Watching television over an IP network," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. ACM, 2008, pp. 71–84.

Desarrollo y despliegue de servicios DVB-IP con software *open source*

David Rincón, Federico Granaiola, Iria Rodríguez, Jesús Alcober
Departamento de Ingeniería Telemática (ENTEL), Escola Politècnica Superior de Castelldefels (EPSC)
Fundación i2Cat / Universitat Politècnica de Catalunya (UPC)
C/ Esteve Terrades, 7 08860 Castelldefels (Barcelona)
drincon@entel.upc.edu, federico.granaiola@yahoo.it, iriuki@gmail.com, jesus.alcober@upc.edu

***Resumen*- DVB-IP es el nuevo conjunto de estándares de la ETSI para el desarrollo de servicios de distribución de TV y vídeo bajo demanda sobre redes IP. Aunque la ETSI ha reaprovechado muchos de los protocolos TCP/IP clásicos, también se han desarrollado soluciones novedosas, como por ejemplo DVBSTP (un protocolo de descubrimiento de servicio), AL-FEC (FEC a nivel de aplicación) o BCG (*Broadband Content Guide*, una guía enriquecida de programación basada en web services), entre otros. El artículo presenta la arquitectura de DVB-IP, así como la implementación de un demostrador de servicios DVB-IP basado en software libre (*open source*), que demuestra que es factible desplegar este tipo de servicios con un coste mínimo. Finalmente se discuten las posibilidades docentes de un despliegue como el descrito en una titulación de Ingeniería Telemática.**

***Palabras Clave*- DVB, TV digital, IP, BCG, IPTV,open source.**

I. INTRODUCCIÓN

DVB-IP (también conocido como DVB-IPI o DVB-IPTV) es un estándar abierto creado por el consorcio DVB (*Digital Video Broadcasting*) e impulsado por el ETSI (*European Telecommunications Standards Insitute*) para la transmisión de servicios multimedia encapsulados en MPEG2-TS sobre redes IP bidireccionales de banda ancha [1]. El objetivo de DVB-IP no es la transmisión de *streaming* sobre Internet del tipo *YouTube* o similar, de calidad relativamente baja, sino de servicios de TV convencional o de alta definición ofrecidos sobre redes IP con calidad de servicio, de manera que la experiencia del usuario sea similar a la TDT o la TV por satélite, con la diferencia de que en este caso se usa una red IP y no una transmisión por radio.

Este artículo presenta la arquitectura de DVB-IP, así como la implementación de un demostrador de servicios DVB-IP basado en software libre bajo sistema operativo Linux, que demuestra que es factible desplegar este tipo de servicios con un coste mínimo, lo que abre su aplicación al mundo de las TV locales o el desarrollo de TVs universitarias, por ejemplo. Finalmente se hace hincapié en las posibilidades docentes de un despliegue como el descrito en una titulación de Ingeniería Telemática, en el contexto de una asignatura centrada en Protocolos y Servicios TCP/IP, o Servicios Audiovisuales sobre Redes IP.

II. DVB-IP: ASPECTOS BÁSICOS

A. Escenario y elementos

Los elementos principales de un escenario DVB-IP, mostrados en la Figura 1, son los siguientes:

1) Proveedor de contenidos (*Content Provider, CP*): Entidad que posee contenidos audiovisuales. Típicamente operadores de TV, o productoras de cine que quieran ofrecer sus contenidos bajo demanda en Internet.
2) Proveedor de servicios (*Service Provider, SP*): la entidad que da el servicio DVB-IP al usuario final. Suele ser el mismo operador de telecomunicaciones que da acceso a Internet (ISP), pero podría ser otra empresa.
3) Red de transporte: la infraestructura que conecta cliente y proveedores de servicios.
4) Pasarela de la red de distribución o DNG (*Delivery Network Gateway*): es el router/gateway/decodificador que conecta la red doméstica del usuario con la red IP del proveedor de servicios.
5) Red Local: red de la vivienda del usuario.
6) HNED (*Home Network End Device*): dispositivo conectado a la red local, utilizado para recibir contenidos DVB. Podría ser un TV, un *set top box*, o un ordenador.

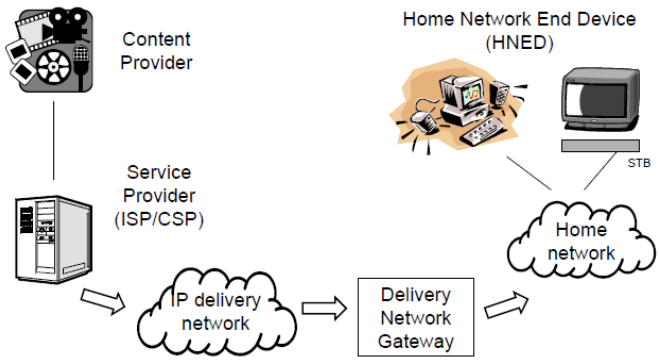


Fig. 1. Escenario y elementos DVB-IP

B. Perfiles DVB-IP

En DVB-IP se definen distintos niveles de funcionalidad, denominados perfiles, de complejidad creciente, y cuyo propósito es establecer escenarios de despliegue incremental de los servicios DVB-IP [2]. Los perfiles definidos son:

Live Media Broadcast: Es el perfil básico, caracterizado por ser el equivalente al servicio *broadcast* de TV. Los contenidos se envían únicamente en vivo, encapsulados en flujos *multicast,* por lo que no permite operaciones *trick mode* (*pause*, *forward*, etc) o acceso a contenido bajo demanda.

Media Broadcast with Trick Modes: Supone la evolución inmediata de LMB ya que los trick modes sí están disponibles. Para ello es necesario que los contenidos multimedia sean enviados en flujos *unicast*. La diferencia con el perfil CoD es que el usuario no puede pedir la visualización de un determinado contenido.

Content on Demand (CoD): Es el perfil más avanzado en el que están implementados los *trick modes* y además el usuario puede escoger los contenidos bajo demanda. Para ello se utiliza unicast como modelo de transporte.

Content Download Service (CDS): Todavía en fase de definición, permitirá la descarga de contenidos (en diferido, por ejemplo durante períodos nocturnos en los que hay baja carga en la red del proveedor de servicio) a un dispositivo de almacenamiento local en el HNED a través de una conexión IP de banda ancha.

C. *Protocolos*

Para ofrecer un servicio amigable y transparente al usuario final, DVB-IP debe solucionar una serie de retos y problemas técnicos que listamos a continuación, junto con los protocolos propuestos como solución:

a. Configuración: el usuario debe intervenir lo mínimo posible en el proceso de configuración del HNED. Protocolos involucrados: DHCP (asignación automática de dirección IP, DNS, gateway), DNS (resolución de nombres), NTP (sincronización de flujos audiovisuales). También se incluye la provisión de servicio y el control remoto del HNED (mediante XML, HTTP y HTTPS).

b. Descubrimiento y selección del servicio (*Service Discovery & Selection*, SD&S): una vez arrancado el HNED, el usuario debe obtener un listado de los canales de TV y películas/programas bajo demanda disponibles, y debe poder seleccionarlos de manera transparente. En este caso los protocolos involucrados incluyen XML (cuyos esquemas permiten la descripción de canales y programas), HTTP y DVBSTP (*DVB Service Discovery Transport Protocol*) para el transporte de XML, y RTSP e IGMP para la selección del servicio (IGMP para suscribirse al grupo multicast en el caso de los servicios de difusión en multicast, y RTSP para acceder al contenido bajo demanda en una sesión unicast).

c. Transporte: consiste en la transmisión (con calidad de servicio) de los flujos audiovisuales MPEG sobre la red IP. En este caso sólo se prevé el transporte de flujos *Transport Stream* (TS) de MPEG-2 sobre IP/UDP o bien IP/UDP/RTP sobre redes con calidad de servicio basadas en priorización (*Differentiated Services*), con la posibilidad de añadir opcionalmente AL-FEC (*Application Layer Forward Error Correction*) y RTP *Retransmission* para mejorar la calidad de la transmisión. CDS (opcional) también estaría en este apartado, aunque en ese caso se prevé el uso de multicast fiable, P2P, y FLUTE (*File Delivery over Unidirectional Transport*).

d. *Broadband Content Guide* (BCG), opcional. Es una guía de programas enriquecida, y como tal, estrictamente hablando, pertenece al conjunto de procedimientos relacionados con el descubrimiento de servicio. Sin embargo su arquitectura (basada en XML, Web Services y TV-Anytime) y su potente funcionalidad, junto con el desarrollo potencial de aplicaciones comerciales y modelos de negocio (como por ejemplo la compra de contenidos asociados a los que el usuario está visualizando, o marketing personalizado basado en el perfil de usuario) hacen que aparezca como un módulo DVB-IP con entidad propia.

Como puede verse en el listado anterior y la Fig. 2, DVB-IP integra buena parte de los protocolos y arquitecturas de servicio actuales.

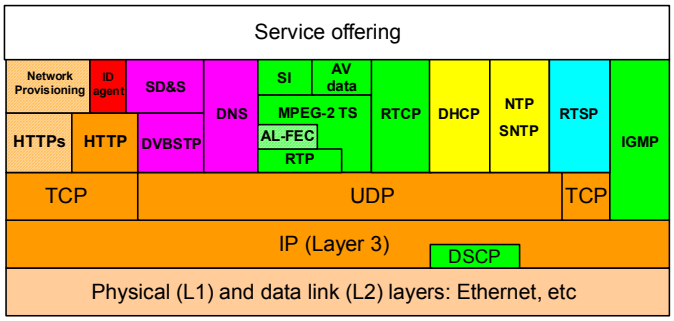


Fig. 2. Protocolos usados por el núcleo de DVB-IP (sin BCG ni CDS).

III. El Demostrador DVB-IP

A continuación presentaremos el demostrador DVB-IP que hemos desarrollado, basándonos sólo en software *open source* o bien desarrollado por nosotros. Nuestra intención es desplegar un escenario completamente compatible con los estándares DVB-IP, creando así un pequeño Proveedor de Servicio DVB-IP realista (la provisión de contenidos la hacemos a partir de antenas y receptores DVB para captar señales de TV comercial), y crear también un conjunto de software que funcione como DNG y HNED, emulados en un PC Linux. En nuestro escenario el DNG y el HNED serán la misma máquina (el *set top box* o decodificador de DVB-IP), ya que asumimos que será el caso más habitual, especialmente en los primeros despliegues del servicio.

A. *Escenario y hardware*

La Fundación i2Cat, en su sede de la Escola Politècnica Superior de Castelldefels (EPSC) de la UPC, dispone de una instalación de recepción de TV digital consistente en dos antenas parabólicas (apuntadas a Astra 19.2ºE) y una antena de TV terrestre orientada hacia el centro emisor de Collserola (Barcelona). Todas las señales van hacia una matriz distribuidora/mezcladora, que permite conmutar cada una de las cuatro señales (polarización vertical / horizontal, banda alta / baja) de cada parabólica, y combinarla con la banda UHF de TDT en un mismo coaxial.

Se dispone también de dos servidores DVB-IP cada uno de los cuales contienen una tarjeta receptora DVB-T y una DVB-S / S2 de bajo coste (aprox. 50 euros), cuyo hardware permite la sintonización y demultiplexado de los Transport Streams de DVB pero no la descompresión de MPEG-2/H.264, aunque esto se puede hacer fácilmente en software, y no en el servidor sino en el receptor. Los servidores corren Linux (Ubuntu 9.04, kernel 2.6.27-7 generic) y la DVB API integrada en Video4Linux. La capacidad total de recepción es de 2 multiplex de TV terrestre y de 2 más (DVB-S + DVB-S2) de TV por satélite. La Fig. 3 resume el montaje, aunque incluye sólo uno de los servidores (el principal). Nuestra intención es que el servidor secundario sea un

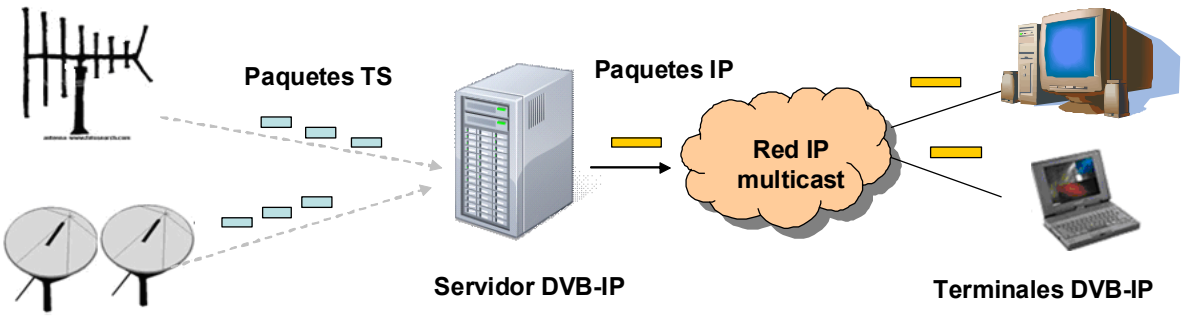


Fig. 3. Elementos del demostrador DVB-IP.

proveedor de servicios "esclavo" del primario, siguiendo uno de los escenarios previstos en DVB-IP (por ejemplo, un redistribuidor regional que es capaz de particularizar el *bouquet* de servicios ofrecidos a sus clientes).

IV. Configuración

La intención de esta parte del proyecto es la configuración de la red y de todos los dispositivos de ésta de modo que el usuario, tan sólo con la conexión del cable Ethernet a la LAN, pueda obtener automáticamente todas las funciones primarias de red (como asignar una dirección IP a cada usuario de la red o la traducción de las direcciones IP) y que la red pueda garantizar el correcto funcionamiento de los servicios DVB, llegando incluso a prever la contratación del servicio de acceso DVB-IP sin intervención de operadores humanos por parte del proveedor de servicio.

A. Servidor DHCP

DHCP (*Dynamic Host Configuration Protocol*) forma parte básica de DVB-IP, ya que la arquitectura de provisión marca que el Proveedor de Servicio controla completamente los parámetros IP del HNED, concretamente la dirección IP, la pasarela (*default gateway*), el nombre del dominio (en nuestro caso `dvb-ip.upc.es`), el servidor DNS, y el servidor NTP. También puede ofrecer uno de los puntos de entrada al descubrimiento de servicio, a través de DHCP *option* 15, tal como se explicará más adelante. Otra de las opciones que DVB-IP usa en DHCP es FORCERENEW, para forzar remotamente la renovación de la dirección IP del HNED. Para desplegar el servicio se ha utilizado el paquete `dhcp3-server` y se ha modificado `dhcpd.conf`.

B. Servidor DNS

En DVB-IP, DNS (*Domain Name System*) no sirve sólo para la resolución de direcciones a partir del nombre del host, sino que también tiene un papel como proveedor de punto de entrada a SD&S, a través de las entradas SRV (ver más adelante). Se ha utilizado BIND, modificando los ficheros de configuración en `/etc/bind/zones`.

C. Servidor NTP

NTP (*Network Time Protocol*) es necesario para ofrecer al HNED un servicio de sincronía con una precisión de 50 ms, con el objetivo de asegurar la correcta reproducción de los flujos audiovisuales. En este caso se ha utilizado el servicio (*daemon*) `ntpd`.

D. Provisión de servicio

DVB-IP define un conjunto de operaciones de control remoto del HNED denominado *Network Provisioning*, y que permite operaciones como descarga remota de *firmware*, reinicio remoto del HNED, consulta/escritura de la configuración del terminal, etc. Las transacciones se efectúan mediante documentos XML transportados sobre HTTP o HTTPS. Dado que nuestro demostrador incluye un HNED basado en software, y que este aspecto está my ligado al proveedor de servicio, por ahora no hemos implementado *Network Provisioning*.

V. Service Discovery & Selection

La presente sección describe los mecanismos utilizados para conocer los servicios DVB disponibles, su selección, y el transporte de las tablas *Service Discovery Information*.

A. Información de Service Discovery

SD&S es el mecanismo que proporciona los medios para el descubrimiento de los servicios DVB-IPTV y que aporta al usuario la información necesaria para que éste haga su elección y pueda acceder a los contenidos seleccionados. Estas listas de servicios llegan a todos los usuarios a través de los *Service Discovery Records*, formateados en XML:

- *SD&S Service Provider Record*: transporta información sobre los *SPs* que ofrecen servicios DVB-IPTV en la red y la localización de dichos *SPs*. El único SP del dominio *dvb-ip.upc.es* es SERVIDOR DVB-IP.
- *SD&S Broadband Content Guide Record*: es el medio para descubrir la localización de las guías enriquecidas tipo BCG que contienen los servicios disponibles, ya sean *Live Media Broadcast* o *Video on Demand*.
- *SD&S Package Discovery Record*: contiene información sobre servicios agrupados como una sola entidad.
- *SD&S Broadcast Discovery Record*: hay dos tipos:
  - *TS Full SI*: contiene la información necesaria para encontrar los servicios *Live Media Broadcast* anunciados mediante las tablas *Service Information* (SI) de MPEG, presentes en las transmisiones DVB.
  - *TS Optional SI*: similar a la anterior, con la salvedad de que proporciona más información al usuario.

Los documentos se generan automáticamente por parte de un módulo desarrollado para este fin (`dvb-xml-editor.c`) que edita el *SD&S Broadcast Discovery Record* (ya sea de tipo *TS Full SI* o *TS Optional SI*), extrayendo la información sobre los servicios *Live Media Broadcast* de las tablas *Service Description Table* y *Bouquet Association Table* de SI, recibidas en los multiplex de DVB-T/S y extraídas con las aplicaciones `scan` y `dvbsnoop` de la DVB API.

B. Transporte de la información SD&S

Existen dos modos que el cliente puede usar para obtener los *SD&S Discovery Records*:

- *Pull Mode*: el usuario pide explícitamente el *SD&S Discovery Record* que quiere recibir. Para ello se utiliza el protocolo HTTP y el transporte es unicast sobre TCP.
- *Push Mode*: el SP envía periódicamente el *SD&S Discovery Record* vía multicast (en modo carrusel) y el usuario debe tan sólo unirse a los grupos multicast donde se envían los *Records*. Para ello se utiliza un protocolo nuevo, DVBSTP (*DVB SD&S Transport Protocol*) que adapta los documentos XML para su transporte sobre UDP. DVBSTP proporciona campos que permiten especificar el tipo de record XML transportado; los números de identificación, sección y fragmento, que permiten enviar los XML en partes que no superen la MTU (*Maximum Transfer Unit*) de la red subyacente (evitando así la fragmentación a nivel IP); y el número de versión, que permite actualizar partes concretas del XML sin tener que reenviarlo completamente. La Fig. 4 ilustra este proceso.

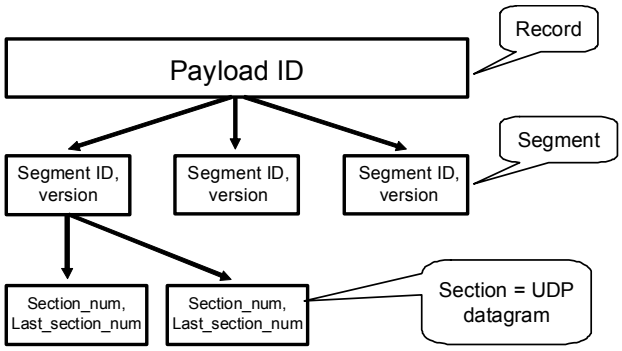


Fig. 4. Fragmentación de SD&S sobre DVBSTP.

Para su implementación, se han creado:

- *Servidor DVB-IP*: para el modo *Pull* se ha instalado el Servidor *Apache* como servidor HTTP, integrando en él dos códigos *PHP* para seleccionar automáticamente en el servidor los documentos SD&S pedidos por el cliente. Para el modo *Push* se ha modificado un código desarrollado en otro proyecto [3] para crear el servidor DVBSTP.
- *Cliente DVB-IP*: se han desarrollado tanto un cliente HTTP "de bolsillo" con la funcionalidad mínima, como un cliente DVBSTP, integrados en el módulo *client_SD.c*, que incluye todas las funciones del Cliente DVB-IP necesarias para SD&S.

C. Operaciones del proceso SD&S

El proceso de *Service Discovery*, ilustrado en la Fig. 5, consta de los siguientes pasos:

1. *Determinación de los Puntos de Entrada* (*Entry Points*): este es el primero paso, necesario para descubrir los Puntos de Entrada, a través de los cuales es posible recibir los *SP Discovery Records*. Se puede encontrar una lista con las diferentes opciones en [1], de las cuales se han implementado las siguientes, con el orden de prioridad de utilización indicado:
   I) Vía *DHCP option 15*, con el cual es posible conocer los puntos de entrada a través de las entradas DNS SRV (por ejemplo, si tenemos una entrada SRV de la forma *_dvbservdsc_.udp.dvb-ip.upc.es*, aparece el nombre del SP y se indica el uso de UDP multicast).
   II) A través de una dirección multicast especificada en [1], concretamente 224.0.23.14.
   III) Manualmente, especificando la URL de HTTP o bien la dirección IP multicast y el número de puerto utilizado, que por defecto es 3937 (*dvbservdscport*).
2. *Recepción de SP Discovery Records*: después de haber obtenido los Puntos de Entrada, nuestra atención se mueve a la recepción de *SP Discovery Records* para cada Punto de Entrada y la sucesiva selección del SP que se desee.
3. *Recepción de los DVB-IPTV Offering Records:* una vez seleccionado el SP, tan sólo queda por escoger el tipo de servicio que se quiere recibir y pedir al SP los correspondientes *DVB-IPTV Offering Records*, que contienen dicho servicio.

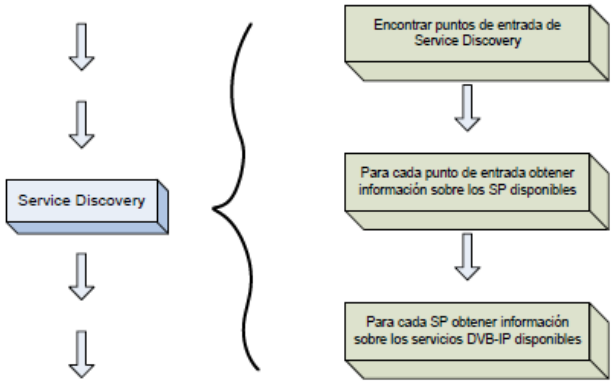


Fig. 5. Proceso de *Service Discovery*.

A. Selección

Por *Selection* se entiende aquella parte de SD&S en la cual el usuario escoge el servicio que desea recibir. Hay dos métodos de selección, en función del modo (*push* o *pull*):

- RTSP (*Real Time Streaming Protocol*) para *Content on Demand* en modo *pull*: mediante una URL del tipo `rtsp://dirección_IP/contenido` y el diálogo RTSP sobre TCP.
- IGMP (*Internet Group Management Protocol*) para *Live Media Broadcast* en modo *push*. La única operación necesaria es unirse al grupo multicast en el que se transmite la información, cuya dirección se ha determinado mediante el *SD&S Discovery Record*.

Para el modo *push* basta con abrir sockets multicast, mientras que el modo *pull* exige la integración de una librería RTSP [4] o de un servidor de streaming tipo Darwin que integre señalización RTSP [5].

VI. Transporte de los contenidos DVB

Esta parte se centra en el transporte de los contenidos DVB sobre redes IP y los protocolos involucrados, así como los métodos de protección y corrección de errores.

A. Contenido y protocolos de transporte

DVB-IP define el transporte de flujos MPEG-2 sobre *Transport Stream* (TS) mediante dos modalidades de entrega: IP/UDP/RTP/TS o directamente IP/UDP/TS, sin RTP. Los paquetes TS recibidos en los multiplex DVB son unidades de longitud fija (188 bytes) y "limpios", en el sentido de haberles despojado de todos los campos relacionados con la corrección de errores de los sistemas de transmisión DVB (por ejemplo, el código bloque Reed-Solomon (204,188) habitual en DVB-T/S/C).

En función de la MTU de la red de capa 2 que se esté utilizando, se acumulan tantos paquetes TS como sean necesarios para llenar el datagrama, siguiendo el criterio habitual de evitar a toda costa la fragmentación a nivel IP. En el caso típico (Ethernet con MTU de 1518 bytes, de los cuales 1460 son de carga útil, una vez descontadas las cabeceras Eth/IP/UDP/RTP), se transportan 7 paquetes TS con un total de 1316 bytes. El caso "UDP directo" es similar, sin RTP.

La razón por la cual se acepta la transmisión de los TS directamente sobre UDP es que los campos de la cabecera TS se solapan, en muchos casos, con los de RTP: existe un número de secuencia, un identificador de flujo, y una marca temporal (*timestamp*), que son básicamente las razones por las que se desarrolló RTP (como "suplemento" a UDP, que no disponía de ellos) [6].

En nuestro demostrador hemos usado el software `dvbstream` [7] como servidor, debido a la sencillez de la integración del código de acceso a las tarjetas DVB y la transmisión sobre IP; y *SMplayer* [8] como reproductor.

B. Application Layer Forward Error Correction (AL-FEC)

En principio, el transporte de DVB-IP se debe realizar sobre redes con calidad de servicio del tipo Servicios Diferenciados (*DiffServ*). Sin embargo, puesto que no siempre será posible (e incluso si lo es, y dado que DiffServ sólo ofrece calidad de servicio estadística y no estricta), pueden darse pérdidas de datagramas. Para proteger la información MPEG-2 de estas pérdidas se propone el uso opcional de una colección de técnicas de corrección de error a nivel de aplicación (por encima de la capa de transporte) que DVB-IP denomina AL-FEC [9]. Ésta es una de las novedades más importantes definidas en DVB-IP.

AL-FEC protege los datos creando uno o más flujos FEC, independientes del flujo de los datos protegido, siguiendo un esquema multicapa. Cada capa adicional requiere un flujo RTP (y RTCP) en puertos UDP crecientes. De esta manera, si hay clientes que no suportan AL-FEC, podrán seguir recibiendo los contenidos de la capa base aunque ignoren los flujos FEC adicionales.

- *Capa base*: es un código simple del tipo "paridad de entrelazado de paquetes" (*packet-based interleaved parity code*), definido por SMPTE (*Society of Motion Picture and Television Engineers*) [10]; este nivel es obligatorio si se usa AL-FEC, y se transporta en el puerto n+2, si tomamos como puerto n el del flujo RTP sin proteger. Los puertos impares se reservan para RTCP.
- *Capa de mejora*: este nivel es opcional y utiliza códigos *Fountain* del tipo *Raptor* [9]. Se trata de códigos convolucionales muy avanzados y potentes, que se transportan con RTP en los puertos n+4, n+6, etc. Esta parte no la hemos implementado todavía.

C. Detalles de la implementación del FEC SMPTE

El FEC base definido por SMPTE consiste en el cálculo de paridad de una matriz de entrelazado del contenido útil de los paquetes RTP, generando símbolos de reparación (*repair symbols*, los datos FEC) mediante una operación XOR (OR exclusivo) bit a bit entre un grupo de símbolos fuente (*source symbols*, los contenidos útiles de RTP). Se generan así un flujo RTP de fuente (*source flow*) que lleva los *source symbols*, y un flujo de reparación (*repair flow*) por separado.

La Figura 6 ilustra el esquema descrito para el caso de una matriz bidimensional de L columnas por D filas, donde cada posición corresponde a la carga útil de un paquete RTP, y se genera un paquete FEC por cada fila o columna, con un total de L+D paquetes de reparación.

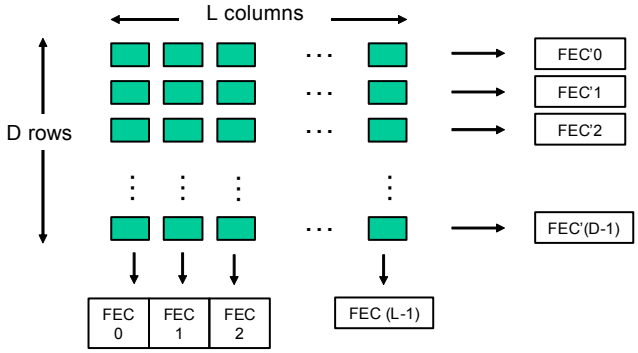


Fig. 6. Ilustración del entrelazado 2D.

El método permite la corrección de hasta un error por fila o columna, lo que posibilita recuperar situaciones "complicadas" como la ilustrada en la Fig. 7, pero en cambio fallaría si perdiéramos simultáneamente los paquetes 4, 5, 10 y 11, puesto que no hay manera de reparar ninguna fila o columna con dos fallos, de manera aislada.

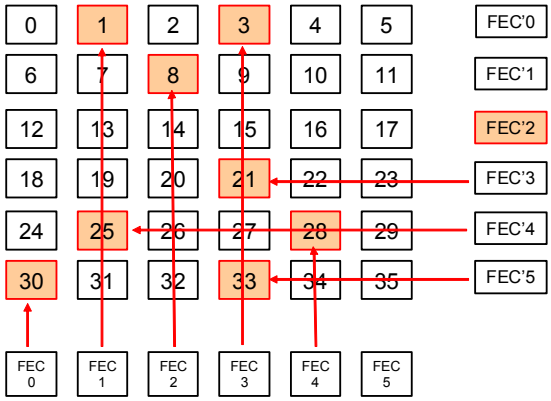


Fig. 7. Proceso de corrección. Los paquetes sombreados son los perdidos.

Nuestra implementación se limita por ahora a una versión unidimensional como la descrita en [11] con LxD limitado a 400 paquetes, y con el envío "en bloque" de los paquetes FEC después del envío de los paquetes de información. Es posible y recomendable (aunque no obligatorio) entrelazar el envío de los FEC con los paquetes originales.

VII. BROADBAND CONTENT GUIDE (BCG)

A. Definición

Con la llegada de la televisión digital y su amplia oferta de servicios se hace necesaria la utilización de algún medio que permita mostrar al usuario los múltiples contenidos multimedia que puede visualizar, así como cierta información sobre estos, por ejemplo, sinopsis, momento de emisión, formato de audio y video, etc. Este servicio de información se conoce como EPG (*Electronic Program Guide*), y es la que se transporta en las tablas *Service Information* (SI) de DVB.

Sin embargo, además de esta funcionalidad, una EPG ofrece un gran abanico de posibilidades comerciales, como la personalización de menús adaptados a cada usuario basados en sus preferencias o la elaboración de estadísticas sobre la forma en que los consumidores utilizan los servicios, que pueden ser de interés para el desarrollo de nuevos contenidos. Si a esto se añade la convergencia de la televisión hacia un nuevo dominio que aúna la TV con Internet, las posibilidades son infinitas. Supongamos que el proveedor de servicios Cuatro está emitiendo la película La ventana secreta, de la cual el actor Johnny Depp es el protagonista. Además de los datos habituales sobre sinopsis, actores, director, etc., la EPG podría mostrarnos un enlace a la filmografía del actor, permitirnos comprar en línea otras películas del mismo actor o subscribirnos a un grupo para recibir noticias sobre próximas emisiones de alguna de sus películas. Esto permite el desarrollo de nuevos modelos de negocio para los operadores de TV basados en servicios innovadores e interactivos, como por ejemplo la posibilidad de comentar con otros internautas determinados contenidos que están siendo emitidos en vivo o realizar votaciones por parte de los telespectadores.

BCG (*Broadband Content Guide*) es la parte del estándar de DVB-IP dedicada a definir las especificaciones para la implementación de una guía de contenidos EPG enriquecida que es transportada sobre una red IP bidireccional [12]. Pese a formar parte del estándar DVB-IP y ser transportada sobre una red IP, podría ser utilizada para describir contenidos transmitidos sobre cualquier tipo de red (IP, DVB-T/S/C).

B. Relación con TV-Anytime

El estándar BCG define una serie de restricciones sobre las especificaciones TV-Anytime [13], en las que se basa. TV-Anytime tiene como objetivo proporcionar un marco para el desarrollo de servicios que permitan el almacenamiento digital y la transmisión de contenidos audiovisuales y de otros tipos de servicios en plataformas de consumidores. Un sistema TV-Anytime comprende tres elementos: un proveedor de servicios que proporciona el servicio TVA, un proveedor de transporte que se encarga de la transmisión del servicio y un equipo en la vivienda del usuario que almacena el contenido y lo reproduce ante la petición del consumidor.

C. Arquitectura

BCG ofrece dos posibilidades para la transmisión de datos: 1) utilización de un mecanismo basado en containers, transmitidos en modo multicast o unicast; o bien 2) mediante un mecanismo de consultas, que precisa de un canal bidireccional, por lo que el transporte debe ser unicast.

Las razones por las que se ha elegido el mecanismo de consultas frente al de containers en nuestro demostrador son varias, destacando su capacidad para el envío de un conjunto de metadatos más completo debido a un ancho de banda menos restrictivo, así como la posibilidad de que proveedores o clientes BCG sin acceso a una red broadcast puedan ofrecer o acceder a los servicios [14].

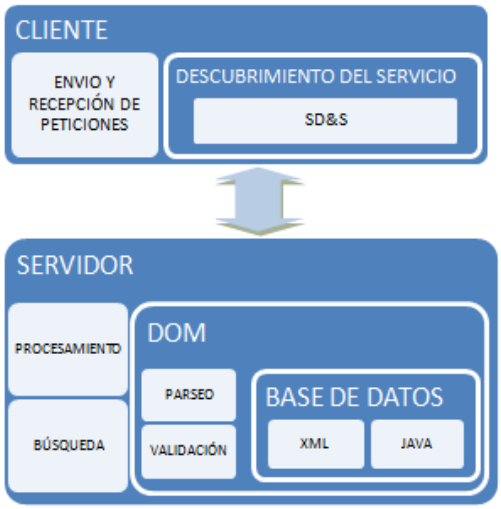


Fig. 8. Escenario y módulos BCG.

La arquitectura del servicio construido, ilustrada en la Fig. 8, es la siguiente:

- Se sigue el modelo cliente-servidor, donde el usuario envía consultas que el servidor responde tras procesar la información de la que dispone en su base de datos.
- El intercambio de peticiones y repuestas entre cliente y servidor se lleva a cabo por medio de un Servicio Web construido para tal fin a partir del documento WSDL (*Web Services Description Language*) que define su estructura y que está especificado por TV-Anytime. La transmisión de los mensajes se realiza utilizando el protocolo SOAP (*Simple Object Access Protocol*), que encapsula documentos XML, transportados sobre HTTP, tal como ilustra la Fig. 9.

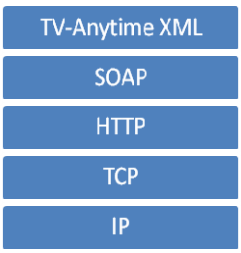


Fig. 9. Pila de protocolos para el servicio BCG.

- La base de datos del servidor está compuesta por un conjunto de documentos XML en los que están contenidos los metadatos sobre determinados servicios que el proveedor ofrece. Dichos documentos XML deben ser bien formados y válidos con respecto a los XML *Schema* que TV-Anytime especifica.
- Para procesar los documentos XML se utiliza un *parser* DOM (*Document Object Model*), de forma que tras su

validación y procesado se obtiene un árbol DOM. Éste será recorrido para obtener la información que el usuario requiere en su consulta, operación que se realiza mediante código Java.

Para usar al servicio BCG, un usuario debe acceder mediante el correspondiente Servicio Web, pero para ello debe primero saber su localización, lo que se conoce como descubrimiento del servicio. Mediante SD&S, concretamente utilizando los campos *HTTP@Location* y *HTTP@SOAP* del documento XML *BCG Discovery Record*, el cliente puede obtener la URL en la que el servicio se encuentra publicado y así comenzar el proceso de consultas.

D. *Tipos de servicio y funcionalidades*

Los servicios de metadatos TV-Anytime pueden ser clasificados en dos tipos [15]:

- Recuperación de datos: Un determinado cliente desea obtener información sobre un determinado servicio, por ejemplo, consulta de la programación para determinado canal y día.
- Envío de metadatos del usuario: Consiste en el envío de un historial de uso del servicio por parte del cliente al proveedor de servicios. Esta operación ofrece ventajas en cuanto a personalización de información adaptándola a usuarios concretos.

BCG contempla en su estándar únicamente dos operaciones de las definidas por TV-Anytime: *get_Data* y *submit_Data*, que se corresponden con los tipos de operación recuperación de datos y envío de metadatos del usuario, respectivamente. Además, para cada una de estas dos operaciones se define la correspondiente operación de descripción: *describe_get_Data* y *describe_submit_Data*, cuya función es la de proporcionar información sobre las capacidades del proveedor respecto a las tablas de datos de las que dispone para ser consultadas, elementos sobre los que se puede realizar una búsqueda, información que desea que el usuario le envíe, etc.

Fig. 10. Uso de un servicio BCG.

La Fig. 10 ilustra los pasos seguidos en la consulta de un servicio BCG:

- Inicialmente se debe descubrir el servicio mediante SD&S, de la forma que ya se ha indicado.
- A continuación se obtienen las capacidades de funcionalidad del servidor mediante el envío de un mensaje *describe_operación*.
- Por último, se puede comenzar a enviar peticiones de consulta al servicio de metadatos.

E. *Implementación del servicio BCG*

Para la implementación del servicio web BCG se ha usado Apache Tomcat 6.0 [16] como servidor web y contenedor de *servlets*. Sobre él se ha instalado la plataforma Apache Axis2/Java 1.5 [17], una herramienta que da soporte a Servicios Web que utilizan los protocolos SOAP y WSDL. Axis2 proporciona diversas herramientas para la generación de un servicio web, de las cuales se ha utilizado *wsdl2java,* cuya función es la de generar parte del código de un Servicio Web Java de manera automática, a partir del correspondiente documento de definición del servicio WSDL. En este aspecto, la versión 1.5 de Axis2 tiene una limitación que no será solucionada hasta la publicación de la nueva versión 1.6. Se trata del bug AXIS2-4273 que impide que el servicio web funcione de forma adecuada en determinadas ocasiones debido a que parte del código generado por Axis2 es erróneo. Este problema ha sido solucionado identificando las secciones de código problemáticas y re-programando a mano dichas secciones (ver [18] para más detalles).

En la fase de desarrollo se ha utilizado la aplicación Eclipse que permite la creación y administración de servicios web mediante su plataforma WTP (*Web Tool Platform*) haciendo uso del servidor Tomcat y Axis2. Además, para la verificación de funcionamiento del Servicio Web se ha utilizado la aplicación TCPMon, cuya finalidad es la monitorización de los mensajes intercambiados en una conexión TCP.

Los documentos XML utilizados como base de datos del servicio de ejemplo usado para probar nuestro despliegue han sido creados por la BBC (*British Broadcasting Corporation*) [19] y se ofrecen como parte de un servicio experimental cuyo propósito es ofrecer un conjunto de metadatos que sirva como material de pruebas para desarrolladores de aplicaciones TV-Anytime. Dichos documentos son actualizados a diario e incluyen distintos tipos de tablas definidas por TVA en las que se almacena información sobre los canales ofrecidos, programas y su localización, grupos de programas, resolución de contenidos, etc. Las funcionalidades implementadas en la actualidad para dicha base de datos comprenden la consulta de las tablas *Service Information*, *Program Information, Program Location, Group Information* y *Content Referencing* definidas por TV-Anytime y permite realizar búsquedas en base a los siguientes elementos: nombre y URL del servicio, título, sinopsis, género, identificadores de programa o grupo de programas y localizadores de contenidos (ubicación real tanto espacial como temporal donde dicho contenido puede ser encontrado).

VIII. CONCLUSIONES Y LÍNEAS FUTURAS DE DESARROLLO

Las tecnologías relacionadas con la televisión se encuentran en un momento de profundo cambio impulsado por la modificación de los hábitos de consumo de los usuarios. Debido a esto se está produciendo una convergencia que tendrá como resultado la unificación de la

TV con Internet. DVB-IP ofrece una solución integrada y estandarizada para el despliegue de servicios de TV digital sobre redes IP, integrando todos los aspectos de un sistema completo: desde la configuración automática del terminal, hasta servicios de guía enriquecida de programas, pasando por los aspectos de descubrimiento y selección de servicio, y transporte con corrección de errores, entre otros.

Se ha desarrollado un demostrador DVB-IP basado en hardware DVB de bajo coste y software *open source*. El demostrador es plenamente funcional y equivalente al perfil *Live Media Broadcast* con el añadido opcional de BCG (con un servicio ficticio de consulta de programas basado en el servicio TV-Anytime de la BBC) y la protección de errores AL-FEC en su versión básica (unidimensional y basado en paridad). Precisamente estos dos últimos aspectos, junto con la implementación de del protocolo de transporte DVBSTP, son los más novedosos de nuestro desarrollo. Para una descripción más detallada del diseño, consultar [3, 18, 20].

Entre las líneas en las que estamos trabajando para completar el demostrador, destacan como prioritarias:

- Conseguir la funcionalidad del perfil *Content on Demand* mediante la integración de un servidor de *streaming* con señalización RTSP, lo cual requerirá código adicional, ya que el perfil RTSP de DVB-IP difiere ligeramente del definido por la IETF, en cuanto a la obligatoriedad de ciertas peticiones y respuestas.
- Completar la implementación de AL-FEC, extendiendo el código al caso 2D y aumentando la capacidad de corrección mediante el uso de capas adicionales basadas en el código *Raptor* [9], así como su evaluación sistemática mediante la introducción de patrones de pérdidas y errores con DummyNet [21]. También es interesante la introducción de las retransmisiones de RTP y su evaluación en servicios interactivos y no interactivos de difusión de TV.
- En cuanto a BCG, se podría aumentar su funcionalidad mediante la definición de una política de privacidad para los datos que el cliente envía al servidor en forma de historial de uso, o la ampliación de la capacidad de búsqueda de la base de datos incluyendo nuevas tablas y nuevos criterios de consulta (elementos, anidación de predicados lógicos) y ordenación, entre otras opciones.
- El desarrollo de un módulo *Content Download Service*, (todavía en fase de definición y estandarización por parte de la ETSI), integrando servicios de distribución de vídeo en tiempo no real del tipo P2P y FLUTE.

Pese a que el trabajo realizado es completamente funcional, queremos completarlo (especialmente la parte de vídeo bajo demanda) y evaluar su rendimiento como sistema integrado, antes de hacer público el código.

Tal como se describe en la sección II.C, DVB-IP integra buena parte de los protocolos y arquitecturas de servicio actuales del mundo IP. Es por ello que el desarrollo de un escenario de este tipo puede tener, aparte del valor puramente técnico, un componente docente en el contexto de una titulación de Ingeniería Telemática, en una asignatura sobre Protocolos y Servicios IP, o una de Servicios Audiovisuales sobre IP (siendo este el caso de la EPSC). El demostrador puede ser un magnífico ejemplo del funcionamiento de cada protocolo por separado (teoría), y configuración de servidores (práctica), y por otra parte del funcionamiento integrado (visión sistémica) de un servicio completo, aparte del atractivo técnico y docente del servicio de TV sobre IP. Una posibilidad que estamos barajando de cara a la puesta en marcha de la asignatura en la EPSC es la compra de una cierta cantidad de receptores DVB-T ("*sticks*" como los presentados en [22]) y asignarlos a cada grupo de 2 o 3 estudiantes, que junto con un puesto de laboratorio compuesto por 3-4 ordenadores podrían ir montando, de manera acumulativa durante todo el cuatrimestre, un mini-escenario que incluya los servidores DVB-IP y un prototipo de cliente; es decir, que monten un demostrador DVB-IP propio. Esta metodología de trabajo en grupo se podría combinar con el uso de técnicas PBL (*Project Based Learning*, al estilo de la experiencia presentada en [23]), en el que los estudiantes propondrían soluciones a los retos técnicos de cada módulo funcional DVB-IP.

AGRADECIMIENTOS

Los autores agradecen a los revisores sus sugerencias, así como el apoyo de la EPSC (CARPAD), i2Cat y el MICINN/FEDER (TSI2007-66637-C02-01 y TEC2009-13901-C02-01).

REFERENCIAS

[1] ETSI TS 102 034 V1.4.1 "Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks", August 2009.
[2] ETSI A118 Rev1 "DVB-IP profiles for DVB-IPTV", June 2008
[3] Eugenio Viudez, "Desarrollo de un cliente DVB-IP con perfil Live Media Broadcast (LMB)". Trabajo Fin de Carrera. EPSC, UPC, 2008.
[4] RTSP library (live555.com) http://www.live555.com/openRTSP/
[5] Darwin streaming server http://developer.apple.com/opensource/server/streaming/index.html
[6] H. Schulzrinne et al, IETF RFC 3550, "RTP: A Transport Protocol for Real-Time Applications".
[7] dvbstream http://packages.debian.org/testing/video/dvbstream
[8] SMPlayer, http://smplayer.org/
[9] ETSI TS 102 542-3-2 V1.3.1 "Digital Video Broadcasting (DVB); Guidelines for the implementation of DVB-IPTV Phase 1 specifications; Part 3: Error Recovery; Sub-part 2: Application Layer - Forward Error Correction (AL-FEC)", January 2010.
[10] SMPTE specification 2022-1 "Forward Error Correction for Real-time Video/Audio Transport over IP Networks", 2007.
[11] RTP Payload Format for 1-D Interleaved Parity FEC, http://tools.ietf.org/html/draft-ietf-fecframe-interleaved-fec-scheme-09
[12] ETSI TS 102 539: "Digital Video Broadcasting (DVB); Carriage of Broadband Content Guide (BCG) information over Internet Protocol".
[13] ETSI TS 102 822-2: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("*TV-Anytime*"); Part 2: Phase 1 - System description", April 2008
[14] ETSI TS 102 542-2: "Digital Video Broadcasting (DVB); Guidelines for the implementation of DVB-IPTV Phase 1 specifications; Part 2: Broadband Content Guide (BCG) and Content on Demand", Jan 2010.
[15] ETSI TS 102 822-6-1: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 6: Delivery of metadata over a bi-directional network; Sub-part 1: Service and transport", April 2008.
[16] ApacheTomcat http://tomcat.apache.org/
[17] Apache Axis2/Java http://ws.apache.org/axis2/
[18] I. Rodríguez, "Desarrollo de un módulo Broadband Content Guide (BCG) para DVB-IP", PFC. Univ. Vigo - UPC, Barcelona, Mayo 2010.
[19] BBC TV-Anytime Data http://backstage.bbc.co.uk/feeds/tvradio/doc.html
[20] F. Granaiola, "Deployment and development of a DVB-IP scenario" MsC Thesis, University of Pisa - UPC, Barcelona, April 2010.
[21] L. Rizzo, DummyNet http://info.iet.unipi.it/~luigi/dummynet/
[22] Hauppauge NOVA-T USB DVB-T stick http://www.hauppauge.co.uk/site/products/data_novatdstick.html
[23] S. Machado et al, "Juegos en red como proyecto docente en Ingeniería Telemática", JITEL 2005, pp 81-86, Vigo, Septiembre 2005.

Acceso y automatización de trámites administrativos a través de dispositivos móviles

Laura Díaz-Casillas, Luis Delgado, Sergio García, Alejandro López, Mercedes Garijo
Departamento de Ingeniería de Servicios Telemáticos
Universidad Politécnica de Madrid
Avenida Complutense 30, Madrid (España)
{ldcasillas, ldelgado, sgalobo, alopez, mga}@dit.upm.es

***Resumen*—En este artículo se presenta un sistema multiagente mediante el cual se pretende automatizar la gestión del trámite de matriculación, facilitando su acceso a través de terminales móviles. En concreto, el sistema presenta un agente secretaría, encargado de determinar los procesos involucrados en dicho trámite mediante un flujo de trabajo, y un agente alumno, responsable de interaccionar con los estudiantes a través de una interfaz adaptada a dispositivos móviles, en concreto, terminales que dispongan del sistema operativo Android.**

***Palabras Clave*—matriculación, agentes, JADE, flujo de trabajo, móviles, Android**

I. Introducción

Actualmente, se está realizando una gran esfuerzo en la Administración Pública, tanto a nivel nacional como europeo, para facilitar a los usuarios finales el acceso a los servicios proporcionados por ésta.

Existen múltiples factores que dificultan dicha labor, entre los que destaca la complejidad de los procesos implicados, debida por un lado a la estructuración del proceso y por otro, al número de participantes que intervienen en él, parámetros que en muchos casos ofrecen una amplia diversidad entre unas aplicaciones y otras.

Con el propósito de solventar esta problemática surge el proyecto AdmiTI2 [1], cuyo objetivo principal es desarrollar una plataforma de código abierto en la que se integren varias herramientas colaborativas a través de las cuales mejorar la eficiencia y la productividad en las relaciones de los usuarios con las administraciones públicas, más concretamente, con las administraciones relacionadas con el ámbito educativo.

AdmiTI2 pretende realizar avances en este campo aplicando nuevas tecnologías para proporcionar una serie de mecanismos genéricos, adaptables a las características de cada caso, a través de los cuales permitir la gestión de trámites educativos de manera eficiente, integrada y homogénea.

Uno de los puntos claves del proyecto consiste en permitir el acceso móvil a dichos trámites. Debido a la reducción de precios en los terminales móviles con acceso a Internet, cada día un mayor número de usuarios dispone de este tipo de dispositivos, por lo que constituye un área de gran interés el desarrollar mecanismos para facilitar el acceso a los servicios desde dichos terminales.

En este contexto, se ha desarrollado un sistema multiagente que se basa en el uso de flujos de trabajo para automatizar las acciones a realizar durante el proceso de matriculación, al que los usuarios acceden a través de dispositivos móviles.

El resto del artículo se organiza de la siguiente manera: en la sección II se realiza una introducción a las principales tecnologías utilizadas, para, a continuación, mostrar en la sección III las soluciones específicas empleadas. En la sección IV se expone una descripción del sistema desarrollado y en la sección V se muestran trabajos relacionados. Por último, en la sección VI, se presentan las conclusiones y líneas futuras de trabajo.

II. Tecnologías empleadas

En la Administración se llevan a cabo numerosos trámites a diario que requieren la ejecución de varios procesos y la intervención de diversos usuarios de manera ordenada, lo que conlleva cierta complejidad a la hora de realizar dichos trámites.

Una forma de facilitar la definición y gestión de estos trámites es mediante el uso de flujos de trabajo. En concreto, un flujo de trabajo [2] posibilita la automatización de una serie de procesos, donde la información y las tareas son manejadas por distintos participantes, atendiendo a una serie de reglas que permiten alcanzar o contribuir a un objetivo de negocio establecido. El uso de flujos de trabajo presenta diversas ventajas, entre las que destacan el facilitar la comprensión, actualización y escalabilidad del sistema, lo que los hace adecuados para su aplicación en la Administración. Así podemos encontrar varios ejemplos de uso en este entorno, como el de Xin [3], donde se emplean flujos de trabajo para desarrollar un centro colaborativo a través del cual gestionar y controlar los procesos de aprobación del gobierno (*e-goverment*), y Verginadis [4], que propone el uso de flujos de trabajo para facilitar la gestión de los servicios de la Administración e implementa una marco de trabajo que permite su desarrollo y facilita su reutilización.

El uso de un flujo de trabajo permite controlar qué proceso ejecutar en cada momento y determinar las interacciones entre ellos, pero además es necesario considerar cómo implementar cada uno de los procesos y su comunicación. Existen varios mecanismos para ello, desde la forma manual hasta la basada en agentes, pasando por aproximaciones en las que se emplean bases de datos. Singh expone en [5] las ventajas de emplear un sistema multiagente, pues éste se adapta mejor a las características impuestas por los sistemas en los que se emplean flujos de datos, habitualmente complejos, heterogéneos y desplegados sobre entornos dinámicos, al facilitar la interacción entre diversos procesos, permitiendo la ejecución flexible de los flujos de trabajo.

Otro parámetro importante a tener en cuenta a la hora de facilitar la gestión de los trámites es su acceso. Gracias a que en los últimos años el número de usuarios con dispositivos

móviles ha aumentado exponencialmente, es posible pensar en el acceso desde cualquier parte y en cualquier lugar. Desafortunadamente, las características de los dispositivos móviles son aún limitadas, siendo necesario adaptar las aplicaciones a este tipo de dispositivos [6]. Existen diversas opciones para tal propósito, desde navegadores móviles, con iniciativas como los dominios .mobi y las hojas de estilo para móviles, que pretenden adaptar las aplicaciones Web, hasta sistemas operativos móviles, los cuales ofrecen un entorno de despliegue completo, pasando por la tecnología J2ME (*Java Platform Micro Edition*) [7], que permite el desarrollo de aplicaciones Java. En la actualidad, J2ME es la tecnología más extendida gracias a su independencia con respecto al dispositivo sobre el que se ejecuta. Pero aún así, es necesario realizar ajustes si se desean aprovechar al máximo las características de cada terminal.

Por todo ello, se propone realizar una aplicación adaptada a dispositivos móviles que automatice la gestión de los trámites educativos mediante el uso de flujos de trabajo a través de un sistema multiagente.

III. Soluciones tecnológicas

El empleo de un sistema multiagente permite la interacción, colaboración y cooperación entre diversas entidades autónomas o agentes, orientadas a la realización de una función concreta. Dicho sistema se basa en la plataforma JADE, la cual proporciona un entorno de ejecución adecuado a los requisitos demandados por los agentes, además de una serie de mecanismos que facilitan su implementación y diversos módulos que permiten ampliar sus funcionalidades, entre los que se encuentra una versión reducida para dispositivos móviles. WADE extiende JADE, permitiendo definir flujos de trabajo para determinar el comportamiento de los agentes, en este caso, destinados a los procesos relacionados con la gestión de los trámites administrativos, con un alto nivel de detalle. El despliegue de la aplicación sobre Android habilita el acceso desde dispositivos móviles que presenten dicho sistema operativo. Además, gracias a la independencia de la plataforma de agentes empleada con la tecnología subyacente, es posible ampliar el sistema a otro tipo de dispositivos.

A continuación, se muestra una breve descripción de cada una de las tecnologías empleadas:

A. JADE

JADE (*Java Agent DEvelopment framework*) [8] es una plataforma de software libre basada en Java que facilita el desarrollo de sistemas multiagente. JADE se caracteriza por cumplir con las especificaciones FIPA (*Foundation for Intelligent Physical Agents*) [9] y presentar una serie de herramientas gráficas que facilitan las tareas de depuración y despliegue.

Los agentes desarrollados con JADE se encuentran desplegados en contenedores, los cuales pueden estar situados en distintas máquinas. De entre todos los contenedores, existe uno, conocido como contenedor principal, que contiene dos agentes esenciales para el correcto funcionamiento de la plataforma:

- AMS (*Agent Management System*), encargado de gestionar el sistema, pudiendo crear y eliminar agentes o parar la plataforma, entre otros. Posee además un servidor de nombres responsable de la identificación de los agentes.
- DF (*Directory Facilitator*), cuya misión es informar sobre los agentes disponibles en la plataforma.

JADE se caracteriza además por presentar un conjunto de extensiones que permiten ampliar sus funcionalidades con el objetivo de poder adaptarse a diversos entornos. Así por ejemplo, posibilita la integración de los agentes con Jess [10], facilitando el uso de sistemas expertos, y con sistemas OSGi [11], entre otros. A destacar es la distribución conocida como LEAP [12], una versión reducida de JADE, que permite desplegar agentes en dispositivos móviles.

B. WADE

WADE (*Workflows and Agents Development Environment*) [13] aporta a JADE la posibilidad de definir las tareas de ejecución de los agentes mediante flujos de trabajo, además de una serie de mecanismos que facilitan su gestión, en términos de administración y tolerancia a fallos. Normalmente, los flujos de trabajo se emplean para gestionar la relación entre sistemas a alto nivel, pero WADE se caracteriza por trabajar a bajo nivel, permitiendo desarrollar aplicaciones complejas, en las que intervengan múltiples tareas.

Para la representación de los flujos de trabajo, WADE adopta un metamodelo del flujo de trabajo derivado de XPDL (XML *Process Definition Language*) [14], en el que cada una de las tareas involucradas se definen como procesos. Éstos se encuentran formados por una serie de actividades que determinan la ejecución de un conjunto de operaciones. En cada proceso se define una única actividad inicial y una o más actividades finales. Las relaciones entre las actividades se determinan mediante transiciones, las cuales suelen presentar condiciones que establecen los requisitos que deben cumplirse para su ejecución. Además, los procesos pueden tener asociados uno o más parámetros formales que determinen los tipos de datos de entrada admitidos y los resultados esperados.

El uso de WADE facilita la definición y modificación de los procesos involucrados en el flujo de trabajo, lo que favorece su control, mantenimiento y actualización futura.

Junto a WADE se presenta un entorno de desarrollo, en concreto un *plugin* de Eclipse llamado WOLF (*WOrkflow LiFe cycle management environment*) [15], que facilita la creación de este tipo de aplicaciones.

C. Android

Android [16] es un sistema operativo para dispositivos móviles basado en Linux. Su código fue liberado en noviembre de 2007, aunque el primer dispositivo que soportaba dicha tecnología no apareció hasta octubre de 2008. Desde entonces, el número de usuarios ha ido en aumento.

Los elementos principales que componen su arquitectura son:

- Aplicaciones básicas, entre las que se encuentran un cliente de correo electrónico, un gestor de SMS, un calendario, un navegador y un gestor de contactos.
- Marco de aplicaciones, el cual facilita el acceso a los recursos del sistema a través de una serie de gestores que controlan tareas fundamentales, encargadas de la localización, las notificaciones del sistema y las operaciones sobre el teléfono, entre otras.

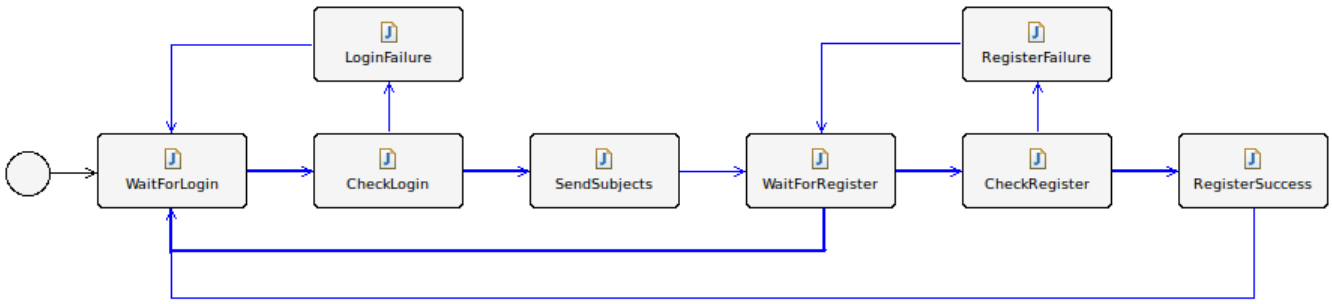


Figura 1: Flujo de trabajo del agente secretaría

- Conjunto de bibliotecas C/C++, usadas por varios componentes del sistema, a las que se accede a través del marco de aplicaciones.
- Android *runtime*, que contiene bibliotecas básicas, encargadas de proporcionar la mayor parte de las funciones disponibles en Java, y la máquina virtual Dalvik, optimizada para dispositivos móviles, sobre la que se ejecutan las aplicaciones.
- Núcleo Linux. Android se basa en la versión 2.6 de Linux para gestionar el acceso al hardware y ofrecer los servicios primarios del sistema al resto del software, como son la gestión de la seguridad, la memoria, los procesos, la conectividad y los controladores.

Las aplicaciones Android están escritas en Java, el código compilado junto con los archivos requeridos se presentan empaquetados en un archivo con extensión .apk (*Android Package*). A la hora de ejecutarse, cada aplicación se despliega sobre un proceso, que tiene su propia máquina virtual de Java y un identificador de usuario, limitando de esta forma el acceso entre aplicaciones (aunque es posible asociar un mismo identificador de usuario a dos aplicaciones, de manera que puedan compartir datos entre ambas). Pero en general, las aplicaciones pueden compartir y reutilizar elementos de otras aplicaciones. Es por ello que no tienen un único punto de inicio, pues puede ocurrir que se requiera solo una determinada parte, encontrándose estructuradas en base a componentes. Existen cuatro tipos de componentes: actividades, servicios, receptores *broadcast* y proveedores de contenidos. Las actividades se caracterizan por presentar una interfaz de usuario, al contrario que los servicios. Los receptores *broadcast* se encargan de recibir y reaccionar ante anuncios *broadcast*. Éstos pueden proceder del sistema, indicando por ejemplo que la batería se está agotando o que se acaba de realizar una foto, o de otras aplicaciones. Los proveedores de contenidos permiten que determinada información pueda compartirse entre varias aplicaciones.

Las aplicaciones desarrolladas se pueden poner a disposición del público en general en el Android Market [17]. Según Salisbuty [18], en diciembre de 2009 había 20.000 aplicaciones disponibles, igualando al mercado de Windows Mobile y superando otros, como el de Symbian.

IV. Descripción del sistema

El principal objetivo del sistema desarrollado es simplificar la tramitación de la matrícula, tanto a los alumnos como a la Administración. En concreto, se pretende facilitar la interacción del usuario alumno y de la secretaría con los distintos procesos involucrados en el trámite de matriculación. Estos procesos se encuentran implementados a través de dos tipos de agentes con distintas funcionalidades que se coordinan entre sí para alcanzar dicho objetivo:

- El agente secretaría emplea la extensión WADE para determinar el flujo de trabajo a realizar, gestionando la interacción entre los distintos procesos involucrados, facilitando a los administradores del sistema su compresión y actualización futura. Estos procesos son:
  - Registro: identificación del usuario en el sistema.
  - Estado del expediente: muestra al usuario un listado con las asignaturas aprobadas.
  - Selección de asignaturas: permite al usuario seleccionar las asignaturas en las que se desea matricular.
  - Validación de la selección: el sistema comprueba que la selección de asignaturas es adecuada.
  - Notificación al usuario: informa del fin del proceso de matriculación al usuario.
- El agente alumno es el encargado de interaccionar con el alumno, guiándole a través del proceso a realizar. Presenta una interfaz de usuario adaptada a dispositivos Android, de manera que el usuario puede acceder al sistema desde su móvil.

Ambos agentes se encuentran desplegados sobre una plataforma JADE.

A. Agente secretaría

El agente secretaría es responsable de gestionar los procesos asociados al trámite de matriculación, comportándose de acuerdo a un flujo de trabajo definido mediante WADE. Gracias a WOLF, un *plugin* de Eclipse, dicho flujo de trabajo puede ser construido gráficamente, siguiendo un esquema similar a las máquinas de estados finitos, en el que las transiciones entre estados se especifican a partir de mensajes recibidos por el agente o decisiones que éste tome. En la figura 1 se puede observar el flujo de trabajo empleado por el agente secretaría. Este flujo de trabajo presenta los siguientes estados:

- `WaitForLogin`. Estado inicial en el que el agente se encuentra esperando recibir un mensaje de tipo `Call for Proposal`, procedente de un agente alumno que desea iniciar el proceso de matriculación.
- `CheckLogin`. Una vez recibida la petición inicial, es necesario validar que se ha realizado correctamente. En

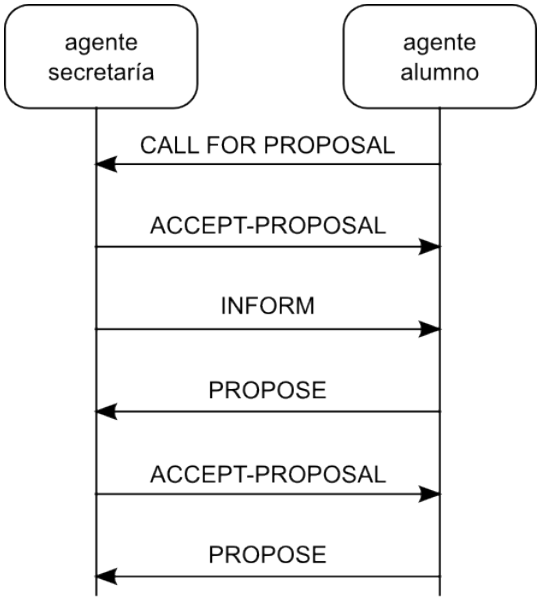


Figura 2: Intercambio de mensajes FIPA entre los agentes secretaría y alumno

caso afirmativo, se pasa al estado `SendSubjects`, mientras que en caso negativo, el siguiente estado sería `LoginFailure`.

- `LoginFailure`. El agente secretaría informa mediante un mensaje de tipo `Failure` de que el proceso de autenticación no se ha realizado correctamente.
- `SendSubjects`. En el caso de que el resultado de la validación sea positivo, se envía un mensaje de tipo `Accept Proposal`, para confirmar la conexión del alumno, y otro de tipo `Inform`, con las asignaturas en las que el alumno tiene pendientes de aprobar. Esta información se encuentra almacenada en una base de datos HSQLDB (*Hyper Structured Query Language Database*) [19], alojada en el servidor de secretaría de alumnos, y se envía en formato JSON (*JavaScript Object Notation*) [20] dentro del mensaje indicado.
- `WaitForRegister`. El agente secretaría debe esperar un mensaje de tipo `Propose`, con las asignaturas en las que el alumno desea matricularse, información enviada en formato JSON. Una vez recibido, el contenido del mensaje es procesado en el estado `CheckRegister`.
- `CheckRegister`. Este estado es responsable de verificar que la selección realizada de las asignaturas es correcta según las políticas de matriculación establecidas. En estos momentos, la única restricción impuesta consiste en asegurar que el alumno se matricula en más de una asignatura. Si el resultado de la validación es satisfactorio, el siguiente estado a ejecutar será `RegisterSucces`, en caso contrario, `RegisterFailure`.
- `RegisterFaiulure`. Si la selección de asignaturas se ha realizado de forma incorrecta, el agente secretaría envía un mensaje de tipo `Reject Proposal` al agente alumno para que éste vuelva a mostrar la lista de asignaturas disponibles y el usuario pueda realizar una nueva selección.

Figura 3: Pantallas inicial y de acceso a la matriculación

- `RegisterSuccess`. El agente secretaría debe informar al usuario de que el proceso de matriculación se ha realizado satisfactoriamente, para ello, envía un mensaje de tipo `Accept Proposal`. A continuación, el agente secretaría regresa al estado inicial en el que espera recibir el NIF de un nuevo alumno, por lo que si alguien quisiera volver a matricularse, tendría que desconectarse de la plataforma JADE y volver a conectarse.

La figura 2 muestra los mensajes intercambiados entre los agentes secretaría y alumno durante un proceso de matriculación realizado correctamente.

Por último, indicar cómo gestiona el agente secretaría la desconexión de un agente alumno. En concreto, cuando un agente alumno se dispone a desconectarse de la plataforma, envía un mensaje de tipo `Propose` informando de ello al agente secretaría. Al recibir este mensaje, el agente secretaría pasa automáticamente al estado inicial, en el que espera un mensaje con el NIF de un nuevo alumno. Es decir, en cierto sentido se reinicia el flujo de trabajo del agente para esperar la llegada de un alumno que desea matricularse.

B. Agente alumno

El agente alumno es el responsable de gestionar la interacción de los usuarios, estudiantes que desean matricularse desde un móvil Android, con secretaría. La comunicación entre ambos agentes se ha explicado en el apartado anterior. El agente alumno será responsable de recoger la información del usuario y enviar los mensajes correspondientes al agente secretaría y procesar los mensajes recibidos en respuesta a sus solicitudes, determinando la actividad adecuada a cada uno de los pasos del proceso de matriculación. A continuación se exponen las actividades involucradas:

- Inicio. Este actividad es responsable de gestionar el acceso al sistema de matriculación. Para ello, muestra una pantalla en la que se proporciona un cuadro de texto para que el usuario pueda introducir su NIF. Además, como se puede observar en la figura 3, muestra un botón mediante el cual informar al usuario de las características de la aplicación.

Figura 4: Pantallas de selección de asignaturas

Figura 5: Pantallas de confirmación de matriculación

Cuando el usuario pulsa el botón “Log in”, se crea un nuevo agente JADE en la plataforma donde reside el agente secretaría, pero en otro contenedor. Tanto el nombre del nuevo agente, como el del contenedor donde se ubica, coinciden con el NIF introducido por el alumno. A continuación, se iniciará la comunicación entre alumno y secretaría y, si el NIF es validado satisfactoriamente, comenzará el proceso de matriculación. En el caso contrario, la aplicación avisará al usuario de que el NIF introducido no es válido y el alumno volverá al punto inicial, debiendo introducir un NIF correcto.

- Matriculación. Tras este primer paso, aparece la pantalla de matriculación, mostrada en la figura 3, en la que se presentan dos botones al usuario, uno para seleccionar las asignaturas de las que desea matricularse, y otro para llevar a cabo dicha matriculación. No obstante, el segundo botón no estará activo hasta que el alumno no haya seleccionado alguna asignatura.
  Una vez realizada la selección, el alumno deberá pulsar el botón “Enviar” para mandar los identificadores de cada una de las asignaturas elegidas a secretaría. Tras procesar la solicitud, al usuario se le mostrará la pantalla de confirmación o error de la matrícula.
- Selección de asignaturas. En este punto es donde el alumno puede elegir aquellas asignaturas de las que desea matricularse. En primer lugar, se le presenta una lista de los cursos disponibles y las asignaturas optativas. Al seleccionar una de las posibilidades, aparecen las asignaturas correspondientes, tanto su nombre como su abreviatura, y la opción de seleccionarlas o no. Ambas pantallas aparecen en la figura 4. Cabe destacar que aquellas asignaturas que el alumno tiene aprobadas están inhabilitadas y no pueden marcarse, evitando así errores en la matriculación. Esta información ha sido obtenida del agente secretaría, que tras la autenticación del alumno, envió la lista de asignaturas disponibles correspondientes. El agente alumno, tras procesar dicha información, la almacena en una base de datos local SQLite [21] para poder consultarla posteriormente.
  Tras marcar las asignaturas deseadas, el usuario debe pulsar el botón de regreso para volver a la pantalla de matriculación. Observará cómo el botón “Enviar” ha sido habilitado, pudiendo aceptar la selección realizada para que dicha información sea enviada al agente secretaria.
- Confirmación/error. Finalmente, el sistema mostrará al usuario una pantalla donde se confirmará su matrícula y se le informará de las asignaturas elegidas, como se refleja en la figura 5. En el caso de que hubiera surgido algún inconveniente, se mostraría un mensaje de error indicando que la matrícula era incorrecta y es necesario realizar una nueva selección de asignaturas.
  Si el proceso de matriculación ha concluido satisfactoriamente, el usuario deberá desconectarse con el botón “Log out” y volver a conectarse con “Log in” si desea realizar una segunda matriculación de asignaturas. Si por el contrario ha habido un error en la matrícula, el alumno podrá seleccionar o eliminar las asignaturas que desee e intentar matricularse de nuevo con el botón correspondiente sin necesidad de conectarse otra vez.

El sistema ha sido probado en un entorno de desarrollo, para ello, se ha utilizado un PC con Ubuntu 9.10 y Windows 7 Professional y un terminal HTC Dream [22] con Android.

V. Trabajos relacionados

Según el Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas [23], el servicio de Matriculación Universitaria, con una disponibilidad del 97 %, es el segundo más extendido, por detrás del servicio de Quejas y Sugerencias, presentando una amplía diferencia con respecto al resto de servicios ofertados.

Habitualmente, la implementación del servicio de Matriculación se realiza de manera muy sencilla, mediante un formulario electrónico de matriculación que se envía a la facultad con los datos introducidos por el alumno. Sonntag expone en [24] la necesidad de adaptar los servicios de la Administración a los usuarios, con el fin de agilizar los trámites a realizar. Considerando que el número de usuarios

con dispositivos móviles aumenta día a día, la adaptación de los servicios a este tipo de dispositivos supone un paso importante a la hora de facilitar la gestión de los trámites administrativos [25]. Hasta ahora, la mayor parte de las aplicaciones desarrolladas para terminales móviles consistían en aplicaciones de usuario, aunque actualmente existe una tendencia hacía el desarrollo de aplicaciones empresariales [26], educativas [27] y administrativas [28]. Dentro de este último grupo, encontramos diversas categorías relacionadas con la gestión de los transportes, la sanidad, los servicios de emergencia y la educación. La gestión de la información en este tipo de aplicaciones requiere de mecanismos especiales para su tratamiento, como es el uso de flujos de trabajo, que permiten definir de forma clara las acciones y los participantes asociados a cada proceso, y sistemas multiagente, que permiten delimitar las tareas asociadas a los diferentes roles involucrados y facilitar la colaboración y cooperación entre ellos.

La combinación de estas tecnologías supone un nuevo reto que facilitará el desarrollo de nuevas funcionalidades en el futuro.

VI. Conclusiones

La gestión de los procesos asociados a los trámites administrativos es una tarea laboriosa tanto para los usuarios finales como para los empleados de la Administración. En este artículo se muestra un sistema mediante el cual se desea facilitar dicho proceso. En concreto, el sistema se encuentra compuesto por dos tipos de agentes, el primero se encarga de gestionar la parte administrativa, mientras que el segundo es responsable de la interacción con los usuarios finales. Ambos se encuentran desplegados sobre la plataforma JADE, lo que facilita la interacción entre ellos, pero mientras el primero se centra en la automatización de las actividades involucradas en los trámites a realizar durante el proceso de matriculación mediante un flujo de trabajo, el segundo se ocupa de facilitar a los usuarios el acceso al sistema desde dispositivos móviles, estando en concreto implementado para dispositivos Android.

Como líneas futuras de trabajo se proponen:

- Realizar una evaluación del sistema con usuarios finales.
- Desarrollar nuevos servicios que amplíen la funcionalidad ofrecida por el sistema en la actualidad.
- Implementar otros clientes de acceso al sistema, para poner el servicio a disposición de un mayor número de usuarios.
- Gestionar la seguridad de la información intercambiada, empleando mecanismos de autenticación, autorización y codificación [29] [30].

Agradecimientos

Este trabajo ha sido cofinanciado por el Ministerio de Industria, Turismo y Comercio a través del Plan Avanza2, mediante el proyecto AdmiTI2 09 (Tecnologías de la Información 2.0 de código abierto para la ADMinistración en el ámbito educativo - TSI-020100-2009-527), y por el Ministerio de Ciencia e Innovación, a través del Plan Nacional de I+D+I, por medio del proyecto T2C2 (Tecnologías Telemáticas para la Colaboración Ciudadana - TIN2008-06739-C04-01).

Referencias

[1] Grupo Gesfor, "AdmiTI2," admiti2.germinus.com.
[2] Workflow Management Coalition, "Workflow Standard - Terminology and Glossary Technical Report WFMC-TC-1011," Workflow Management Coalition, Tech. Rep., 1996.
[3] H. Xin and F. Xue, "Workflow Interoperability - Enabling Online Approval in E-government," *Grid and Cooperative Computing*, vol. 3033/2004, pp. 1018–1021, 2004.
[4] G. Verginadis and G. Mentzas, "A light modelling framework for e-government service workflows," *Electronic Government*, vol. 1, no. 4, pp. 420–438, 2004.
[5] M. P. Singh and M. N. Huhns, "Multiagent Systems for Workflow," in *International Journal of Intelligent Systems in Accounting, Finance and Management*, 1999, pp. 8–105.
[6] K. Siau and Z. Shen, "Mobile communications and mobile services," *Int. J. Mob. Commun.*, vol. 1, no. 1-2, pp. 3–14, 2003.
[7] ORACLE, "Java ME Technology," java.sun.com/javame/technology.
[8] F. Bellifemine, A. Poggi, and G. Rimassa, "JADE - A FIPA-compliant agent framework," Telecom Italia, Tech. Rep., 1999.
[9] IEEE Foundation for Intelligent Physical Agents, "FIPA," www.fipa.org.
[10] Sandia National Laboratories, "Jess," www.jessrules.com.
[11] OSGi Alliance, "OSGi - The Dynamic Module System for Java," www.osgi.org.
[12] G. Caire and F. Pieri, "JADE LEAP User Guide," Telecom Italia, Tech. Rep., 2003.
[13] G. Caire, D. Gotta, and M. Banzi, "WADE: a software platform to develop mission critical applications exploiting agents and workflows," in *AAMAS '08: Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems*. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2008, pp. 29–36.
[14] Workflow Management Coalition, "XML Process Definition Language," www.wfmc.org/standards/xpdl.htm.
[15] G. Caire, M. Porta, E. Quarantotto, and G. Sacchi, "Wolf - An Eclipse Plug-In for WADE," in *WETICE '08: Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2008.
[16] Google, "Android Developers," developer.android.com/index.html.
[17] ——, "Android Market," www.android.com/market.
[18] B. Salisbuty, "Android Market Going Strong, Now Has 20000 Apps," Maximun PC, 2009.
[19] The hsql Development Group, "HyperSQL," hsqldb.org.
[20] D. Crockford, "RFC 4627. The application/json Media Type for JavaScript Object Notation (JSON)," http://tools.ietf.org/html/rfc4627, 2006.
[21] R. Hipp, "SQLite," sqlite.org.
[22] HTC, "HTC Dream," www.htc.com/www/product/dream.
[23] Capgemini Consulting, "Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas," Fundación Orange, Tech. Rep., 2009.
[24] M. Sonntag, J. R. Mühlbacher, and S. Reisinger, "Personalization of Web-Based Interfaces for Humans and Agents, Applied to E-Government Portals," in *Knowledge Management in E-Government*, 2002.
[25] I. Kushchu and M. H. Kuscu, "From e-government to m-government: Facing the inevitable," in *European Conference on E-Government (ECEG 2003)*, 2003.
[26] A. S. Atkins, A. H. N. P. H. Ali, and H. Shah, "Extending e-business applications using mobile technology," in *Mobility '06: Proceedings of the 3rd international conference on Mobile technology, applications & systems*. New York, NY, USA: ACM, 2006, p. 44.
[27] K. Svetlana and Yonglk-Yoon, "Adaptation e-learning contents in mobile environment," in *ICIS '09: Proceedings of the 2nd International Conference on Interaction Sciences*. New York, NY, USA: ACM, 2009, pp. 474–479.
[28] I. Kushchu, *Mobile Government: An Emerging Direction in E-government*. IGI Publishing, 2007.
[29] JADE Board, "JADE Security Guide," Telecom Italia Lab, Tech. Rep., 2005.
[30] X. Vila, A. Schuster, and A. Riera, "Security for a multi-agent system based on JADE," *Computers & Security*, vol. 26, no. 5, pp. 391 – 400, 2007.

Evitar el Dilema del Prisionero en negociaciones automáticas para espacios de utilidad complejos

Ivan Marsa-Maestre, Miguel A. Lopez-Carmona, Juan R. Velasco y Enrique de la Hoz
Departamento de Automática, Universidad de Alcala
{ivan.marsa,miguelangel.lopez,juanramon.velasco,enrique.delahoz}@uah.es

***Resumen*—Existen múltiples trabajos de investigación que abordan negociaciones complejas en espacios de utilidad altamente rugosos. Sin embargo, la mayoría se centran en superar los problemas impuestos por la complejidad del escenario, sin analizar el comportamiento estratégico de los agentes en los modelos que proponen. Analizar la dinámica de los procesos de negociación cuando coexisten agentes que emplean diferentes estrategias es necesario para aplicar estos modelos a entornos reales y competitivos, donde no puede asumirse que todos los agentes se comportan del mismo modo. Especialmente problemáticas son las situaciones como el conocido dilema del prisionero o, de un modo más general, situaciones con un alto precio de anarquía. Estas situaciones implican que la racionalidad individual lleve a los agentes a soluciones de escaso bienestar individual y social. En escenarios altamente rugosos, este tipo de situaciones suelen hacer que las negociaciones fracasen, por lo que los mecanismos de negociación deben ser diseñados de forma que se eviten en la medida de lo posible. En este artículo se realiza un análisis estratégico de un modelo de negociación basado en subasta diseñado para escenarios de alta rugosidad, y se propone un conjunto de técnicas destinadas a evitar estas situaciones problemáticas. Finalmente, se realiza una evaluación experimental para validar la adecuación de los mecanismos propuestos para mejorar la estabilidad estratégica del proceso de negociación.**

***Palabras Clave*—sistemas multiagente, negociación multiatributo, espacios de utilidad altamente rugosos**

I. Introducción

En los últimos años, existe un creciente interés investigador acerca de las negociaciones complejas que implican múltiples agentes y múltiples atributos interdependientes [5]. Entre estas, aquellos escenarios que implican espacios de utilidad de alta rugosidad suponen un desafío especial, ya que los enfoques tradicionales (en general, orientados a funciones lineales o cuasi-cóncavas) no pueden aplicarse a estos escenarios más complejos.

Podemos encontrar en la literatura algunos trabajos previos que abordan la negociación en espacios de utilidad complejos. En [4], se propone un protocolo basado en subasta para espacios de utilidad no lineales generados por medio de restricciones ponderadas. Este enfoque se basa en tomar muestras aleatorias del espacio de contratos, aplicar temple simulado a esas muestras para identificar regiones de alta utilidad para cada agente, enviar esas regiones como ofertas a un mediador y realizar una búsqueda en el mediador para encontrar solapamientos entre las ofertas de los diferentes agentes. En un escenario similar [8], propusimos como enfoque la toma de muestras del espacio de restricciones. Los experimentos realizados muestran que estos enfoques alcanzan una efectividad elevada en espacios de utilidad moderadamente rugosos, que se manifiesta como unas altas tasas de optimalidad y bajas tasas de fallo para las negociaciones.

En [9], unimos esfuerzos con los autores mencionados anteriormente para abordar de forma conjunta espacios de utilidad de alta rugosidad. Propusimos el uso de un *factor de calidad* para equilibrar la utilidad y la probabilidad de acuerdo en el proceso de negociación. Este factor de calidad se emplea para sesgar la generación de ofertas y la identificación de acuerdos teniendo en cuenta las actitudes de los agentes hacia el riesgo (i.e permitiendo que los agentes den más importancia a la utilidad o a la probabilidad de acuerdo en función de su actitud hacia el riesgo). Los experimentos muestran que este equilibrio entre utilidad y probabilidad de acuerdo mejora significativamente la efectividad de las negociaciones en espacios altamente rugosos.

Sin embargo, el enfoque propuesto plantea diversas cuestiones adicionales. Aunque el factor de calidad permite modelar las actitudes hacia el riesgo de los agentes, los experimentos realizados limitan esas actitudes a un entorno "cooperativo", donde todos los agentes tienen una misma actitud neutral hacia el riesgo. En un entorno real competitivo, es de esperar que coexistan agentes con diferentes actitudes hacia el riesgo. De este hecho surge el problema del comportamiento estratégico de los agentes. ¿Qué pasa cuando mezclamos agentes aversos al riesgo con agentes tendentes al riesgo? ¿Hay una estrategia dominante? Si es así, ¿esta estrategia dominante lleva a los agentes a soluciones satisfactorias, o el enfoque es proclive al dilema del prisionero? Por último, puesto que la complejidad (i.e. rugosidad) del espacio de utilidad puede variar, parece lógico pensar que las estrategias de los agentes deban variar de acuerdo con este factor. En este artículo, abordamos estas cuestiones del siguiente modo:

- Realizamos un análisis estratégico del protocolo basado en subasta para espacios de utilidad basados en restricciones. Este análisis nos ha permitido determinar la estrategia dominante a nivel individual y la estrategia social óptima para diferentes niveles de rugosidad de los espacios de utilidad. Los resultados de los experimentos nos permiten concluir que el protocolo basado en subasta descrito en [9] tiene problemas de estabilidad, siendo proclive al dilema del prisionero (Sección III).
- Proponemos un conjunto de mecanismos destinados a evitar el dilema del prisionero en el protocolo analizado. El enfoque se basa en desacoplar las estrategias de los agentes del mecanismo de identificación de acuerdos, aplicando diferentes técnicas en el mediador una vez que se han recibido las ofertas de los agentes (Sección IV).

Para validar nuestras hipótesis y evaluar los efectos de nuestras contribuciones se ha realizado una evaluación experimental. El escenario experimental se describe en las Secciones III-

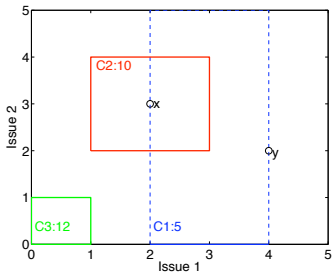


Fig. 1. Ejemplo de espacio de utilidad para un agente, con dos atributos y tres restricciones

B y IV-B, junto con la discusión de los resultados obtenidos. Finalmente, nuestra propuesta se compara brevemente con los trabajos más relacionados del estado del arte (Sección V). La última sección resume nuestras contribuciones y perfila líneas futuras de investigación que surgen del trabajo realizado.

II. Negociación basada en subastas en espacios de utilidad altamente rugosos

El trabajo que proponemos es una contribución al comportamiento estratégico de los agentes en negociaciones basadas en subasta para espacios de utilidad complejos. En esta sección ofrecemos una panorámica de los trabajos previos más relevantes relacionados con nuestra investigación.

A. Espacios de ultilidad no lineales basados en restricciones

Las preferencias no lineales de los agentes pueden describirse empleando diversas representaciones, como funciones K-aditivas, lenguajes de subasta o restricciones ponderadas [9]. En este trabajo nos centramos en espacios de utilidad no lineales generados por medio de restricciones ponderadas. En este caso, las funciones de utilidad de los agentes se describen por medio de un conjunto de restricciones. Cada restricción representa una región de una o más dimensiones, y un valor de utilidad asociado. El número de dimensiones del espacio viene dado por el número de atributos que se negocian n, por lo que el número de dimensiones de una restricción debe ser menor o igual que n. La utilidad que una determinada solución potencial (contrato) proporciona a un agente es la suma de los valores de utilidad de todas las restricciones satisfechas por ese contrato. La Figura 1 muestra un ejemplo muy sencillo para dos atributos y tres restricciones: una restricción unaria $C1$ y dos restricciones binarias $C2$ y $C3$. Los valores de utilidad asociados a las restricciones también se muestran en la figura. En este ejemplo, el contrato x daría un valor de utilidad para el agente $u(x) = 15$, ya que satisface tanto $C1$ como $C2$, mientras que el contrato y daría un valor de utilidad $u(y) = 5$, porque sólo satisface $C1$.

De un modo más formal, podemos definir los *atributos negociados* como un conjunto finito de variables $X = \{x_i | i = 1, ..., n\}$, y un *contrato* o una *solución potencial* al problema de negociación planteado como un vector $s = \{s_i | i = 1, ..., n\}$ definido por los valores de los atributos. Los atributos toman valores del dominio de los enteros $[0, X]$.

El espacio de utilidad de un agente se define como un conjunto de restricciones $C = \{c_k | k = 1, ..., l\}$. Cada restricción viene dada por un conjunto de intervalos que delimitan la región en la que debe estar contenido un contrato para satisfacer la restricción. Formalmente, una restricción c se define como $c = \{I_i^c | i = 1, ..., n\}$, donde $I_i^c = \left[x_i^{min}, x_i^{max}\right]$, con $x_i^{min}, x_i^{max} \in [0, x_D^{max}]$, define el valor mínimo y máximo para cada atributo para satisfacer la restricción. Las restricciones así definidas describen regiones hiperrectangulares en el espacio n-dimensional. Cada restricción c_k tiene asociado un valor de utilidad $u(c_k)$.

Un contrato s *satisface* una restricción c si y sólo si $x_i^s \in I_i^c \forall i$. Por simplicidad de notación, denotaremos esto como $s \in x(c)$, queriendo decir que s está en el conjunto de contratos que satisfacen c. La utilidad para un agente de un contrato s se define como $u(s) = \sum_{c_k \in C | s \in x(c_k)} u(c_k)$, esto es, la suma de los valores de utilidad de todas las restricciones satisfechas por s. El uso de restricciones ponderadas genera un espacio de utilidad no lineal e "irregular", con puntos elevados donde se satisfacen muchas restricciones, y regiones bajas donde se satisfacen pocas o ninguna restricción.

B. Aproximaciones basada en subastas para la negociación en espacios de utilidad altamente rugosos

En [4] se propone un mecanismo de negociación basado en subastas para abordar espacios de utilidad no lineales generados empleando restricciones ponderadas. El protocolo consiste en los siguientes cuatro pasos:

1) *Muestreo*. Cada agente toma un número fijo de muestras aleatorias del espacio de contratos, empleando una distribución uniforme.
2) *Ajuste*. Cada agente aplica temple simulado a cada muestra para intentar encontrar un máximo local a su alrededor. El resultado es un conjunto de contratos de alta utilidad.
3) *Ofertas*. Cada agente genera una oferta por cada contrato ajustado de alta utilidad. Las ofertas se generan como la intersección de todas las restricciones satisfechas por cada contrato. Cada agente envía sus ofertas al mediador, junto con la utilidad asociada a cada una de ellas.
4) *Identificación de Acuerdos*. El mediador emplea búsqueda en anchura con poda para encontrar solapamientos entre las ofertas de los diferentes agentes. Las regiones del espacio de contratos que corresponden con la intersección de al menos una oferta de cada agente se marcan como soluciones potenciales. La solución final es aquella que maximiza la utilidad conjunta, definida como la suma de utilidades para los diferentes agentes.

En [8], propusimos una perspectiva alternativa para el proceso de generación de ofertas, tomando el espacio de utilidad basado en restricciones del agente como un grafo ponderado no dirigido. Consideremos de nuevo el ejemplo de espacio de utilidad de la Figura 1. Pensemos en cada restricción como un nodo del grafo, con un peso asociado que es el valor de utilidad asociado a la restricción. Ahora conectemos todos los nodos cuyas restricciones correspondientes sean *incompatibles*, es decir, que tengan intersección vacía. El grafo resultante se muestra en la Figura 2.

Encontrar la oferta de mayor utilidad en este tipo de grafo puede verse como encontrar el conjunto de nodos no conectados que maximice la suma de sus pesos. Como sólo

los nodos incompatibles están conectados, las restricciones resultantes tendrán intersección no vacía. En el ejemplo, esto se conseguiría tomando el conjunto $\{C1, C2\}$.

El problema de encontrar un conjunto de nodos no conectados con peso máximo es un problema conocido, llamado conjunto independiente de peso máximo (*maximum weight independent set*, MWIS). Aunque la búsqueda de conjuntos MWIS es también un problema NP-completo, en [1] se utiliza un algoritmo de paso de mensajes para obtener una estimación aproximada del conjunto MWIS en un tiempo acotado.

Como el algoritmo es determinista, sólo puede generarse una oferta por cada conjunto de restricciones. Para resolver este problema, en [8] se aplica el algoritmo a un subconjunto de restricciones $C' = \{c'_k | k = 1, ..., n_c; n_c < l; c'_k \in C\}$. Las restricciones c'_k se obtienen de forma aleatoria del conjunto de restricciones C. De este modo, en cada ejecución al algoritmo se le pasa un subconjunto de restricciones C' diferente, lo que da como resultado diferentes ofertas no deterministas.

Ambos enfoques se evalúan en escenarios no lineales para diferente número de agentes y de atributos, y logran buenos resultados en términos de optimalidad (medida como la relación entre la utilidad de las soluciones encontradas por el protocolo y las soluciones encontradas por medio de un optimizador que emplee información completa) y tasa de fallo (medida como la relación entre negociaciones fallidas y el total de negociaciones).

C. *Factor de calidad de restricciones y ofertas para espacios de utilidad altamente rugosos*

El uso de restricciones ponderadas genera espacios de utilidad "irregulares", con muchos picos y valles. Sin embargo, el grado de "irregularidad" puede variar ampliamente de un escenario a otro. De un modo más formal, la complejidad de los espacios de utilidad de los agentes puede medirse por medio de la distancia de correlación, que es una métrica ampliamente utilizada para valorar la complejidad de los espacios de adaptación en computación evolutiva [13]. La distancia de correlación se define como la mínima distancia entre muestras en el espacio de utilidad que hace que la correlación entre dichas muestras caiga por debajo de un determinado umbral.

De forma intuitiva, la principal diferencia entre espacios altamente correlados y espacios altamente incorrelados es la anchura de los picos. Los espacios de utilidad más complejos presentarán picos más estrechos. Como los mecanismos definidos en la sección anterior llevan a los agentes a escoger estos picos (o regiones de alta utilidad) como ofertas, el resultado es que al mediador se le enviarán regiones más estrechas. Asumiendo espacios de utilidad generados de forma uniforme, el ancho de las ofertas (o de un modo más general, el volumen de las ofertas en el espacio n-dimensional) influirá directamente sobre la probabilidad de que una oferta se solape con otra de otro agente, y de ese modo influirá sobre la probabilidad de que la oferta resulte en un acuerdo. En [9], introdujimos la hipótesis de que un agente sin conocimiento acerca de las preferencias del resto debería tratar de equilibrar la utilidad de sus ofertas (para maximizar su propio beneficio) y su volumen (para maximizar la probabilidad de acuerdo). Para permitir esto, definimos el *factor de calidad* de una restricción u oferta como $Q_c = u_c^{\alpha} \cdot v_c^{1-\alpha}$, donde u_c y v_c son, respectivamente, la utilidad y el volumen de la oferta o restricción c, y $\alpha \in [0, 1]$ es un parámetro que modela la actitud hacia el riesgo del agente. Un agente averso al riesgo ($\alpha < 0.5$) tenderá a considerar como mejores ofertas aquellas que sean más anchas, y con ello las ofertas que aumentan la probabilidad de acuerdo. Un agente tendente al riesgo o egoísta ($\alpha > 0.5$), por contra, dará mayor importancia a la utilidad de las ofertas. Finalmente, propusimos un conjunto de mecanismos para integrar este factor de calidad en los pasos de generación de ofertas e identificación de acuerdos descritos en los trabajos previos, y validamos nuestras hipótesis por medio de un conjunto de experimentos que muestran que los enfoques propuestos mejoran el proceso de negociación tanto en efectividad como en rendimiento.

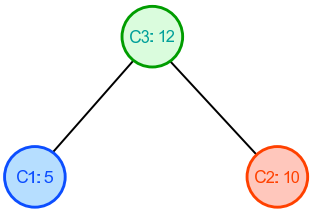


Fig. 2. Grafo ponderado no dirigido correspondiente a la Figura 1

Aunque el enfoque propuesto en [9] proporciona resultados satisfactorios en espacios de utilidad de alta rugosidad, hay algunos aspectos que no se abordan en el trabajo previo. Aun cuando el factor de calidad está diseñado para modelar la actitud hacia el riesgo de los agentes por medio del parámetro α (y con ello α permite modelar estrategias), la evaluación experimental sólo se realiza para $\alpha = 0.5$. Esto implica asumir que todos los agentes que negocian tienen la misma actitud hacia el riesgo, y que esa actitud es neutral (i.e. los agentes ponderan por igual utilidad y probabilidad de acuerdo). En un escenario real competitivo, estas suposiciones no tienen por qué ser ciertas, y por lo tanto es necesario un análisis estratégico para evaluar los mecanismos en situaciones en las que coexisten agentes que emplean diferentes estrategias.

III. Análisis estratégico

El principal desafío en un escenario de negociación automática desde el punto de vista de los mecanismos de decisión es diseñar agentes *racionales,* capaces de escoger una estrategia de negociación adecuada. En negociaciones entre agentes egoístas, los mecanismos de negociación deben diseñarse de manera que sean estables, entendiendo la estabilidad como la imposibilidad (o al menos dificultad) de que el mecanismo sea manipulado desde un punto de vista estratégico. Esto quiere decir que el mecanismo debe motivar a los agentes para actuar de una manera adecuada, ya que si un agente racional egoísta puede beneficiarse de utilizar una determinada estrategia en lugar de la prevista por el mecanismo, es de esperar que lo haga. Este problema está muy relacionado con la noción de *equilibrio* en teoría de juegos. [14], [6]. Para aproximaciones heurísticas tales como

las descritas en [9], no es posible aplicar directamente análisis basados en teoría de juegos, pero alguno de esos conceptos puede ser de utilidad.

Podemos hablar, por ejemplo, de una *estrategia dominante* si existe una estrategia tal que siempre es la mejor elección para un agente independientemente de lo que haga el resto de agentes. En general, la mejor estrategia para un agente dependerá de las estrategias que usen sus oponentes. En estos casos no existen estrategias dominantes, y la estabilidad se consigue por medio de perfiles de estrategias (conjuntos de estrategias para todos los agentes) que hacen que el sistema esté en equilibrio. Se entiende que un perfil de estrategias $F = \{f_1, \ldots, f_N\}$ constituye un equilibrio Nash para un determinado escenario, si cada agente i no dispone de ninguna estrategia que le proporcione una mayor utilidad que la obtenida empleando la estrategia f_i, asumiendo que cada uno de los otros agentes j emplean sus correspondientes estrategias f_j. Esto significa que, si todos los agentes usan las estrategias especificadas para ellos en el conjunto equilibrio, no existe motivación para ninguno de ellos de desviarse a otra estrategia [10]. Por supuesto, dado un determinado mecanismo de negociación, a menudo no es trivial determinar la existencia de alguna de las formas de estabilidad señaladas. Además, en el caso de que existan condiciones de equilibrio, pueden no ser únicas, con lo que existe el problema añadido de determinar cuál de los perfiles de estrategias en equilibrio posibles va a usarse en una negociación concreta. Finalmente, la estabilidad de un mecanismo de negociación no garantiza la obtención de soluciones que maximicen el bienestar social de los agentes. En muchas ocasiones, la racionalidad individual lleva a los agentes a adoptar estrategias que conducen a un bajo bienestar social e individual. Estas estrategias, que deberían ser evitadas en el diseño de los mecanismos, se suelen denominar instancias del *dilema del prisionero*[12] o, de forma más general, situaciones de alto *precio de la anarquía (Price of Anarchy, PoA)* [11].

Tal y como enunciamos anteriormente, los conceptos de equilibrio descritos aquí están relacionados con la teoría de juegos por lo que son muy difíciles de determinar mediante mecanismos de negociación heurísticos. Sin embargo, de forma análoga es posible realizar análisis probabilísticos y evaluaciones empíricas de estos mecanismos. El resto de esta sección está dedicado a evaluar el comportamiento estratégico de la aproximación propuesta en [9], determinando la existencia de estrategias individuales dominantes y estrategias sociales óptimas, y verificando si los mecanismos de negociación basados en ofertas son proclives al dilema del prisionero.

A. Análisis probabilístico

Intuitivamente, puede verse que el factor de calidad definido en [9] permite a un agente equilibrar la utilidad (para maximizar su propio beneficio) y el volumen (para maximizar la probabilidad de un acuerdo) de la oferta. De forma más sistemática, pueden obtenerse expresiones matemáticas para la probabilidad de éxito de la negociación y para la utilidad esperada para un agente en una iteración del protocolo en función de la utilidad y volumen de las ofertas. El desarrollo matemático asociado a la deducción de dichas expresiones queda fuera del alcance de este artículo, y puede encontrarse en [7].Para los propósitos de esta sección, sin embargo, basta citar las expresiones finales. En concreto, la probabilidad de que una iteración del protocolo determine al menos una solución válida al problema de negociación planteado viene dada por la expresión

$$P_{solution} = \sum_{j=1}^{\prod n_{bp}^k} (-1)^{j+1} \binom{\prod n_{bp}^k}{j} \left(\frac{1}{|D|^{n(n^a-1)}} \right)^j, \quad (1)$$

donde n_a es el número de agentes implicados en la negociación, n_i es el número de atributos negociados, $|D|$ es el tamaño del dominio para los atributos (asumiendo que todos los atributos tienen dominios del mismo tamaño), y n_{bp}^k es el *número de puntos ofertados* por el agente k, esto es, una indicación de la porción del espacio de soluciones que cubren las ofertas del agente k, que viene dado por $n_{bp}^k = \sum_{l=1}^{n_b^k} v_l^k$, donde n_b^k es el número de ofertas enviadas por el agente k y v_l^k es el volumen de la oferta l del agente k. Por simplicidad, el cálculo se ha hecho asumiendo ofertas de forma arbitraria (i.e., no necesariamente hiperrectángulos).

De forma similar, podemos ver que la *utilidad esperada* para un agente k viene dada por la expresión

$$E[u^k] = \left[\sum_{l=1}^{n_b^k} u_l^k \cdot v_l^k \right] \left[\sum_{j=1}^{\prod n_{bp}^k} \binom{\prod n_{bp}^k}{j} \left(\frac{(-1)^{j+1}}{\left(|D|^{n(n^a-1)}\right)^j} \right) \right], \quad (2)$$

donde u_l^k es la utilidad asignada a la oferta l del agente k. De esta expresión se deduce que, para maximizar su utilidad esperada, un agente debería revelar el máximo de información posible. En el caso de que la revelación de información esté limitada, un agente debería tratar de maximizar $\sum_{l=1}^{n_b^k} u_l^k \cdot v_l^k$, equilibrando de este modo el volumen de las ofertas y su utilidad. Evidentemente, esta estrategia no modelaría la actitud de un agente no averso al riesgo, que estaría dispuesto a asumir el riesgo de que la negociación fracase para tener la posibilidad de una mayor ganancia. Para modelar esto, podemos emplear una *utilidad de acuerdo esperada*, es decir, la utilidad esperada para el agente en el supuesto de que se encuentre un acuerdo. Esta utilidad de acuerdo esperada viene dada por:

$$E[u^k \,|deal] = \frac{\sum_{l=1}^{n_b^k} u_l^k \cdot v_l^k}{n_{bp}^k} \quad (3)$$

De acuerdo con eso, un agente tendente al riesgo priorizaría la utilidad de la oferta frente al volumen de la misma, tratando de reducir n_{bp}^k para maximizar la utilidad esperada del acuerdo, pero reduciendo la probabilidad de alcanzar el mismo.

Estas expresiones son coherentes con la noción intuitiva de la actitud de un agente frente al riesgo introducida en el factor de calidad en [9]. Podemos emplearlas también para inferir algunas de las propiedades estratégicas del protocolo. Dado que la probabilidad de acuerdo crece con el volumen del mismo, es esperable que valores bajos de α incrementen también la probabilidad de alcanzar un acuerdo. Tal y como hemos visto, la utilidad esperada se maximiza para $\alpha = 0.5$ cuando hay incertidumbre total sobre los espacios de utilidad de los agentes. Si los espacios de utilidad de los agentes son

especialmente complejos (altamente incorrelados), es razonable pensar que la probabilidad de alcanzar un acuerdo será más baja, por lo que los agentes deberían usar valores más bajos de α (esto es, deberían minimizar el riesgo) con objeto de mantener la utilidad esperada en un valor aceptable. Del mismo modo, si los espacios de utilidad de los agentes son altamente correlados, deberían emplear valores más elevados de α (esto es, más orientados a la utilidad), tratando de maximizar la utilidad esperada del acuerdo, dado que la probabilidad de acuerdo será más alta. Además, dado que valores bajos de α incrementan la probabilidad de acuerdo, un agente podría beneficiarse de una estrategia tendente al riesgo si los otros agentes son aversos al riesgo (su valor más bajo de α compensarían el decremento de la probabilidad de acuerdo). Sin embargo, si los agentes decidieran emplear estrategias tendentes al riesgo, la probabilidad de acuerdo se reduciría drásticamente, conduciendo a un bienestar individual y social reducido. Tal y como explicábamos anteriormente, estaríamos en una situación de alto precio de anarquía, análoga al dilema del prisionero.

B. Análisis Experimental

En esta sección se verifican las propiedades estratégicas del protocolo inferidas del análisis estadístico. En primer lugar, se pretende estudiar las condiciones de equilibrio individual para un agente, determinando si existe una *estrategia dominante* que sea la más ventajosa para un agente en cualquier circunstancia, o si existe una estrategia de máxima ventaja diferente en función de las estrategias del resto de agentes, lo que permitiría establecer un equilibrio *bayesiano*.

Lo que intentamos determinar es si existe una estrategia individual, determinada por un cierto valor de α, que otorgue máxima utilidad a un agente en función de las estrategias del resto de agentes. Para ello, hemos realizado experimentos comparando la utilidad obtenida por un *agente individualista,* que emplea una estrategia determinada por α_i, con la utilidad obtenida para el resto de agentes negociadores, que emplean una estrategia determinada por α_s. Los experimentos se han realizado variando los valores de α_i y α_s en el intervalo $[0, 1]$ en pasos de 0.1.

Las Figura 3 presenta los resultados de los experimentos con 6 agentes y 6 atributos. Las figura muestran la relación entre la utilidad obtenida por el agente individualista y la utilidad obtenida por el resto de agentes para diferentes valores de α_i y α_s. En general, el agente individualista obtiene mayor ganancia de utilidad respecto al resto de agentes para valores de α_i elevados. En concreto, para cualquier valor de α_s, el máximo valor de utilidad para el agente individualista si la negociación tiene éxito se obtiene para $\alpha_i = 1$. Por lo tanto, podemos concluir que esa es la *estrategia dominante* desde el punto de vista individual para los agentes negociadores.

Una vez estudiadas las estrategias a nivel individual, se han estudiado las estrategias desde el punto de vista social, tratando de determinar si existe una combinación de estrategias para los diferentes agentes que maximice el bienestar social. Puesto que el modelo de negociación es simétrico y también lo es la medida del bienestar social (el producto Nash), parece razonable que la combinación de estrategias que buscamos sea también simétrica. Teniendo esto en cuenta, hemos realizado experimentos empleando para todos los

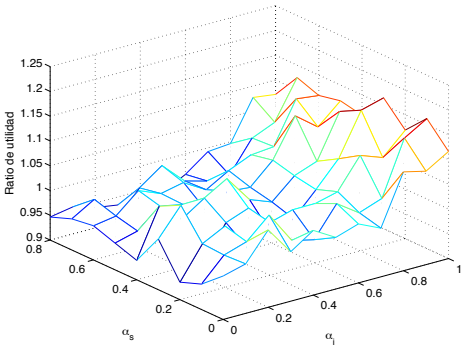


Fig. 3. Análisis de equilibrio individual

agentes una misma *estrategia social*, determinada por α_s. Los experimentos se han realizado variando los valores de α_s en el intervalo $[0, 1]$ en pasos de 0.1. Asimismo, para estudiar la posible variación de los resultados al variar la complejidad de los espacios de utilidad de los agentes, se han repetido los experimentos generando espacios de utilidad con distintos valores de la distancia de correlación ψ. Tal y como se presentó en la sección III-A, se define distancia de correlación como la mínima distancia entre muestras del espacio de utilidad que hace que la correlación entre muestras caiga por debajo de un determinado umbral. Para el propósito de este trabajo, hemos elegido un umbral de 0.7

Los resultados de los experimentos con 6 agentes y 6 atributos se muestran en la Tabla I. En la tabla se han representado las optimalidades medianas obtenidas en las negociaciones para el bienestar social de los agentes en función del valor de α_s, para distintos valores de la distancia de correlación ψ. Se define optimalidad como el cociente entre el bienestar social obtenido con el protocolo y el biestar social obtenido empleando un optimizador con información completa. Podemos observar que los valores de α que maximizan la optimalidad social están alrededor de 0.6 y 0.8. Estos valores son superiores al valor óptimo teórico ($\alpha = 0.5$), lo que es razonable si tenemos en cuenta que los cálculos se realizaron asumiendo una incertidumbre total sobre el espacio de utilidad (esto es, $\psi = 0$).

Una vez identificada una estrategia óptima desde el punto de vista social, una propiedad deseable para esa estrategia es que constituya un *equilibrio Nash*, es decir, que no existe incentivo para ningún agente por desviarse de la estrategia social. Desafortunadamente, como veíamos en la sección anterior, existe una estrategia dominante individual para los agentes dada por $\alpha_i = 1$. Por lo tanto, un agente racional puede decidir tomar esa estrategia, ya que le proporciona un mayor beneficio a nivel individual (como veíamos en la Figura 3). Todos los agentes tienen el mismo incentivo, por lo que el equilibrio se alcanza cuando todos los agentes escogen como estrategia $\alpha_i = 1$. Tal y como podemos ver en la Tabla I, esto hace que a negociación fracase en escenario de complejidad media y alta lo que confirma que el protocolo es propenso al dilema del prisionero.

IV. Evitando el dilema del prisionero en el protocolo de negociación basado en subasta

En esta sección se abordan los problemas de estabilidad del protocolo de negociación basado en subasta. Se proponen

Tabla I
ANÁLISIS DE ESTRATEGIA SOCIAL

		α_s										
		0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$\psi_{0.7}$	2.8	0.3335	0.3788	0.3836	0.3765	0.4336	0.4801	0.5521	0.4855	0	0	0
	3.1	0.4600	0.5282	0.4951	0.5041	0.5544	0.5553	0.5960	0.6822	0	0	0
	4.0	0.7954	0.7849	0.7977	0.8137	0.8211	0.8380	0.8283	0.8270	0.8139	0	0
	4.3	0.9672	0.9634	0.9759	0.9608	0.9728	0.9690	0.9710	0.9707	0.9774	0	0
	4.6	1.0000	1.0000	0.9748	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
	5.9	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

un conjunto de mecanismos orientados a evitar situaciones en el proceso de negociación con alto precio de anarquía, y se evalúa empíricamente su efectividad.

A. Incentivando estrategias sociales en el mediador

Para mejorar la estabilidad estratégica de la negociación, los mecanismos descritos deberían ser modificados para incentivar la adopción de estrategias socialmente óptimas. Para hacer cualquier modificación en el protocolo, el paso lógico es la identificación de acuerdos en el mediador. Dado que se supone que los agentes que negocian son racionales individualmente, el mediador es el único que podemos asumir que perseguirá la obtención del bienestar social. En el protocolo básico propuesto en [9], el mediador selecciona como la solución final la que maximice el bienestar social, calculado como el producto Nash de las utilidades de los agentes individuales. Dado que el producto Nash es simétrico, aquellos agentes cuyas pujas tegan una utilidad media más elevada obtendrían, en media, utilidades más altas en el acuerdo final, lo que incentiva el uso de la estrategia dominante. Para mitigar este efecto, una posibilidad es premiar en la selección de la solución final a aquellos agentes que hayan revelado un mayor volumen de su espacio de utilidad en sus ofertas. Para ello, proponemos emplear una variación del producto Nash que hemos denominado *producto ponderado por volumen medio*:

$$sw_{\bar{V}}(s,U) = \prod_{i=1}^{n_a} \left(u^i(s)\right)^{\frac{\bar{v}^i}{\max_{1\leq j\leq n_a} \bar{v}^j}}, \qquad (4)$$

donde $u^i(s)$ es la utilidad de la solución s para el agente i, y $\bar{v}^i$ es el volumen medio de las ofertas del agente i.

De este modo, la utilidad de los agentes que han hecho ofertas más anchas (y por tanto, más socialmente orientadas) tiene más peso a la hora de medir el bienestar social que la de aquellos agentes que han sido más egoístas. Un efecto interesante de esta métrica es que puede hacer que un agente racional tienda a enviar algunas ofertas de alto volumen (aunque tengan una utilidad muy baja) para aumentar el volumen total de sus ofertas, y de este modo conseguir que la métrica favorezca a sus ofertas de alta utilidad (aunque sean más estrechas). Una posibilidad para evitar este efecto es emplear un *producto ponderado por factor de calidad medio*:

$$sw_{\bar{Q}}(s,U) = \prod_{i=1}^{n_a} \left(u^i(s)\right)^{\frac{\bar{Q}^i}{\max_{1\leq j\leq n_a} \bar{Q}^j}}, \qquad (5)$$

donde $\bar{Q}^i$ es el factor de calidad medio para las ofertas generadas por el agente i.

Finalmente, la selección de oferta para la identificación de acuerdos en el mediador se realiza empleando el factor de calidad de las ofertas *tal como lo haya declarado el agente que realiza las ofertas*. Esto hace que la evaluación de las ofertas hecha por el mediador dependa de las actitudes de los agentes frente al riesgo favoreciendo, por tanto, a aquellos agentes con estrategias más egoístas. Teniendo esto en cuenta, proponemos que el mediador emplee su propio parámetro α_m para el cálculo de Q . De este modo, esperamos desacoplar la identificación de acuerdos de las estrategias de negociación de los agentes, mejorando la estabilidad del protocolo. Una opción posible para α_m es la estrategia social óptima para una distancia de correlación dada, o $\alpha_m = 0.5$, que es el valor teórico óptimo teórico cuando hay una incertidumbre total acerca de los espacios de utilidad de los agentes. Sin embargo, hay un problema relacionado con el uso de esos valores de α_m. Cualquier $\alpha_m \geq 0.5$ daría al menos el mismo peso a la utilidad de la oferta que a su volumen. Debido a esto, no sería posible para el mediador discriminar si una oferta dada tiene un factor de calidad elevado debido a un volumen alto(siendo, por tanto, probablemente una oferta realizada por un agente orientado a maximizar el bienestar social) o debido a su elevada utilidad (por consiguiente, generada por un agente egoísta). Parece razonable emplear $\alpha_m < 0.5$, dando más peso a ofertas de mayor volumen, y por tanto forzando el comportamiento social entre agentes. El límite sería usar $\alpha_m = 0$, que haría que el mediador seleccionara ofertas basándose únicamente en su volumen, independientemente de su utilidad. Nuestra hipótesis es que esto desacoplaría completamente el mecanismo de identificación de acuerdos del comportamiento estratégico de los agentes, lo que reforzaría la estabilidad del protocolo.

B. Análisis de Estabilidad

El análisis de estabilidad pretende determinar la capacidad de un agente para manipular la negociación en su propio beneficio. En el caso del modelo de negociación que nos ocupa, esta manipulación puede darse cuando el agente se desvía de la estrategia social adoptando una estrategia más egoísta. Para evaluar esta capacidad de forma experimental, se han realizado experimentos comparando la utilidad obtenida por un *agente individualista,* que emplea su estrategia dominante $\alpha_i = 1$, con la utilidad obtenida para el resto de agentes negociadores, que emplean la estrategia social óptima α_s en cada caso. Nuevamente, se han repetido los experimentos generando espacios de utilidad con distintos valores de la distancia de correlación ψ. Finalmente, puesto que se trata un modelo de negociación multiagente, se han realizado experimentos para distinto número de agentes individualistas, para analizar los posibles efectos de coalición.

La tabla II refleja los resultados de los experimentos para 6 agentes y 6 atributos, mostrando el cociente entre las utilidades de agentes individualistas y sociales paras distintas distancias de correlación y distinto número de agentes individualistas. La tabla muestra las medianas y los intervalos de confianza al 95% para cien ejecuciones de cada experimento.

Tabla II
ANÁLISIS DE ESTABILIDAD DEL MODELO PARA 6 AGENTES Y 6 ATRIBUTOS

		Número de agentes individualistas					
		1		2		3	
		mediana	int. conf.	mediana	int. conf.	mediana	int. conf.
$\psi_{0.7}$	2.8	–	–	–	–	–	–
	3.1	–	–	–	–	–	
	4.0	2.0086	[1.8574,2.1598]	–	–	–	–
	4.3	1.1066	[1.0610, 1.1522]	1.1986	[1.1431,1.2541]	–	–
	4.6	0.9795	[0.9567, 1.0024]	1.0081	[0.9870, 1.0292]	0.9785	[0.9567,1.0003]
	5.9	1.0336	[1.0081, 1.0591]	1.0243	[1.0043, 1.0443]	0.9811	[0.9598,1.0024]

Podemos ver qué sólo existe una ganancia significativa para los agentes individualistas en los escenarios de complejidad media. En escenarios de complejidad muy alta, la presencia de agentes individualistas provoca que las negociaciones fallen, por lo que no existe ganancia de unos agentes respecto a otros, y con ello no existe incentivo para desviarse de la estrategia social óptima. Al reducir la complejidad de los espacios de utilidad ($\psi_{0.7} = 4$), se observa que un agente egoísta puede obtener un beneficio en torno al 200%, aunque el aumento de número de agentes egoístas hace que las negociaciones fallen, por lo que la existencia de coaliciones es poco probable. Para escenarios de complejidad media-baja ($\psi_{0.7} = 4.3$), sigue existiendo ventaja para los agentes egoístas, y esa ventaja aumenta con el número de agentes egoístas hasta un máximo de tres agentes (coaliciones mayores de tres agentes hacen que las negociaciones fallen). Finalmente, para los escenarios menos complejos ($\psi_{0.7} \geq 5.9$), una actitud egoísta no supone una diferencia significativa en utilidad, ya que todos los agentes obtienen utilidades elevadas empleando la estrategia social óptima. A la vista de estos resultados, podemos concluir que el modelo es estable en escenarios de complejidad baja y en escenarios de complejidad elevada, y que es en escenarios de complejidad media donde presenta problemas de inestabilidad, y donde será necesario aplicar mecanismos adicionales para solucionar estos problemas.

En la sección anterior, se plantearon una serie de métricas alternativas para la selección del acuerdo final en el mediador, destinadas a incentivar en los agentes el comportamiento social, y con ello solucionar en cierta medida los problemas de inestabilidad del modelo. Para verificar la adecuación de las diferentes métricas a este propósito, se ha repetido el experimento anterior para cada una de las métricas discutidas en la Sección IV-A:

1) *Reference.* Métrica de referencia, empleando el producto Nash.
2) *Average_V*.Producto ponderado por volumen medio (Ecuación 4).
3) *Average_*$Q_{0.5}$. Producto ponderado por factor de calidad medio (Ecuación 5), con $\alpha_m = 0.5$, correspondiente a la estrategia óptima social teórica.
4) *Average_*Q_0. Producto ponderado por factor de calidad medio (Ecuación 5), con $\alpha_m = 0$, correspondiente a la estrategia de identificación de un acuerdo totalmente desacoplada de la utilidad del agente (el mediador sólo considera el volumen de la oferta).

La figura 4 muestra los resultados de los experimentos para 6 agentes y 6 atributos para los escenarios más críticos en términos de estabilidad de acuerdo al experimento previo ($\psi_{0.7} = 4$ y $\psi_{0.7} = 4.3$). Cada gráfico muestra un diagrama de cajas para los resultados de cien ejecuciones

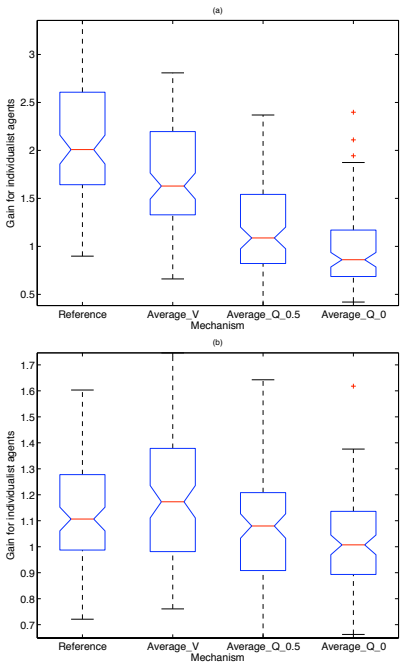


Fig. 4. Efecto de los distintos mecanismos en la estabilidad del protocolo para los escenarios más críticos: a) $\psi_{0.7} = 4$, b) $\psi_{0.7} = 4.3$

del experimento. El eje horizontal representa la aproximación bajo análisis, mientras que en el eje vertical se presenta la tasa de optimalidad mediante diagramas de cajas. Las cajas muestran mediante líneas la mediana y los percentiles 25 y 75 de la ganancia en cada negociación para un agente individualista (calculada como el cociente entre las utilidades obtenidas por agentes individualistas y sociales), y los bigotes muestran valores de datos adyacentes. Los elementos aislados se muestran utilizando el símbolo (+). Las muescas muestran la variabilidad de la mediana entre muestras. Podemos observar que el mecanismo basado en el volumen medio no proporciona una mejora en estabilidad, dado que ambos casos los resultados de la utilidad mediana son más elevados para agentes individualistas. Sin embargo, el mecanismo basado en el factor de calidad medio mejora de forma adecuada la estabilidad del protocolo, siendo esta mejora mayor para r $\alpha_m = 0$. A partir de estos resultados podemos afirmar que el mecanismo de desacoplamiento de la identificación del acuerdo de las actitudes de los agentes que negocian basado en que el mediador calcule su propio factor de calidad mejora la estabilidad del proceso de negociación.

V. DISCUSIÓN Y TRABAJO RELACIONADO

Hay diversas líneas de investigación recientes que abordan el problema de la negociaciones complejas automatizadas. La mayor parte de estas líneas de investigación describen técnicas que tienen como objetivo superar la complejidad de espacios de utilidad intratables computacionalmente, ya sea aproximando estos espacios complejos mediante funciones de utilidad simplificadas [3], o desarrollando mecanismos heurísticos que realizan una búsqueda más eficiente de acuerdos en el espacio de negociación [4]. Sin embargo, muy pocos trabajos abordan el comportamiento estratégico de los agentes en los modelos propuestos. En [9], encontramos la primera referencia en el ámbito de las negociaciones complejas, a la

posibilidad de que los agentes tengan un rango amplio de estrategias, incorporando la noción de actitud hacia el riesgo en el modelo de negociación. Aunque dicho modelo soporta el comportamiento estratégico de los agentes, no se analiza la dinámica de la negociación cuando los agentes interactúan utilizando diferentes estrategias, ni se prueba la estabilidad estratégica del modelo. En este artículo, hemos desarrollado tanto el análisis teórico como la evaluación experimental del modelo. Esta aproximación híbrida está motivada por el hecho de que los mecanismos de decisión de los agentes negociadores y el mediador están basados en heurísticas. Por ello, análisis sistemáticos como los realizados en [2] no son posibles.

El análisis estratégico nos ha permitido la identificación de algunos aspectos críticos relacionados con la estabilidad, como el hecho de que el protocolo basado en subasta tiende a provocar situaciones de alto precio de anarquía, siendo ésta una propiedad indeseable en cualquier sistema de negociación. Para superar este problema, hemos propuesto un conjunto de medidas que tienen como objetivo incentivar el comportamiento social de los agentes negociadores. Los mecanismos propuestos están basados en hacer que la identificación de acuerdos en el mediador dé más preferencia a las ofertas orientadas socialmente. Esta aproximación es de alguna manera similar a la desarrollada en [5] para el caso de negociaciones bilaterales con dependencias binarias de atributos, aunque nuestra propuesta permite que los agentes negociadores retengan el control de su perfil estratégico, en lugar de delegar dicho control sobre un mediador.

VI. Conclusiones y trabajo futuro

El dilema del prisionero, o de manera más general, la situaciones de alto precio de anarquía, que implican que la racionalidad individual conduzca a los agentes hacia estrategias que comportan bajos beneficios sociales e individuales, son condiciones que deben evitarse en los mecanismos de negociación. Esto es especialmente importante cuando se tratan negociaciones complejas que implican espacios de utilidad altamente rugosos, ya que en estos casos "beneficio social e individual bajos" significan a menudo que las negociaciones fallan. Así, es fundamental realizar un análisis estratégico del modelo para poder trabajar con espacios de utilidad altamente rugosos, con el objetivo de determinar las propiedades estratégicas del modelo y permitir el establecimiento de mecanismos de estabilidad en caso necesario.

En este artículo hemos desarrollado un análisis estratégico para el protocolo de negociación basado en subasta sobre espacios de utilidad altamente rugosos propuesto en [9]. Este análisis estratégico ha comenzado estudiando las condiciones de equilibrio, que han revelado la existencia de una estrategia dominante individual, que es diferente de la estrategia sociall óptima. Un análisis de estabilidad en mayor profundidad ha mostrado que, para escenarios altamente correlados o muy poco correlados, no hay incentivo para que los agentes negociadores se desvíen de las estrategias sociales óptimas. Sin embargo, para escenarios de complejidad media, un agente egoísta puede beneficiarse al utilizar su estrategia dominante, lo que genera problemas relacionados con la estabilidad, llevando al modelo a situaciones análogas al conocido dilema del prisionaero. Para solventar el problema, hemos propuesto un conjunto de mecanismos que tienen como objetivo incentivar el comportamiento social de los agentes negociadores. Estos mecanismos están basados en desviar la identificación de acuerdos en el mediador hacia ofertas que estén más orientadas socialmente, desacoplando de esta manera la búsqueda de bienestar social de los objetivos individuales de los agentes. Los resultados muestran que los mecanismos propuestos estabilizan con éxito el protocolo. Sin embargo, queda todavía mucho por explorar en este área. Estamos interesados en la implementación de medidas adaptativas, que permitan al mediador deducir las estrategias de los agentes durante el proceso de negociación, y así aplicar los diferentes mecanismos según sea necesario. Además, el efecto de la correlación entre las funciones de utilidad de diferentes agentes (en contraposición a la distancia de correlación de la función de utilidad de cada agente) debería analizarse en profundidad. Finalmente, estamos trabajando en la generalización de estas aproximaciones a otros protocolos de negociación y tipos de funciones de utilidad.

Agradecimientos

Este trabajo ha sido financiado por el Ministerio de Educación (TIN2008-06739-C04-04).

Referencias

[1] M. Bayati, D. Shah, and M. Sharma. Max-product for maximum weight matching: Convergence, correctness, and lp duality. *IEEE Transactions on Information Theory*, 54(3):1241–1251, 2008.

[2] S. S. Fatima. Bidding strategies for multi-object auctions. *Negotiation, Auctions, and Market Engineering*, pages 200–212, 2008.

[3] K. Hindriks, C. M. Jonker, and D. Tykhonov. Eliminating interdependencies between issues for multi-issue negotiation. In *Cooperative Information Agents X*, volume 4149 of *Lecture Notes in Computer Science*, pages 301–316, 2006.

[4] T. Ito, M. Klein, and H. Hattori. Multi-issue negotiation protocol for agents: Exploring nonlinear utility spaces. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI07)*, pages 1347–1352, 2007.

[5] M. Klein, P. Faratin, H. Sayama, and Y. Bar-Yam. Protocols for negotiating complex contracts. *IEEE Intelligent Systems*, 18(6):32–38, 2003.

[6] S. Kraus. Automated negotiation and decision making in multiagent environments. In *Mutli-agents systems and applications*, pages 150–172. Springer-Verlag New York, Inc., New York, NY, USA, 2001.

[7] I. Marsa-Maestre. *Contribución a la negociación automática en espacios de utilidad complejos*. PhD thesis, Universidad de Alcalá, 2009.

[8] I. Marsa-Maestre, M. A. Lopez-Carmona, J. R. Velasco, and E. de la Hoz. Effective bidding and deal identification for negotiations in highly nonlinear scenarios. In *Proc. of the 8th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2009)*, pages 1057–1064, 2009.

[9] I. Marsa-Maestre, M. A. Lopez-Carmona, J. R. Velasco, T. Ito, K. Fujita, and M. Klein. Balancing utility and deal probability for negotiations in highly nonlinear utility spaces. In *Proc. of the 21st Int. Joint Conf. on Artificial Intelligence (IJCAI-09)*, pages 214–219, 2009.

[10] J. F. Nash. Two-person cooperative games. *Econometrica*, 21(1):128–140, 1953.

[11] C. Papadimitriou. Algorithms, games, and the internet. In *STOC '01: Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 749–753, New York, NY, USA, 2001. ACM.

[12] W. Poundstone. *Prisoner's Dilemma*. Anchor, New York, USA, 1993.

[13] E. Weinberger. Correlated and uncorrelated fitness landscapes and how to tell the difference. *Biological Cybernetics*, 63(5):325–336, 1990.

[14] G. Weiss. *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*. MIT Press, 1999.

Protocolo Anónimo y Equitativo de Acceso a Servicios de Pago Basados en Localización

Andreu Pere Isern-Deyà, M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Josep Lluís Ferrer-Gomila
Departament de Matemàtiques i Informàtica, Universitat de les Illes Balears
Cra. de Valldemossa, km 7.5. Palma (Illes Balears)
{andreupere.isern, mpayeras, macia.mut, jlferrer@uib.es}

***Resumen*—Hasta el momento, las propuestas de acceso a servicios basados en localización no habían unido el acceso anónimo de los usuarios con la capacidad de los proveedores de cobrar por sus servicios. Este trabajo pretende dar una solución a esta problemática, proponiendo un nuevo protocolo de acceso anónimo, eficiente y seguro a servicios de pago basados en localización. El protocolo aquí presentado implementa un esquema de micropago anónimo además de incorporar un intercambio equitativo de un micropago a cambio de un servicio o respuesta de localización.**

***Palabras Clave*—privacidad, anonimato, servicios basados en localización, LBS, equidad, micropagos, cadena de hash**

I. Introducción

Actualmente se está observando un gran incremento del uso de dispositivos móviles y una tendencia clara a que éstos sean terminales principalmente diseñados para conexiones a redes de datos, dejando de ser terminales únicamente conectados a redes de voz. Muchos de estos dispositivos, además, incorporan sistemas de localización espacial como el GPS u otras técnicas de localización basadas en GSM o WiFi. La combinación de ambas tecnologías en movilidad implica la aparición de nuevas aplicaciones y servicios basados en la localización de los usuarios, con las que se podrá acceder a servicios que proporcionarán información específica con valor añadido para el contexto en el que el usuario está situado. Como ejemplos claros de servicios de localización se pueden encontrar redes sociales generalistas como Twitter [1], redes sociales móviles como Foursquare [2] o aplicaciones que hacen uso de Google Maps [3].

Estas nuevas aplicaciones y servicios usan datos que pueden ser considerados de carácter privado, y que por tanto deben ser protegidos debidamente, como son la identidad de los usuarios y la localización de los mismos. Por tanto, las dos propiedades buscadas para el acceso a estos servicios son el anonimato y la privacidad de los datos. Existen numerosas propuestas de protocolos en la bibliografía para el acceso a servicios basados en localización. Algunas se basan en esconder la localización exacta del usuario mediante diversos algoritmos de ofuscación [4] [5], mientras que otras realizan peticiones de forma privada mediante una técnica llamada PIR [6] . No obstante, ninguna combina de forma eficiente el acceso anónimo a los servicios de localización y el pago por los mismos. En este artículo se presenta por primera vez un nuevo protocolo eficiente y anónimo de acceso a servicios de pago de localización basado en un sistema de micropago. Además, incorpora un esquema de intercambio equitativo de un micropago por un servicio (las respuestas de localización). Es decir, con el uso de este protocolo, el usuario puede acceder a servicios de localización sin tener que identificarse con su identidad real y al mismo tiempo los proveedores pueden cobrar por sus servicios.

El artículo se organiza como sigue: las secciones II y III hacen un repaso de las características de los sistemas de micropago y de los servicios basados en localización; en la sección IV se explica la herramienta criptográfica usada para la definición del protocolo; el capítulo V define el protocolo propuesto; en la sección VI se analizan de forma informal las propiedades del protocolo; y finalmente la sección VII expone las conclusiones y el trabajo futuro.

II. Sistemas de Micropago

Los sistemas de micropago son un tipo de sistema de pago electrónico diseñado especialmente para el pago de pequeñas cantidades de dinero. Estos sistemas se diseñan para maximizar su eficiencia y por tanto reducir al máximo los costes de almacenamiento y proceso relacionados. Este tipo de pagos, al ser de pequeñas cantidades, permiten relajar las medidas de seguridad, ya que los riesgos financieros están más controlados que en sistemas de pago de grandes cantidades.

II-A. Características de los Sistemas de Micropago

Las características principales de un sistema de micropago ideal son las siguientes [7], [8]:

- *Seguridad*. La seguridad incrementa la confianza de los usuarios. Debe asegurarse principalmente la privacidad, la integridad y la autenticación de los participantes cuando sea necesaria.
- *Anonimato*. Deben preservar el anonimato de sus usuarios.
- *Costes reducidos*. Los costes para cada micropago deben ser lo suficientemente pequeños respecto al valor pagado para que el sistema no provoque pérdidas económicas. Un sistema de micropago debe llegar a un compromiso entre los costes asociados y la seguridad del mismo. Los costes dependen principalmente de:
  - *El almacenamiento*. La cantidad de información a guardar.
  - *La comunicación*. El volumen de datos intercambiados entre los participantes.
  - *El procesamiento de datos*. El coste de procesado está relacionado con las medidas de seguridad y la cantidad de datos a almacenar.
  - *Las medidas de seguridad*. Su seguridad puede relajarse ligeramente al tratarse de sistemas de pago de pequeñas cantidades de dinero, pero los riegos deben estar controlados.

  - *El uso de dispositivos resistentes a manipulación*. El uso de dispositivos especializados aumenta el coste.
  - *La tipo de moneda: específica o genérica*. El uso de la moneda será diferente si ésta es específica para un comerciante o genérica para cualquiera.
- *Intercambio atómico*. En la compra de productos, es deseable que el pago se realice de forma atómica [9] con la transferencia del bien, es decir, que sea equitativo.
- *Control de los riegos financieros*. Las medidas de seguridad se relajan para mejorar la eficiencia y minimizar costes, pero los riesgos financieros deben ser controlados.
- *Escalabilidad*. A medida que el comercio electrónico basado en micropagos aumente, los servicios y aplicaciones deben escalar para no generar cuellos de botella.
- *Fiabilidad*. El servicio de micropago debe tener una alta fiabilidad y disponibilidad.
- *Latencia*. El tiempo de respuesta del servicio debe minimizarse aún cuando se esté en períodos de pico de actividad.

III. Servicios Basados en Localización

La proliferación de las redes móviles y de las tecnologías de posicionamiento espacial como GPS, GSM o WiFi, que hoy en día ya muchos dispositivos móviles llevan incorporadas, fomenta la creación de nuevas aplicaciones que hacen uso de estos datos de posicionamiento para proporcionar a los usuarios información específica para el contexto en el que están posicionados en un determinado momento. Estas aplicaciones o servicios se llaman Servicios Basados en Localización o LBS en sus siglas en inglés (Location-Based Services). Existen multitud de ejemplos de servicios basados en localización, como por ejemplo la localización del hospital o el cine más cercano. Es notorio que el uso de la información de localización puede beneficiar a los usuarios desde el punto de vista de la utilidad de recibir servicios específicos dependiendo de su localización, así como a las empresas y compañías de telecomunicaciones que ven en estas aplicaciones nuevas oportunidades de negocio para explotar. No obstante, la localización puntual o contínua del usuario abre nuevos riesgos acerca de la seguridad de estos servicios y por consiguiente, de la privacidad de los usuarios que hacen uso de los mismos.

La localización del usuario debe ser tratada como un dato de carácter privado, y por tanto, debe ser protegida del uso no autorizado por terceras partes o adversarios, ya que en determinadas situaciones podría revelar la identidad del usuario a entidades no deseadas. Este hecho puede ocurrir con la recopilación de series de datos de localización de un usuario móvil, es decir, mediante la creación de un histórico de posiciones del usuario, vinculándolas entre sí, para obtener un perfil del usuario. No obstante, el nivel de privacidad de un servicio depende del servicio en sí mismo, es decir, de las funcionalidades que proporciona a sus usuarios, así como del propio usuario, el cual tiene la potestad de publicar sus datos si así lo autoriza.

III-A. Clasificación de Servicios Basados en Localización

Los servicios basados en localización pueden clasificarse en tres tipos dependiendo de los requerimientos de anonimato del usuario [10]:

- *Anónimo*. En este tipo de LBS, el usuario puede manejarse completamente anónimo, ya que no es necesario ningún tipo de identificación ni de pseudónimo. Por ejemplo, un servicio de alertas meteorológicas para la ciudad donde está localizado el usuario o un servicio de aviso de congestión en una calle por donde el usuario debería pasar.
- *Identificado*. Un LBS de tipo identificado solo puede trabajar si el usuario proporciona su verdadera identidad. Por ejemplo, informar de la llegada de un representante de una empresa al lugar asignado o la aplicación mediante la cual se alerta del quebrantamiento de una orden de alejamiento de un agresor.
- *Basado en pseudónimos*. Un LBS basado en pseudónimos está situado en un punto intermedio entre los dos anteriores. En este tipo de servicios el usuario no requiere emitir su identidad real, sino que es suficiente publicar un pseudónimo. Por ejemplo, en una aplicación para encontrar pareja puede no ser necesario publicar la identidad real aunque se publiquen otros datos personales, como edad o sexo.

IV. Herramienta Criptográfica: Cadena de Hash

La cadena de hash fue inicialmente propuesta [11] para la autenticación de *one-time passwords*, planteamiento que posteriormente fué redefinido como el estándar S/KEY [12]. Payword [13] fué el primer protocolo en aplicar la cadena de hash en un esquema de micropagos, en el que cada valor de la cadena se usa como un cupón para el pago de pequeñas cantidades de dinero. Otros usos de las cadenas de hash son por ejemplo en las cadenas de certificados digitales [14], en la construcción de *one-time signatures* [15] o para autenticar actualizaciones del estado del enlace [16].

Una cadena de hash $(W_N ... W_0)$ se define como una colección de valores tales que cada W_i (excepto el valor W_N) es el resultado de aplicar una función de una sola vía, típicamente una función de hash criptográfica, sobre el valor $W_{(i+1)}$, esto es, $W_i = H(W_{i+1})$ para $0 \leq i \leq N-1$. Para inicializar la cadena de hash, el generador elige aleatoriamente y guarda en secreto la semilla de la cadena (W_N) y deriva los sucesivos valores W_i aplicando iterativamente la función de hash H tal como se ha descrito arriba. El valor W_0, llamado valor final de la cadena, típicamente se revela y es vinculado a la identidad del usuario generador que posee el valor semilla.

En la verificación de una cadena de hash, el verificador debe conocer el valor final de la misma, W_0. Para verificar un valor W_i, debe aplicarle iterativamente la función de hash H i veces y comparar el resultado con el valor final de la cadena, es decir, verificar si $H^i(W_i) \stackrel{?}{=} W_0$. Si el valor obtenido es igual al valor final de la cadena, entonces se puede afirmar que el valor es auténtico. Para aumentar la eficiencia del algoritmo, si se conoce un valor W_k, para $k < i$, entonces es suficiente aplicar iterativamente H $(i-k)$ veces sobre el valor de entrada, y comparar el resultado con este valor intermedio W_k.

La principal propiedad, y a su vez ventaja, es que dado un identificador W_i, es imposible encontrar un valor W_j donde $j > i$, tal que $H^{j-i}(W_j) = W_i$. Por otra parte, verificar la

validez de un valor W_j donde $j > i$, se reduce a verificar que $H^{j-i}(W_j) = W_i$. Por su parte, la principal desventaja de la cadena de hash es que el verificador debe ejecutar $j - i$ operaciones para validar W_j dado W_i, proceso que puede resultar costoso si $j - i$ es un valor grande.

V. Descripción del Protocolo de Acceso a LBS

La propuesta de protocolo aquí presentada es la primera que incorpora satisfactoriamente un sistema de micropago anónimo y eficiente [17] y un intercambio equitativo a cambio de la obtención de un servicio de localización sujeto a pago. Las principales características y propiedades de los sistemas de micropago (Apartado II-A) y algunas características específicas del sistema de micropago descrito en [17] son ideales para construir un protocolo de acceso a servicios basados en localización. Este tipo de servicios, basados en ciclos cortos de petición/respuesta, deben maximizar la eficiencia y la sencillez dado que mayoritariamente son usados por terminales móviles con recursos limitados. Pero al mismo tiempo deben garantizar una serie de requerimientos de seguridad, como el anonimato del usuario y la privacidad de las comunicaciones y de los datos de localización.

El protocolo usa moneda específica para un único proveedor para mejorar la eficiencia del esquema y esta moneda no contiene ningún tipo de información de la identidad del usuario. Además, la moneda está construida como una cadena de cupones que serán usados para pagar las peticiones que se envían al servicio de localización. El protoclo también implementa un algoritmo de detección de doble gasto que puede evitar el riesgo que la moneda sea reusada. Por otra parte, el esquema propuesto añade por primera vez un intercambio equitativo entre un micropago y un servicio. Este intercambio debe cumplir la propiedad de atomicidad [9], es decir, el intercambio debe relacionar varias operaciones que tienen que ser ejecutadas por completo o no ejecutadas.

Los participantes y la notación usada en la descripción del protocolo presentado puede consultarse en el Cuadro I. El protocolo se divide en una serie de subprotocolos que serán descritos en los siguientes apartados: *listado de servicios*, *emisión de cupones*, *uso*, *depósito* y *reintegro*.

Listado de participantes	
U	Usuario del servicio
P	Proveedor del servicio LBS
B	Banco
Notación usada	
$H(x)$	Función de hash de una sola vía resistente a colisión aplicada sobre el elemento x
$H^i(x)$	Aplicación de la función de hash H i veces sobre el elemento x
sk_A y pk_A	Par de claves secreta y pública de un criptosistema de clave pública del actor A
$Cert_A$	Certificado de clave pública del actor A
$Sign_A(x)$	Firma digital del actor A sobre el elemento x
$Sign_{B.Q}(x)$	Firma digital de B para la cantidad Q sobre el elemento x
$Y^* = (Y, Sign_A(Y))$	Elemento Y y firma sobre Y generada por A
$x \overset{R}{\leftarrow} Z_q$	Extracción aleatoria de un elemento x del conjunto Z_q
$E_K[x]$	Cifrado de x usando la clave simétrica K
$D_K[x]$	Descifrado de x usando la clave simétrica K

Cuadro I
Actores y notación usada en la descripción del protocolo

V-A. Consideraciones Iniciales

Antes de describir en profundidad los diferentes subprotocolos, se listan una serie de condicionantes iniciales que marcan el desarrollo de los mismos:

- El protocolo es diseñado para ser usado principalmente en dispositivos móviles con recursos limitados, hecho que implica que debe diseñarse para maximizar la eficiencia.
- El sistema funciona mediante la modalidad de débito, es decir, la cuenta del usuario U sufre un decremento de su saldo en el *subprotocolo de emisión de cupones.*
- B es una entidad de confianza que no revelará información sobre ningún participante en el protocolo.
- P proporciona sus servicios en paquetes, es decir, permite el acceso a su sistema para un número determinado de veces, aunque no es obligatorio el consumo de todo el paquete.
- Los cupones serán de valor suficientemente pequeño para no tener que ser divididos en varias porciones.
- La respuesta a la petición de localización será generada con la mínima latencia para que el usuario la reciba en un tiempo razonable.

El protocolo define una serie de fechas e intervalos de tiempo en el sistema (Fig. 1). Los períodos de tiempo T_1 y T_2 son parámetros fijados por el sistema.

- T_{Cad} es la fecha de caducidad, incorporada dentro de la moneda, que marca la fecha hasta que U puede usar la moneda para acceder a P.
- T_d, definida como $T_{Cad} + T_1$, marca el instante hasta el cual P puede depositar los cupones recibidos y el inicio del período en el que U puede pedir el reintegro de los cupones no usados.
- T_r, es calculada como $T_d + T_2$ y marca el instante hasta el cual U puede devolver los cupones restantes, reintegrando el valor sobrante en su cuenta bancaria. A partir de T_r, la moneda deja de ser válida, y puede ser borrada de los sistemas de B.

El esquema propuesto usa ElGamal [18] para realizar el intercambio de claves, pero cualquier otro algoritmo similar puede usarse. El sistema tiene unos parámetros públicos (g, q, h), donde g es el generador del grupo cíclico G de orden q, siendo q tal que cumpla que $q - 1$ tiene como mínimo un factor primo grande. h se calcula como g^x donde x es un elemento elegido aleatoriamente dentro de Z_q

V-B. Apertura de una Cuenta Bancaria

U y P deben abrir una cuenta bancaria en B. En este paso previo, el banco B asociará un certificado de clave pública a un número de cuenta bancaria. B utilizará estos certificados para autenticar a sus clientes en los *subprotocolos de retirada*, *depósito* y *reintegro*.

V-C. Subprotocolo de Listado de Servicios

El *subprotocolo de listado de servicios* (Cuadro II) permite a U obtener una lista de servicios disponibles en P. P de-

requestCapabilities. U sigue los siguientes pasos:	
U $\rightarrow$ **P**	Petición
responseCapabilities. P sigue los siguientes pasos:	
	Construye la lista de servicios disponibles: $list(c, n, d)$ Elige $W_{1p} \overset{R}{\leftarrow} Z_q$ y lo guarda en secreto Construye $W_{0p} = H(W_{1p})$ Firma $Sign_P(W_{0p})$ Elige $x \overset{R}{\leftarrow} Z_q$ y lo guarda en secreto Calcula el elemento $h = g^x$ para el algoritmo ElGamal
P $\rightarrow$ **U**	$W_{0p}, Sign_P(W_{0p}), list(c, n, d)$, $Cert_P, h, q, g$
chooseService. U sigue los siguientes pasos:	
	Guarda $W_{0p}, Sign_P(W_{0p})$ Elige el servicio y calcula su coste: $Q = n_s \cdot c_s$

Cuadro II
SUBPROTOCOLO DE LISTADO DE SERVICIOS

makeCoupons. U sigue los siguientes pasos:	
	Elige $W_{Mu} \overset{R}{\leftarrow} Z_q$ Construye la cadena de cupones: $W_{iu} = H(W_{(i+1)u})$ donde $0 \leq i \leq M-1$ y $M = 2n$ Construye la firma sobre el último cupón y Q: $Sign_U(W_{0u}, Q)$
U $\rightarrow$ **B**	$W_{0p}, Q, 2n, W_{0u}$, $Sign_u(W_{0u}, Q), Cert_U$
issueCoupons. B sigue los siguientes pasos:	
	Verifica si $Sign_U(W_{0u}, Q)$ es válido Cuenta de U debe cumplir que $balance \geq Q$, sino denegar Genera la moneda $C = (W_{0p}, W_{0u}, 2n, T_{Cad})$ Firma la moneda $Sign_{B.Q}(C) = sk_{B.Q}[H(C)]$ Construye $C^* = \left(C, Sign_{B.Q}(C)\right)$
B $\rightarrow$ **U**	C^*
storeCoupons. U sigue los siguientes pasos:	
	Verifica si C^* es correcto Guarda C^*

Cuadro III
SUBPROTOCOLO DE EMISIÓN DE CUPONES

berá contestar a la petición con una lista indexada de servicios, donde cada ítem es descrito como:

- El coste de cada petición (c);
- El número de peticiones permitidas para cada paquete (n);
- Una breve descripción textual (d) sobre el servicio.

Al mismo tiempo, P genera un identificador W_{0p} a partir de la aplicación de una función de hash sobre un elemento obtenido aleatoriamente, W_{1p}, el cual deberá ser guardado de forma secreta por P. P también calcula los elementos necesarios para el intercambio de la clave simétrica de sesión mediante ElGamal [18]. Luego, P envía a U el identificador W_{0p}, la firma sobre el mismo, listado de servicios y el certificado digital de P.

Finalmente, U guarda los elementos recibidos, elige el servicio y calcula el coste total (Q).

V-D. Subprotocolo de Emisión de Cupones

En el *subprotocolo de emisión de cupones* (Cuadro III) participan U y B, permitiendo a U extraer una cierta cantidad

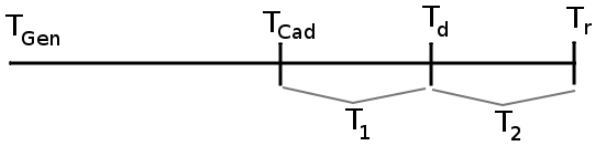


Figura 1. Tiempos

monetaria de su cuenta en B en forma de cupones específicos que se usarán posteriormente para el acceso a los servicios de P.

U genera una cadena de hash o cadena de cupones a partir de un elemento inicial obtenido de forma aleatoria (W_{Mu}), aplicando $M = 2n$ veces una función de hash, donde n se corresponde con el número de peticiones ofrecidas por el paquete elegido. Con este proceso, U obtiene $2n+1$ elementos encadenados, que cumplen las propiedades de las cadenas de hash. La novedad que aporta este subprotocolo reside en la forma en que estos elementos son utilizados (Cuadro IV). El último valor de la cadena de hash se reserva para la construcción de la moneda, mientras que los cupones restantes están disponibles para ser utilizados en el *subprotocolo de uso*. La mitad de los cupones los llamamos *cupones de pago* (tienen un valor monetario y se corresponden con los índices impares), mientras que la otra mitad son *cupones de prueba* (cupones con índice par que demuestran la validez del cupón de pago). El planteamiento es que para cada ciclo de petición/respuesta, U envía los cupones por parejas, de forma que la obtención del *cupón de pago* no es suficiente para que P realize su depósito en B, ya que es necesario el conocimiento del *cupón de prueba* correspondiente.

Siguiendo con el flujo del subprotocolo, U debe identificarse a B para empezar el proceso de emisión de cupones. Para hacerlo, U firma el último identificador de la cadena (W_{0u}) juntamente con la cantidad solicitada, esto es $Sign_U(W_{0u}, Q)$. Este elemento indica a B que U quiere extraer la cantidad Q de su cuenta y que quiere generar una moneda de cupones identificada por W_{0u}. Luego U envía a B este elemento juntamente con el número de cupones ($2n$) y el identificador de P (W_{0p}).

Cuando la petición es recibida, B debe comprobar la validez de la firma de U. Si es válida y el saldo de la cuenta de U es suficiente, B genera la moneda de $2n$ cupones. De otra forma, B envía un mensaje de error a U. Seguidamente, B firma con su clave privada para la cantidad Q el conjunto formado por el identificador de P (W_{0p}), el último identificador de la cadena de cupones de U (W_{0u}), el número de cupones de la moneda ($2n$) y la fecha de caducidad de la moneda (T_{Cad}). Finalmente, B envía C^* compuesto por la moneda y su firma a U.

V-E. Subprotocolo de Uso

El *subprotocolo de uso* (Cuadro V) es un protocolo *offline*, ya que solo participan U y P, sin intervención de B. Este subprotocolo define un intercambio equitativo entre un micropago y un servicio, que en este caso se trata de la respuesta de localización. U puede ejecutar este subprotocolo a lo largo de la validez de la moneda, es decir, cuando $t_{current} < T_{Cad}$.

En el primer paso, U elige un K_S aleatorio, que servirá como clave simétrica de sesión, que intercambiará con P mediante al algoritmo de ElGamal [18]. No es necesa-

Elemento	$2n+1$ cupones										
	$2n$ cupones para usar en el subprotocolo de uso										Último identificador
Cadena de hash	W_{Mu}	$W_{(M-1)u}$	$W_{(M-2)u}$	...	$W_{(i+1)u}$	W_{iu}	...	W_{3u}	W_{2u}	W_{1u}	W_{0u}
Cupones de pago		$W_{(M-1)u}$		...		W_{iu}	...	W_{3u}		W_{1u}	
Cupones de prueba	W_{Mu}		$W_{(M-2)u}$	...	$W_{(i+1)u}$		...		W_{2u}		

Cuadro IV
CONSTRUCCIÓN DE LA CADENA DE CUPONES

	makeRequest. U sigue los siguientes pasos:
	Elige $K_S \overset{R}{\leftarrow} Z_q$
	Elige $y \overset{R}{\leftarrow} Z_q$
	Construye $Z_1 = g^y$
	Construye $Z_2 = K_S \cdot h^y$
	Construye la petición $request(lat, long) = [(lat, long), question]$
	Cifra la petición $req = E_{K_S}[request(lat, long)]$
	Cifra el cupón de pago $cpay = E_{K_S}[W_{iu}]$
U $\rightarrow$ **P**	$Z_1, Z_2, req, cpay, C^*$
	verifyRequest. P sigue los siguientes pasos:
	Recupera la clave de sesión: $K_S = Z_2 \cdot Z_1^{-x} = K_S \cdot g^{xy} \cdot g^{-xy}$
	Descifra el cupón recibido: $W_{iu} = D_{K_S}[cpay]$
	Verifica que $t_{current} < T_{Cad}$
	Verifica la firma de C^*
	Verifica múltiples usos:
	IF $(i \leq j) \rightarrow$ reuso: P envía mensaje de denegación ELSE continuar
	Verifica el cupón recibido $H^{(i-j)}(W_{iu}) \overset{?}{=} W_{ju}$
	Guarda en la BBDD (i, W_{iu}, C^*)
	Descifra la petición recibida req: $request(lat, long) = D_{K_S}[req]$
	Procesa la petición y busca en la BBDD de localización para generar $answer$
	Construye la respuesta $response(lat, long) = [H(request(lat, long)), answer]$
	Cifra la respuesta $res = E_{K_S}[response(lat, long)]$
P $\rightarrow$ **U**	res
	sendProof. U sigue los siguientes pasos:
	Descifra $response(lat, long) = D_{K_S}[res]$
	Extrae el cupón de prueba: $W_{(i+1)u}$
	Cifra el cupón de prueba $cproof = E_{K_S}\left[W_{(i+1)u}\right]$
U $\rightarrow$ **P**	$cproof$
	verifyProof. P sigue los siguientes pasos:
	Descifra $W_{(i+1)u} = D_{K_S}[cproof]$
	Verifica $H\left(W_{(i+1)u}\right) \overset{?}{=} W_{iu}$
	Guarda $\left(i+1, W_{(i+1)u}, C^*\right)$

Cuadro V
SUBPROTOCOLO DE USO

rio que la clave de sesión sea renovada para cada ciclo de petición/respuesta, siendo suficiente cambiarla para cada nueva cadena de cupones o tras un período determinado de tiempo de validez de la misma. Con esta clave simétrica, la comunicación entre U y P será privada. U cifra con K_S la petición de localización y un *cupón de pago* aún sin usar, y lo envía a P.

Al recibir la petición, P recupera la clave de sesión K_S y descifra el cupón. Ahora, P debe verificar que la moneda es válida, que no esté caducada y que la firma de C^* sea válida. Entonces P verifica si el cupón había sido usado en peticiones previas. Para hacerlo, P compara el índice del cupón recibido (i) con el índice del cupón anterior (j) guardado en su base de datos. Si $i \leq j$ P detecta un intento de reuso de un cupón ya gastado, y por tanto P envía un mensaje de denegación a U. P denegará el servicio a U hasta que U envía un *cupón de pago* no usado o un cupón con un índice superior. Si no, P verifica si el *cupón de pago* recibido pertenece a la cadena C^*. Para eso, P aplica $(i-j)$ veces la función de hash sobre W_{iu} y verifica que el resultado sea igual al cupón guardado préviamente (W_{ju}). Notar que si la petición es la primera recibida por la moneda C^*, P no tiene ningún cupón guardado, por lo que la comparación se realizará con el valor final W_{0u}, por tanto $j = 0$. Luego P guarda en su base de datos el cupón

requestDeposit. P sigue los siguientes pasos:	
	Genera la petición $r = (C^*, W_{1p}, W_{ku}, k)$ Cifra la petición: $pk_B(r)$
P $\rightarrow$ **B**	$pk_B(r), Cert_P$
doDeposit. B sigue los siguientes pasos:	
	Verifica que $T_{Cad} < t_{current} < T_d$ Verifica la firma de C^* Verifica la prueba secreta de P: $W_{0p} \stackrel{?}{=} H(W_{1p})$ Comprueba múltiples usos: IF $(k \leq j) \rightarrow$ reuso: P envía mensaje de denegación ELSE continuar Verifica el cupón $H^{(k-j)}(W_{ku}) \stackrel{?}{=} W_{ju}$ Deposita en la cuenta de P el valor de los cupones dependiendo de si $(k-j)$ es: par P deposita $\frac{k-j}{2}$ cupones impar P deposita $\frac{k-j-1}{2}$ cupones

Cuadro VI
SUBPROTOCOLO DE DEPÓSITO

requestRefund. U sigue los siguientes pasos:	
	Genera la petición $r = (C^*, W_{iu}, i)$ Cifra la petición: $pk_B(r)$
U $\rightarrow$ **B**	$pk_B(r), Cert_U$
doRefund. B sigue los siguientes pasos:	
	Verifica que $T_d < t_{current} < T_r$ Verifica la firma de C^* Comprueba múltiples usos: IF $(i \leq j) \rightarrow$ reuso: P envía mensaje de denegación ELSE continuar Verifica cupón $H^{(i-j)}(W_{iu}) \stackrel{?}{=} W_{ju}$ Reintegra en la cuenta de U el valor de los cupones dependiendo de si $(i-j)$ es: par P reintegra $\frac{i-j}{2}$ cupones impar P reintegra $\frac{i-j-1}{2}$ cupones

Cuadro VII
SUBPROTOCOLO DE REINTEGRO

recibido, el índice y la moneda C^*. Posteriormente, P descrifa y reponde a la petición de localización buscando en su base de datos de localización. Finalmente, P construye la respuesta, la cifra y la envía a U.

En el tercer paso, U descrifa la respuesta recibida y envía el *cupón de prueba* $W_{(i+1)u}$ cifrado con la clave compartida con P. Entonces, P verifica el *cupón de prueba* y si es correcto, P guarda en la base de datos esta prueba y el índice actual $i+1$. Si no, P denegará el servicio a U.

V-F. Subprotocolo de Depósito

El *subprotocolo de depósito* (Cuadro VI) permite a P intercambiar los cupones recibidos por un ingreso en su cuenta bancaria en B. P puede proceder a la ejecución de este subprotocolo en cualquier momento, aunque no haya recibido todos los cupones de la cadena y siempre y cuando se cumpla que $T_{Cad} < t_{current} < T_d$. Para depositar, P debe mostrar la prueba secreta W_{1p} que prueba que P es el destinatario de la moneda. P también muestra el último *cupón de prueba* recibido (W_{ku}), el índice correspondiente (k) y la moneda (C^*). Estos cuatro elementos se envían a B cifrados con su clave pública, pk_B juntamente con un elemento que identifique a P o a su cuenta bancaria.

Una vez recibida la petición, B procede a verificar los elementos recibidos. Primero comprueba si la petición está dentro del período durante el cual P puede depositar. Después verifica si la prueba secreta de P es auténtica calculando $H(W_{1p}) \stackrel{?}{=} W_{0p}$. Entonces, B verifica si P trata de realizar un depósito múltiple verificando si $k \leq j$. Si éste es el caso, B envía a P un mensaje de denegación y la identificación del tramposo es directa, ya que solo P puede depositar la moneda mostrando la prueba secreta W_{1p}. Si no, B verifica que el cupón recibido pertenece a C^* y que es válido. Si la verificación es correcta, B puede depositar el valor de $\frac{k-j}{2}$ cupones si el número de cupones es par o $\frac{k-j-1}{2}$ si es impar en la cuenta de P. El número de cupones se divide entre 2 porque solo la mitad de los cupones recibidos son *cupones de pago* con valor monetario. El resto de cupones solo son *cupones de prueba*.

V-G. Subprotocolo de Reintegro

El *subprotocolo de reintegro* (Cuadro VII) es muy similar al *subprotocolo de depósito* y sirve a U para que pueda reintegrar el valor de los cupones no usados en su cuenta bancaria. Este subprotocolo solo puede usarse durante el intervalo de duración T_2, es decir, $T_d < t < T_r$. Si todas las verificaciones son correctas, B reintegra el valor de los cupones en la cuenta de U.

VI. ANÁLISIS INFORMAL DE PROPIEDADES

VI-A. Eficiencia

El uso de criptografía asimétrica y de clave pública se ha reducido en los pasos en los que es estrictamente necesaria solo para autenticar a los participantes en los subprotocolos de *emisión de cupones*, *depósito* y *reintegro*, es decir, cuando los clientes tienen que acceder a sus cuentas bancarias.

En el *subprotocolo de emisión de cupones* y en el de *reintegro* es necesario identificar a U para vincularlo con su cuenta bancaria en B. Este paso solo es ejecutado una única vez para cada cadena de $2n$ cupones, por lo que el coste del uso de criptografía asimétrica es minimizado. Por su parte, el *subprotocolo de depósito* es ejecutado por P, entidad que presenta mayor capacidad de proceso comparada con un dispositivo móvil, por lo que el uso de certificados de clave pública no supone un impedimento. Además, P no necesita ejecutar el depósito por cada cupón recibido, sino que lo hará por grupos o cuando obtenga la cadena entera. La detección de reuso o doble gasto por parte de B se realiza mediante simples comparaciones de índices, por lo tanto, la carga que tiene que asumir B para detectar comportamientos maliciosos es baja.

El uso de funciones de hash en el *subprotocolo de uso* es menos costoso que el uso de criptografía asimétrica, por lo tanto, el uso continuado de estas funciones no revierte en una disminución del rendimiento del protocolo.

VI-B. Anonimato

La comunicación de U y P con B no puede ser anónima, ya que tiene que estar autenticada y los usuarios identificados para que B acceda a sus cuentas bancarias. En cambio, toda la comunicación entre U y P es anónima ya que usa un

subprotocolo de acceso anónimo. Ni la moneda de cupones, ni los cupones en sí mismos llevan ningún tipo de identificación del usuario, por lo que P no puede deducir la identidad de U.

VI-C. N-vinculabilidad

Los pagos realizados con cupones pertenecientes a una misma moneda son vinculables porque estan relacionados con el mismo identificador. No obstante, ni el proeveedor ni ningún intruso pueden revelar la identidad del usuario que ha realizado el pago. Los proveedores pueden crear un historial de pagos, pero nunca pagos a diferentes receptores pueden ser vinculados. La vinculabilidad del sistema puede minimizarse si se reduce la longitud de las cadenas de cupones.

VI-D. No Trazabilidad

Los pagos pueden ser trazados por B, porque B conoce donde U ha gastado su moneda en los *subprotocolos de depósito* y *reintegro*. No obstante, ni B ni P pueden construir un perfil completo del usuario. Solo si B se confabula con P puede crear un perfil completo del usuario. Estamos trabajando para mejorar esta propiedad en la próxima versión del esquema.

VI-E. Equidad

En el *subprotocolo de uso*, se ejecuta un intercambio de un micropago por un servicio. En este subprotocolo pueden darse situaciones conflictivas que pueden afectar la equidad del intercambio.

Una primera situación conflictiva sucede si maliciosamente P no envía la respuesta de localización en el segundo paso. En este caso, P solo obtiene la primera parte del cupón que U quiere gastar, el *cupón de pago*. Sin el correspondiente *cupón de prueba*, P no puede depositar la moneda en B. El *cupón de prueba* no es enviado por U si éste no recibe la respuesta. Por eso, P se daña a sí mismo si él no envía la respuesta.

Otra situación conflictiva se da si U no envía la prueba secreta del cupón en el tercer paso. De esta forma, U obtiene la respuesta pero P no obtiene el *cupón de prueba*, por lo que en principio P se encuentra en desventaja frente a U. Según el *subprotocolo de uso*, en esta situación P denegará el servicio para posteriores peticiones de localización de U hasta que éste le proporcione el *cupón de prueba* correspondiente o en su caso un nuevo *cupón de pago* con identificador superior al que tiene guardado en su base de datos. Cuando U envía un cupón con un índice mayor, P puede calcular el *cupón de prueba* del último micropago. Así pues, P puede perder como máximo un único cupón, que al ser de muy pequeño valor, se tratará de una pérdida asumible. Notar que si la cadena es de longitud $n = 1$, P puede perder toda la cadena, por eso, es conveniente que el valor de n sea suficientemente grande para que U no pueda beneficiarse maliciosamente. Aunque haya perdido un cupón, P sigue siendo capaz de depositar los cupones recibidos hasta el identificador no recibido. A cambio, U no podrá acceder al servicio hasta que cumpla con su parte y a su vez, U no podría usar la moneda de cupones en otro servicio, ya que la moneda es específica para P.

VI-F. Privacidad

La privacidad del intercambio de mensajes entre U y P se asegura por el cifrado simétrico mediante clave compartida K_S sólamente conocida por U y P, y que ha sido intercambiada de forma segura usando el protocolo ElGamal.

Los datos de localización de U son conocidos por P para que éste le pueda proporcionar el servicio. P podría crear un historial de localizaciones de U, siempre limitado por la vinculabilidad de los cupones de una misma moneda (Ver VI-C), pero de ningún modo podría descubrir la identidad de U (VI-B), esto es, vincular el perfil con una identidad.

VI-G. Robo de Monedas

Las monedas podrían ser robadas si un usuario consiguiera robar toda la cadena de cupones, cosa que es imposible ya que U solo revela cupones individuales (un cupón para pago y un cupón de prueba secreta). Ningún cupón puede ser interceptado por un observador externo a P y U, ya que las comunicaciones son cifradas. En la comunicación entre U y B, U solo revela el identificador final de la cadena, el cual no proporciona ninguna información sobre valores con identificador superior. En caso de robo de toda la cadena, el atacante no podría depositar la cadena sin el conocimiento de la prueba secreta W_{1p}, solo conocida por P.

VI-H. Prevención de la Reutilización

P mantiene una tupla (i, W_{iu}, C^*) para todas las monedas válidas, no caducadas y que aún no están completamente gastadas. P borra la moneda de su base de datos cuando los $2n$ cupones se han recibido o la moneda ha caducado. A medida que recibe nuevos cupones de U, P aumenta y guarda el índice del identificador. Entonces puede impedir la reutilización si U intenta usar un cupón con número de orden inferior o igual al guardado. En este caso, P evita la reutilización denegando el servicio. En todo caso, la detección del intento de reutilización no revela la identidad del reutilizador. Si P deniega el servicio porque está reclamando reuso, P no podrá depositar ya que no tiene la pareja de cupones requerida, y U por su parte, puede solicitar el reintegro.

En los *subprotocolos de depósito* y *reintegro*, la detección de la reutilización se realiza de forma similar, ya que B mantiene una lista de monedas válidas y no caducadas emitidas con el índice correspondiente al último cupón depositado. La comparación de este índice con el nuevo recibido puede revelar el intento de reutilización y B puede denegar el depósito. La identificación del reutilizador es inmediata, ya que sólo P al que va dirigida la moneda es capaz de depositarla con el conocimiento de su prueba secreta.

VI-I. Imposibilidad de Falsificación

La falsificación de la moneda de cupones no es posible ya que su creación requiere del conocimiento de la clave privada de B para la cantidad Q solicitada.

VI-J. Imposibilidad de Sobreutilización

Cuando el *subprotocolo de emisión de cupones* es ejecutado, debido a que está basado en un sistema a débito, B reduce el saldo de la cuenta de U en el momento de la emisión de la moneda. Por tanto, es imposible que un cliente pueda gastar más del saldo disponible en su cuenta bancaria.

VI-K. Minimización de Pasos

Todos los subprotocolos propuestos intentan minimizar el número de pasos necesarios para su ejecución. Así pues, el *subprotocolo de uso* se ejecuta en tres únicos pasos, el mínimo número necesario para obtener la propiedad deseada de equidad. Por otra parte, el *subprotocolo de emisión de cupones* require el envío de solo dos mensajes entre U y B. Finalmente, en los *subprotocolos de depósito* y *reintegro* solo es necesaria una única interacción entre P y B.

VI-L. Bajos Costes de Almacenamiento

Los costes de almacenamiento son reducidos para todos los participantes. Así pues, B y P solo necesitan guardar la tupla (i, W_{iu}, C^*), donde el primer elemento es un entero, el segundo una cadena de carácteres (el último cupón recibido) y el tercero una cadena de bits correspondiente a la moneda y a su firma digital. Esta tupla es borrada de B cuando la fecha máxima de reintegro expira (T_r). P también puede borrar las monedas cuando se hayan depositado por completo. U es el único participante que debe guardar la cadena de cupones entera para su uso.

VI-M. Posibilidad de Reintegro

La definición de tres períodos temporales para el uso, el depósito y el reintegro de la moneda permite consumir parcialmente los paquetes de servicios así como evitar la pérdida de cupones si éstos no fueran usados por U. La separación del período de reintegro del de depósito permite evitar que U pueda pedir el reintegro de cupones usados pero que aún no hubieran sido depositados por P.

VII. Conclusiones

El uso de aplicaciones y servicios basados en localización se está incrementando en los últimos años a medida que se desarrollan y expanden las tecnologías de comunicaciones móviles. El uso de este tipo de servicios ofrecen información de valor añadido a los usuarios y oportunidades de negocio a las empresas. Pero también presentan riesgos para la seguridad de sus usuarios que temen por la privacidad de sus datos. Además de la privacidad, otro punto interesante es la habilidad de los proveedores para cobrar a sus usuarios por los servicios que ofrecen. Esta capacidad es demandada por éstos ya que están interesados en poder recibir pagos pero no obstante, los usuarios no quieren tener el riesgo de perder dinero si pagan por un servicio que posteriormente no usen. Hasta ahora, la manera de cargar a los usuarios era en base a paquetes de subscripción que si no eran consumidos no podían ser reintegrados.

El artículo propone y define por primera vez un protocolo anónimo, eficiente y seguro de acceso a servicios de localización sujetos a pago. El protocolo usa la idea de los esquemas de micropago y además añade un intercambio equitativo entre un micropago y un servicio. El esquema descrito asegura la privacidad de los datos de localización intercambiados entre los participantes de manera que los usuarios no tienen que temer por la revelación de datos privados por un intruso o un atacante. El usuario puede actuar anónimamente cuando se comunica con el proveedor, porque el acceso a éste no necesita ningún tipo de identificación por parte del usuario. Además, el usuario tiene la posibilidad de reintegrar las monedas que no ha gastado, por tanto, los usuarios no tienen el riego de perder dinero. Finalmente, el artículo incluye un análisis informal de las propiedades del protocolo.

El trabajo futuro se centrará en mejorar el esquema propuesto, incorporando aspectos como la privacidad de la localización entre el usuario y el proveedor mediante el estudio de técnicas basadas en PIR [6] u ofuscación de la posición real [4], y la mejora de la propiedad de no trazabilidad. Por otra parte, se está trabajando en la implementación del protocolo sobre la plataforma Android de Google [19]. La adaptación de este protocolo a otro tipo de servicios que requiren otro tipo de propiedades y características también será estudiada, como por ejemplo aplicaciones de aviso de quebrantamiento de órdenes de alejamiento o de estado del tráfico.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el MEC y FEDER bajo los proyectos: ”Seguridad en la Contratación Electrónica basada en Servicios Web”(CICYT TSI2007-62986) y ARES ”Grupo de Investigación Avanzada en Seguridad y Privacidad de la Información”(Consolider - Ingenio CSD2007-004).

Referencias

[1] “http://www.twitter.com.”
[2] “http://www.foursquare.com.”
[3] “http://maps.google.com y http://latitude.google.com.”
[4] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in *MobiSys ’03: Proceedings of the 1st international conference on Mobile systems, applications and services*. New York, NY, USA: ACM, 2003, pp. 31–42.
[5] B. Gedik and L. Liu, “A customizable k-anonymity model for protecting location privacy,” in *In ICDCS*, 2004, pp. 620–629.
[6] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, “Private queries in location based services: anonymizers are not necessary,” in *SIGMOD ’08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data*. New York, NY, USA: ACM, 2008, pp. 121–132.
[7] C. Schmidt and R. Müller, “A framework for micropayment evaluation,” *http://mmm.wiwi.hu-berlin.de/IMI/micropayments.html*, 1996.
[8] J. Kytöjoki and V. Kärpijoki, “Micropayments –requirements and solutions,” *Seminar on Network Security, Security in Electronic Transactions, Proceedings of the Helsinki University of Technology*, 2000.
[9] J. Tygar, “Atomicity in electronic commerce,” *15th annual ACM Symposium on Principles of Distributed Computing, pp. 8-26*, 1996.
[10] L. Liu, “Privacy and location anonymization in location-based services,” *SIGSPATIAL Special, Volume 1, Issue 2 (July 2009), pp. 15-22*, 2009.
[11] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM 24*, 1981.
[12] N. Haller, “The s/key one-time password system,” *RFC 1760*, 1995.
[13] R. Rivest and A. Shamir, “Payword and micromint: Two simple micropayment schemes,” *LNCS 1189, pp. 69-87*, 1996.
[14] S. Micali, “Efficient certificate revocation,” *Technical Report MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science*, 1996.
[15] S. Even, O. Goldreich, and S. Micali, “On-line/off-line digital signatures,” *Advances in Cryptology – CRYPTO ’89, LNCS 435, p. 263-277*, 1989.
[16] R. Hauser, A. Przygienda, and G. Tsudik, “Reducing the cost of security in link state routing,” *In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS ’97), pages 93–99*, 1997.
[17] M. Payeras-Capellà, J. L. Ferrer-Gomila, and L. Huguet-Rotger, “An efficient anonymous scheme for secure micropayments,” *ICWE 2003, LNCS 2722, pp. 80–83*, 2003.
[18] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory, Vol. 31, No. 4*, 1985.
[19] “http://www.android.com/.”

Plataforma de Composición, Provisión y Consumo de Servicios para el Nuevo Universo Inteligente

Ramon Alcarria, Tomas Robles, Augusto Morales Domínguez, Sergio González-Miranda
Departamento de Ingeniería de Sistemas Telemáticos.
Universidad Politécnica de Madrid
Av. Complutense, 30. 28040 Madrid
{ralcarria, trobles, amorales, miranda}@dit.upm.es

***Resumen*- La sociedad actual necesita nuevas soluciones en el ámbito de la creación y provisión de servicios. El concepto de universo inteligente asegura una relación más fácil e intuitiva entre el usuario, su terminal y el entorno que le rodea, permitiéndole generar nuevos servicios y provisionarlos para que otros usuarios puedan consumirlos. Se propone una arquitectura basada en componentes como la mejor solución para lograr un bajo acoplamiento entre la lógica de servicio y la implementación de bajo nivel, desarrollada a través de un escenario relativo al universo inteligente, detectando los principales problemas que aparecen en el desarrollo de este tipo de arquitecturas: Interacción entre subsistemas, gestión de componentes, formato de los datos intercambiados y bajo acoplamiento en el acceso a las capacidades del entorno. Como validación de la arquitectura se describe una propuesta de implementación de una plataforma de composición, provisión y consumo de servicios.**

***Palabras Clave*- Provisión de servicios, composición, arquitecturas basadas en componentes, *Service Description Language*.**

I. INTRODUCCIÓN, EL NUEVO UNIVERSO INTELIGENTE

Un nuevo modelo de servicio es necesario en una sociedad en la que los individuos, compañías y ciudades están relacionados, y en la que los usuarios contribuyen con información procedente de sus propios servicios al resto de la comunidad. Para resolver las necesidades de evolución de la sociedad actual se proporcionan algunas guías[1] que deben tenerse en cuenta:

La creatividad en productos, servicios e información multimedia será mejorada gracias a la evolución de las tecnologías que permiten a los usuarios crear y prestar sus servicios de forma inmediata, utilizando el terminal móvil extendido con capacidades del entorno.

El estudio de tecnologías de interfaz permitirá desarrollar servicios que combinen información real con virtual, contribuyendo así a la mezcla entre el mundo real y el digital.

También será necesario desarrollar nuevas tecnologías que permitan a los ciudadanos escoger libremente y de forma sencilla qué servicios necesitan. La posibilidad de generar servicios por los propios usuarios y la existencia de elementos de red que rodean tanto a los usuarios como a sus terminales móviles contribuyen al concepto de *Mobile 2.0* y a la evolución de una sociedad de masas a una sociedad de la información.

Este trabajo analiza el entorno tecnológico de un futuro universo inteligente. El paradigma de universo inteligente sitúa al usuario en el centro del entorno. Este usuario, usando su teléfono móvil, puede diseñar sus servicios seleccionando los componentes apropiados de un catálogo de componentes y utilizando herramientas de interacción que le permitan conectar estos componentes y configurarlos a su antojo. El concepto de universo inteligente surge como la evolución lógica de la relación de los usuarios con sus teléfonos móviles y con los servicios y capacidades que los rodean. El usuario, en movilidad, interactuará con elementos cercanos que proporcionarán capacidades o funcionalidades que podrán ser utilizadas para componer servicios.

El usuario, como elemento central del entorno, podrá interactuar con el universo de servicios existente: información, entretenimiento, relaciones sociales, servicios propios, etc. Las posibilidades de este paradigma son innumerables. En la Fig. 1 puede verse a un usuario accediendo a través de la pantalla interactiva de una marquesina de autobús a un servicio de transporte público y, en la imagen de debajo, los turistas están utilizando unas gafas de realidad aumentada para observar el aspecto de la mezquita cuando fue creada.

El usuario *prosumer*, utilizando su terminal para componer, provisionar y consumir servicios, es el principal actor en este entorno futuro. El término *prosumer* [2] es un acrónimo formado por la fusión de las palabras en inglés *producer* y *consumer*. En la actualidad este término se aplica a aquellos usuarios que son al mismo tiempo consumidores y productores de servicios y contenidos. La palabra prosumer describe perfectamente a millones de usuarios en la revolución de la Web2.0, ya que estos están cada vez más involucrados en la provisión de información a la red y, al mismo tiempo, son consumidores de la misma. Este término tiene similaridades con el utilizado en el modelo EMEREC de Jean Cloutier [3], que asume que los nuevos medios de comunicación permiten que cualquier usuario sea al mismo tiempo emisor y receptor de mensajes. Este cambio de visión, en la que los usuarios se transforman en proveedores de

[1] Basado en el informe ISTAG [1] para la comisión europea en Marzo de 2006

servicios, llamada Nomadic Mobile Service Provisioning [4], tiene una gran relevancia, ya que constituye un paso más hacia la realización práctica de muchos paradigmas de computación que están siendo investigados actualmente (computación ubicua, inteligencia ambiental o sistemas sensibles al contexto, entre otros).

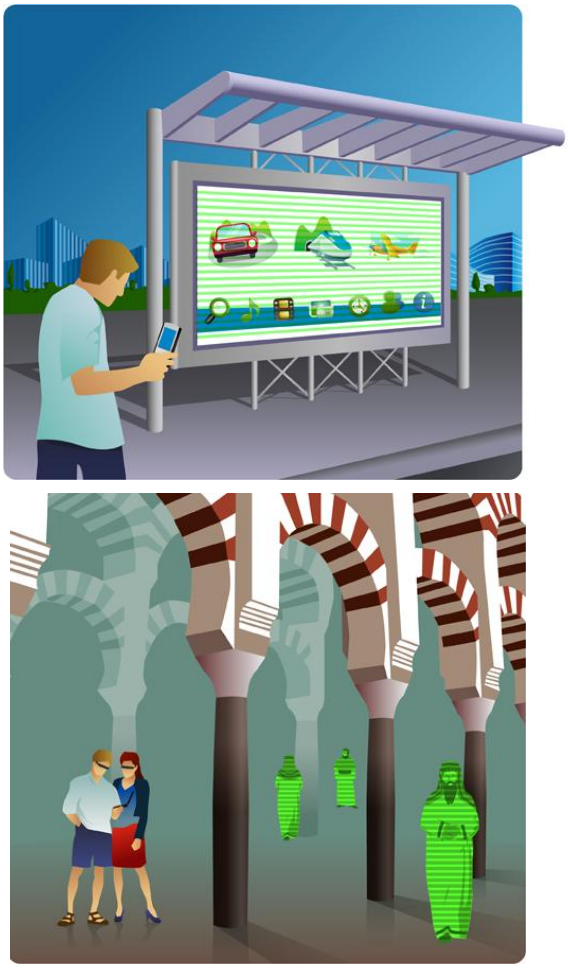


Fig. 1. Tecnologías y aplicaciones móviles.

Para que la visión del usuario *prosumer* se haga realidad dentro del contexto del universo inteligente es necesario diseñar una arquitectura basada en componentes que permita desacoplar la lógica de servicio definida por el usuario con la funcionalidad implementada por cada componente. Para esto proponemos una solución para el diseño de una plataforma de composición, provisión y consumo de servicios en la que un usuario inexperto, o no familiarizado con las tecnologías de creación pueda crear sus propios servicios mediante la combinación y la interacción de componentes.

En la sección **II Ciclo de Vida de un Servicio** se define un conjunto de estados en los que un servicio puede situarse. Además, se proporcionan terminología y varias razones para utilizar una arquitectura software basada en componentes para este tipo de entornos. En la sección **III Arquitectura funcional para la creación, provisión y consumo de servicios** se presenta la arquitectura del sistema describiendo los principales sistemas de los que se compone. Como principal sección de este trabajo, realizamos un esfuerzo en describir nuestras contribuciones a los principales problemas tecnológicos que se encuentran al utilizar arquitecturas basadas en componentes. En la sección **IV Validación de la arquitectura** se introducen las tecnologías disponibles para hacer frente a los problemas tecnológicos citados en la anterior sección y en la sección **V Conclusiones** se explica cómo esta propuesta contribuye a la validación de este nuevo paradigma tecnológico.

II. Ciclo de Vida de un Servicio

La creación y la provisión de servicios deben basarse en un ciclo de vida preciso. Antes de describir el proceso del ciclo de vida es importante presentar cuáles son los elementos lógicos que definen un servicio.

Basándonos en análisis de casos de uso y escenarios y en la identificación de elementos tecnológicos clave que aparecen en la plataforma de creación y composición de servicios diseñada hemos determinado que un servicio presenta una estructura lógica que debe ser definida en diferentes niveles dependiendo del rol que cada usuario interpreta, como consumidor o productor de servicios.

La utilización de una arquitectura basada en componentes está justificada por la necesidad de separar conceptualmente los distintos procesos que han de llevarse a cabo durante el ciclo de vida de un servicio. Definiendo un servicio como un conjunto de componentes interconectados se mejora el intercambio de datos, esto es, los distintos tipos de datos generados como resultado de operaciones que se producen dentro de los componentes. También el servicio adquiere algunas características y propiedades que difícilmente podrían ser adquiridas por decisiones que el usuario creador hubiera efectuado sobre un servicio completo.

A. *Estructura lógica de un servicio*

Podemos definir un servicio de muchas formas, dependiendo del estado del ciclo de vida en el que se encuentra. La estructura lógica de un servicio ha sido dividida en tres niveles que corresponden con el nivel de usuario, el nivel de creación y en nivel de ejecución. En la siguiente figura puede verse un ejemplo de servicio (*Sport Tracker*) creado por un usuario que pretende visualizar en un mapa su localización e información sobre su pulso cardiaco cuando sale a correr. Siguiendo el paradigma del universo inteligente el usuario debe tener un sistema para crear servicios de forma fácil desde su móvil donde, con sólo agregar los componentes de Localización, Mapa y Pulso cardiaco y algunas opciones de configuración, este servicio pueda ser generado automáticamente por la plataforma. En tiempo de ejecución el servicio accederá a las capacidades disponibles en el entorno

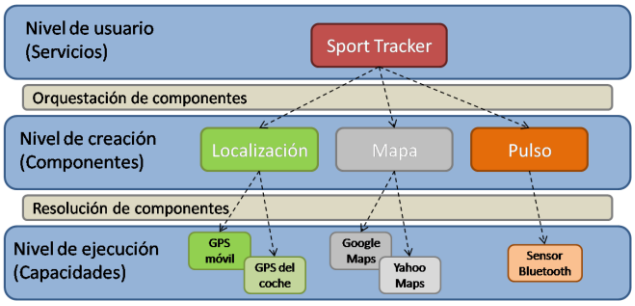


Fig. 2. Estructura lógica del servicio *Sport Tracker*.

que le permitirán resolver estos componentes de la mejor manera posible. Una vez que el servicio está creado el usuario puede publicarlo para que otras personas lo puedan ejecutar y puedan beneficiarse de la información que proporciona.

Desde el punto de vista del usuario (**nivel de usuario**), el servicio puede verse como una estructura monolítica donde los componentes permanecen ocultos. Esta visión corresponde a un modelo de caja negra [5] donde el usuario que consume el servicio puede permanecer ajeno a la funcionalidad interna del mismo mientras conozca el resultado de ejecutarlo. El elemento más importante en este nivel es la interfaz gráfica de servicio, que contiene la lógica necesaria para procesar las acciones del usuario y mostrar una respuesta apropiada.

Continuando con el **nivel de creación** el servicio puede dividirse en unidades lógicas denominadas componentes, los cuales están interconectados mediante conectores y una lógica que describe la funcionalidad del servicio. Definimos un componente como la unidad básica funcional de un servicio. Es una abstracción de alto nivel que se implementa con una capacidad encontrada, dependiendo de las condiciones de ejecución de servicio. Los componentes son utilizados por el sistema para hacer un proceso de creación más sencillo y para proporcionar el nivel de abstracción adecuado para que un usuario pueda comprender su funcionamiento pero los detalles de implementación permanezcan ocultos. Es importante recordar que esta propuesta tiene como restricciones las condiciones impuestas por el universo inteligente en el que un usuario no experto puede crear servicios de un forma sencilla.

Llamamos **orquestación de componentes** al proceso por el cual se define un flujo resultado de la combinación de diversos componentes. Este flujo es en general controlado por una entidad externa a los componentes que determina el orden de ejecución de los mismos y realiza las correspondientes invocaciones, al contrario que el proceso de coreografía, en el que los componentes son conscientes del lugar que ocupan dentro del flujo e invocan al siguiente componente en orden, una vez que han terminado de ofrecer su funcionalidad.

Desde el punto de vista del **nivel de ejecución**, un servicio es un conjunto de capacidades que ofrecen las funcionalidades que el servicio pretende cumplir. Una capacidad es la implementación de un componente utilizado en el entorno de creación. Las capacidades se encuentran en repositorios locales, cercanos o remotos y pueden ser dispositivos como una impresora, un monitor o recursos como un servidor web, etc. La división entre los modelos de componente y capacidad se ha realizado por dos razones:

El empleo de componentes, más allá de la importancia que tienen en la reutilización de código, supone una enorme ventaja para el usuario en el proceso de creación ya que una generación de servicios basada en el empleo de *workflows* de componentes es una buena alternativa para un usuario no experto a la hora de crear servicios simples.

Las capacidades ocultan características particulares del elemento al que están accediendo proporcionando un middleware con métodos conocidos que son compatibles con la gestión de componentes. De esta forma, un componente puede ser resuelto con diferentes capacidades dependiendo de las condiciones de ejecución del servicio y de las preferencias proporcionadas por el usuario en el proceso de creación. Como las capacidades proporcionan un conjunto común de métodos para acceder a los recursos, los componentes pueden utilizar los nombres de los métodos desacoplando así la funcionalidad proporcionada de la implementación particular de esta funcionalidad.

Llamamos **resolución** al proceso por el cual una capacidad se asigna a un componente en tiempo de ejecución. Según lo que se ha comentado sobre componentes y capacidades se necesita identificar un componente con una capacidad que sepa implementarlo. El proceso de decisión para encontrar la capacidad óptima para un componente dado se denomina proceso de armonización de capacidades. Encontrar la capacidad óptima depende de múltiples factores, por ejemplo, de las opciones de configuración que el usuario ha establecido en tiempo de creación y que se convertirán en restricciones utilizadas en el proceso de armonización de capacidades para seleccionar la capacidad apropiada. En la siguiente sección se describe con detalle este proceso y cómo se transforman las preferencias de usuario a restricciones. En la Fig. 2, el componente del servicio *Sport Tracker*, denominado "Pulso cardiaco", siempre accede a la capacidad "sensor Bluetooth" mientras que el componente de "Mapa" puede ser resuelto por distintos proveedores de mapas (Google o Yahoo) dependiendo de preferencias de usuario o restricciones en el servicio.

B. Descripción del ciclo de vida de un servicio

Definimos el ciclo de vida de un servicio como el conjunto de estados entre los que el servicio puede encontrarse, desde su creación hasta su destrucción, y el conjunto de operaciones que pueden llevarse a cabo en cada estado y que producen una transición hacia otro estado. La Fig. 3 muestra una representación gráfica del ciclo de vida de un servicio.

El servicio comienza a existir en manos del creador (**proceso de creación**). El creador utiliza las herramientas que proporciona la plataforma para crear su servicio desde cero o a partir de un servicio creado previamente. En todo caso, el usuario arrastra algunos componentes en el entorno de creación y establece conexiones entre ellos. Estos componentes han sido previamente creados por un desarrollador de la plataforma y almacenados en un repositorio de componentes al que el sistema tiene acceso. El usuario creador, además, configura los componentes con el fin de establecer restricciones que serán tenidas en cuenta en tiempo de resolución. Con la información introducida por el usuario el servicio está listo para ser desplegado.

El principal objetivo del proceso de publicación es que el servicio generado esté disponible para todos los usuarios que utilicen la plataforma. Un repositorio distribuido se utiliza para almacenar la referencia del servicio, indexándolas por categorías (**repositorio de servicios**). Si un usuario pretende consumir el servicio publicado el proceso de búsqueda y descubrimiento se pondrá en marcha. En el proceso de búsqueda el usuario mantiene un rol activo e inicia una búsqueda de servicios introduciendo algunas palabras clave en un motor de búsqueda. Respecto al proceso de descubrimiento, en este caso es la plataforma la que juega un rol activo mediante la selección del servicio más adecuado de

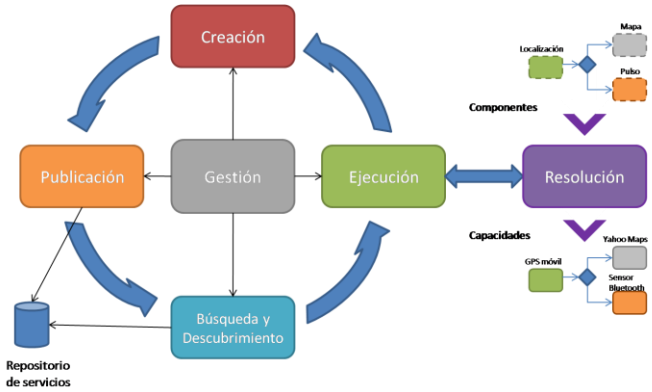


Fig. 3. Ciclo de vida de un servicio.

acuerdo con preferencias de usuario o información de contexto.

El **proceso de ejecución** arranca tanto en el terminal del usuario consumidor como en el del usuario proveedor. Este estado es alcanzado cuando el usuario ha descubierto un servicio y contacta con el usuario proveedor del mismo. La plataforma gestiona esta petición y arranca una sesión que conecta los dos entornos de ejecución. En este punto la parte cliente del servicio a ejecutar es transferida al terminal del usuario consumidor mientras que la parte servidora permanece en el dispositivo del usuario proveedor. Antes de empezar la ejecución se necesita completar de forma satisfactoria el proceso de resolución para que se asignen las capacidades apropiadas a los componentes involucrados en el servicio. Para completar el ciclo el usuario podría decidir crear un nuevo servicio basado en el anterior. Para ello accedería al repositorio de servicios y descargaría el código fuente del mismo para posteriormente cargar esta información en el entorno de creación, modificar el servicio a su antojo y volviendo a publicar esta copia personalizada.

El **proceso de resolución** es invocado por el proceso de ejecución para asignar una capacidad a cada componente que la requiera. En este proceso tienen que tenerse en cuenta algunos factores como las restricciones impuestas por los componentes, el contexto de ejecución, las limitaciones hardware y software del dispositivo, etc. La posibilidad de mantener un proceso de resolución es una de las principales ventajas de una arquitectura basada en componentes que permite crear servicios de una manera sencilla que accedan a las capacidades del entorno que rodea al usuario.

El último proceso que se ha definido es el **proceso de gestión de servicios**. Este proceso ocurre de manera trasversal al resto del ciclo de vida de un servicio y proporciona a los distintos usuarios de la plataforma herramientas para crear, modificar o eliminar los servicios o las sesiones almacenados en sus dispositivos. Por ejemplo, un usuario puede eliminar la información de publicación de un servicio que publicó hace tiempo y que ya no le interesa proveer.

III. Arquitectura Basada en Componentes para la Composición, Provisión y Consumo de Servicios

Las propuestas de arquitectura SOA (*Service Oriented Architecture*) sitúan al servicio como la unidad básica funcional y proporcionan mecanismos para la creación, provisión y consumo sin tener en consideración que, en algunas ocasiones, estos servicios han sido generados utilizando una estructura basada en componentes. Estos componentes están interrelacionados e intercambian información que puede ser útil para el posterior tratamiento del servicio. Esto debe tenerse en cuenta a la hora de diseñar un modelo de arquitectura para este tipo de plataformas.

Durante algunos años se han propuesto muchos modelos de arquitectura que consideran técnicas de generación para componentes software. Czamecki y Eisenecker [6] desarrollan un trabajo muy interesante desde el punto de vista de la "ingeniería del dominio". El problema de este trabajo aparece a nivel de diseño de la arquitectura, ya que no describe de forma precisa la separación entre las especificaciones que definen un componente y la implementación de éste. Además la separación lógica entre las interfaces de composición y la información intercambiada debería ser más clara. En nuestro trabajo los modelos de componente y capacidad están perfectamente definidos y separados y en esta sección se describe la solución que permite un bajo acoplamiento entre interfaces y tipos de datos intercambiados.

En el trabajo de Hans de Bruin [7] se utilizan algunas técnicas de generación basadas en "Grafos de Características" para la transferencia de conocimiento. Estas técnicas se utilizan de forma independiente para obtener, por una parte, requisitos funcionales y no funcionales, y por otra, soluciones que cumplan estos requisitos. El problema de esta propuesta es que si se encuentran nuevos aspectos que definen un componente la arquitectura tiene que ser rediseñada. Desde nuestro punto de vista no es misión de la arquitectura el considerar estos aspectos (por ejemplo rendimiento o seguridad en los servicios) sino que debe existir un proceso de resolución en el que las preferencias de seguridad se conviertan en restricciones utilizadas para elegir capacidades más seguras. De esta forma se obtiene la división lógica entre el diseño del componente y su implementación y ejecución.

Existen otras contribuciones como entornos adaptativos con cambios de comportamiento en los componentes dependiendo de los cambios en el entorno (véase el trabajo de Zewdie [8] en el que los componentes mantienen una fase de reconocimiento del entorno donde se establecen unos parámetros que influyen en la ejecución del mismo a través de distintos "puntos de variabilidad"). El problema de este diseño es que todos los posibles cambios en el comportamiento del componente deben ser definidos dentro de éste por lo que, una vez que el componente ha sido definido sus cambios de comportamiento son fijos, sin posibilidad de añadir más "puntos de variabilidad". En este trabajo se propone que esta variabilidad vaya ligada al proceso de armonización de capacidades y así, por ejemplo, si un usuario desea que un servicio se ejecute utilizando los mínimos recursos posibles estas preferencias actuarán en el proceso de resolución recomendando la asignación de capacidades más "ahorradoras". Creemos que esta solución es más efectiva que diseñar cada componente con puntos de variabilidad para un bajo consumo de procesador y memoria.

Esta sección describe la parte principal de nuestra contribución en la que se propone una arquitectura funcional para el diseño de una plataforma de composición, provisión y consumo de servicios a través de un conjunto de subsistemas

que realizan diferentes acciones de acuerdo con la descripción del ciclo de vida del servicio de la sección II.

A. *Arquitectura funcional*

La arquitectura funcional diseñada en este trabajo se compone de distintos sistemas que interactúan entre sí: creación, publicación, ejecución, búsqueda y descubrimiento y armonización de capacidades. La Fig. 4 propone una arquitectura general para esta plataforma.

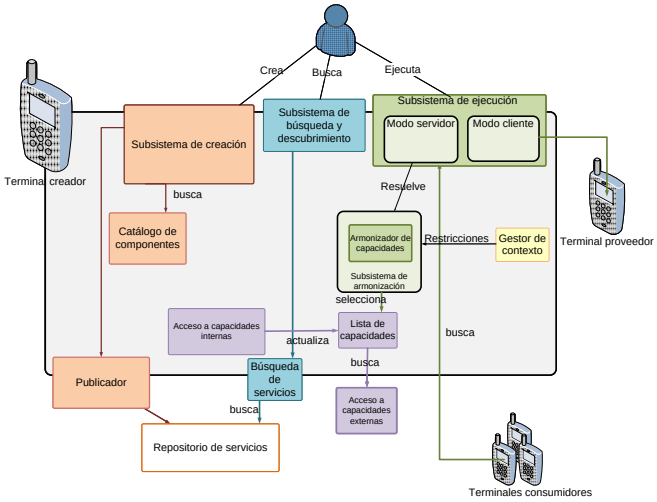


Fig. 4. Propuesta de arquitectura general.

Subsistema de creación: proporciona una interfaz para el usuario no experto que resulta fácil de utilizar, permitiéndole crear sus propios servicios utilizando componentes como elementos atómicos del proceso de creación.

Subsistema de publicación: una vez que el usuario ha creado sus servicios necesitará publicarlos en repositorios para que otros usuarios los encuentren.

Subsistema de ejecución: el objetivo de este sistema es servir como entorno de ejecución de los servicios. Puede funcionar en modo cliente, servidor o ambos.

Subsistema de búsqueda y descubrimiento: incluye un conjunto de herramientas que facilitan que los usuarios puedan encontrar cualquier servicio publicado (búsqueda) y permite al entorno móvil seleccionar de forma automática el servicio más apropiado para el usuario, basado en preferencias e información contextual (descubrimiento).

Subsistema de armonización: Mientras que el componente es la unidad atómica en el proceso de creación, el término capacidad se relaciona con la implementación de la funcionalidad de este componente. Los componentes manejados por el *prosumer* deben ser fáciles de comprender y utilizar y pueden ser utilizados para la creación de múltiples servicios. Las capacidades identifican recursos que serán utilizados por el componente para cumplir su propósito. En este subsistema se produce la elección de la capacidad más apropiada para el componente que la requiera. Por ejemplo, si el usuario quiere crear un servicio para ver su localización en un mapa, en el subsistema de armonización se buscará la capacidad de localización más apropiada, por ejemplo, la capacidad GPS interna del móvil o un dispositivo GPS Bluetooth que el usuario lleva conectado.

B. *Problemas tecnológicos*

Durante el diseño de la arquitectura del sistema hemos identificado algunos problemas tecnológicos que describimos a continuación incluyendo la solución hallada para cada caso.

El primer problema que se ha tratado es cómo hacer que la **interacción entre subsistemas** funcione. Los servicios creados deben ser publicados antes de que sean requeridos por otros usuarios y ejecutados en el entorno de ejecución. Por eso, mecanismos como la publicación, que mantiene el ciclo de vida del servicio, han sido integrados en la plataforma.

Para que exista una interacción entre subsistemas es necesario definir un Lenguaje de Descripción de Servicios (SDL) que describa al servicio a lo largo de su ciclo de vida. Definimos el SDL como un conjunto de reglas gramaticales y sintácticas que permiten la descripción de los diferentes aspectos de un servicio, como la funcionalidad que proporciona, aspectos de seguridad, autenticación, capacidades no-funcionales e incluso las posibles interacciones con otros servicios. Para el diseño del SDL hemos tenido en cuenta que la plataforma se integra en dispositivos móviles por lo que se necesita un SDL ligero y no muy complejo.

Existen muchos lenguajes estándar que pueden utilizarse como BPEL [9], que emerge como la solución general para la composición de servicios Web en los procesos de negocio. BPEL requiere una interfaz de descripción bastante rígida [10] en la que se deben proporcionar datos como los nombres para los tipos de puerto, nombres de operación para servicios Web, etc. Además ni el estándar BPEL ni las actuales extensiones soportan características de reutilización [11]. En otras palabras, necesitamos un mecanismo más modular y granular para definir y describir fragmentos reutilizables de modelos de proceso de negocio.

La iniciativa OWL-S [12] se centra en la descripción semántica de servicios Web y en la automatización de un conjunto de tareas como el descubrimiento de servicios Web y su composición. Desde un punto de vista técnico OWL-S constituye una buena alternativa a considerar gracias a su enfoque directo. Sin embargo existen algunos puntos y responsabilidades que no están claros desde el punto de vista de los modelos de negocio, como la falta de monitorización y el manejo de errores [13]. Otros aspectos como la escalabilidad de la tecnología y la necesidad de intervención manual para la gestión de servicios Web convierte a la tecnología OWL-S en una opción no muy viable para entorno de ejecución en tiempo real.

Teniendo en cuenta las ventajas de BPEL y de OWL-S se decidió diseñar un lenguaje SDL propio siguiendo las siguientes premisas:

El documento SDL está dividido en distintas vistas, que contienen la información proporcionada por todos los subsistemas.

El SDL está basado en XML (*eXtensive Markup Language*) [14]. La utilización de este lenguaje proporciona modularidad y mecanismos estándar para modificar el documento.

Cada vista SDL se define utilizando distintos lenguajes basados en XML, por lo que será posible encontrar una vista semántica en OWL o RDF, una vista de ejecución descrita en alguna variante de BPEL o SCA [15] o una vista de presentación expresada en XHTML y JavaScript.

Este SDL actúa como mecanismo de enlace entre los distintos subsistemas de la plataforma y contendrá requisitos

especificados en uno de los subsistemas que actuarán como restricciones en otro de ellos (por ejemplo los requisitos impuestos en creación pueden ser decisivos en el proceso de armonización de capacidades).

Otro problema que ha sido considerado es como gestionar los componentes que se utilizan para construir un servicio compuesto. Los componentes son arrastrados en el entorno de creación y son interconectados. En el entorno de ejecución estos componentes son procesados y ejecutados siguiendo las conexiones definidas, las cuales establecen el flujo de ejecución. Para producir una interacción entre componentes sencilla ha sido necesario proporcionar mecanismos de gestión de componentes que permitan que se intercambien datos entre componentes conectados. En esta sección se analiza una tecnología que hace posible esta gestión:

La tecnología OSGi [16] define una infraestructura eficiente para el despliegue de aplicaciones basadas en servicios sobre una máquina virtual de Java (JVM). Este *framework* de desarrollo implementa un modelo dinámico de componentes o bundles, que pueden ser instalados, desinstalados, ejecutados y detenidos de forma remota, sin necesidad de reiniciar el dispositivo o el *framework*.

El elemento clave en la plataforma OSGi es el bundle. Un bundle puede consumir servicios de otros bundles y puede proporcionar servicios a éstos gracias a que es posible registrar un servicio en el *framework* al proporcionar una interfaz y una clase Java que la implemente. Cualquier cambio en el estado de un servicio (registro, modificación, desregistro) produce eventos que son capturados y procesados por el *framework*.

El archivo de manifiesto (Manifest.mf) es un archivo de configuración que el bundle proporciona a la plataforma. Contiene información sobre cómo ejecutar el bundle, si el bundle interactúa con otros, paquetes que importa o exporta, etc.

Sin embargo, esta tecnología, que permite implementar arquitecturas basadas en componentes no es adecuada para gestionar componentes que no existían previamente en la plataforma [17][18]. Un escenario básico con dos componentes que intercambian datos puede ser implementado en una plataforma OSGi con dos bundles. Uno de ellos constituye el proveedor de datos y el otro el consumidor. Para que el intercambio de datos se lleve a cabo el bundle consumidor debe encontrar el servicio declarado por el bundle proveedor mediante una búsqueda con filtros basados en propiedades. Utilizando la tecnología OSGi existen limitaciones en el lado proveedor como una falta de dinamismo en la declaración de propiedades de los servicios y en el lado consumidor como la poca expresividad en las declaraciones de filtros de búsqueda de servicios. Por tanto, se necesita extender la plataforma OSGi para que gestione dependencias dinámicas más allá del modelo de servicios declarativos (DS), derivado del proyecto Service Binder [19][20].

La especificación DS permite a los desarrolladores especificar dependencias de componentes en un archivo XML. Nuestra propuesta incluye un nuevo bundle que gestiona las vinculaciones de cada uno de los bundles que componen un servicio. Este nuevo bundle asigna una instancia de un gestor de bundles (bundleManager) a cada componente en su proceso de arranque para que este gestor resuelva sus dependencias en tiempo de ejecución utilizando peticiones de servicio OSGi. La pérdida de una vinculación (producida por un desregistro de servicio, fallo en el proceso de negociación/adaptación, etc) produce un evento que es capturado por el gestor de componentes, el cual intenta encontrar otro proveedor de servicio o, si la búsqueda no resulta fructífera, desactivar el componente.

Otro elemento que ha sido resuelto es el **intercambio de datos entre los componentes**. Los componentes utilizados para crear servicios son piezas de código compiladas que pueden verse en el entorno de creación como cajas negras, con entradas, salidas y algunos parámetros de configuración. El tipo de datos intercambiado entre componentes se describe en el documento SDL del componente con la particularidad de que, en algunas conexiones, la información aceptada por un componente a su entrada no corresponde con la información que otro componente envía. Para resolver este problema se pueden utilizar dos enfoques distintos.

Una solución radica en la utilización de mecanismos de adaptación entre componentes. La adaptación se define como la transformación del formato de los datos de salida de un componente para que se ajuste al formato aceptado a la entrada de otro componente. Para que la adaptación se lleve a cabo se necesita un componente adaptador para cada punto de comunicación de los componentes, que se sitúe en medio de los componentes a adaptar. El principal inconveniente de esta propuesta es que se necesita un gran catálogo de adaptadores que sean capaces de transformar el formato de salida de un componente a otros muchos formatos de entrada.

Otra solución es definir un proceso de negociación entre componentes. En este caso un componente contempla más de un tipo de datos en sus puntos de comunicación. El bundle especial que vincula una instancia de *bundleManager* a cada bundle en su proceso de arranque pasa a denominarse ***mediador***. Cuando el usuario intenta conectar dos componentes, el mediador permite que esos componentes interactúen y que determinen cual es el mejor formato y tipo de dato que debe ser intercambiado.

El proceso de negociación introduce las siguientes ventajas:

- No son necesarios nuevos componentes que actúen como adaptadores sino que las transformaciones están integradas en la implementación del componente.
- La adaptación podría considerarse un mecanismo fácil para realizar conexiones pero al no existir un proceso de negociación entre los datos intercambiados (codificación, resolución, bitrate) en el proceso de adaptación quizás este mecanismo no sea el más adecuado desde el punto de vista de la flexibilidad y el rendimiento en ejecución.

El último elemento que se ha definido es el mecanismo utilizado para desacoplar la implementación del componente con el mecanismo de acceso a la capacidad.

Considerando un recurso que proporciona una funcionalidad que ha sido representada como una capacidad dentro de la plataforma el primer paso es realizar un envoltorio que rodee el acceso al recurso de una manera uniforme para que los componentes puedan acceder a todos los recursos de la misma forma. Por ejemplo, si se desea utilizar la funcionalidad GPS del teléfono móvil para esta plataforma el recurso GPS se envuelve como una capacidad genérica de GPS para que pueda ser utilizado como una capacidad estándar por el módulo de gestión de capacidades. Internamente, la envoltura realiza una conversión del lenguaje y tipo de datos utilizado en la plataforma (para tratar capacidades genéricas) al formato utilizado por el sistema operativo del terminal móvil para acceder físicamente al módulo GPS. Al tratar cada capacidad utilizando la misma

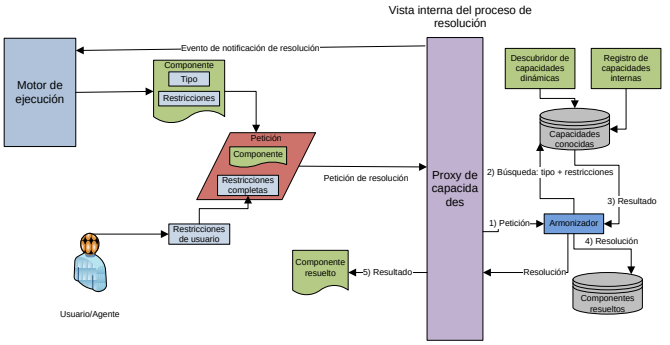


Fig. 5. Proceso de resolución de capacidades.

sintaxis es posible lograr la armonización de las mismas mientras el usuario está en movilidad y las capacidades que lo rodean cambian constantemente.

La Fig. 5 muestra el proceso de resolución de capacidades que hemos definido, realizado por el subsistema de resolución:

Para llevar a cabo la resolución de componentes se necesita realizar una petición al proxy de capacidades, proporcionando información como el componente a resolver y las restricciones impuestas por el usuario (1). El modulo de armonización de capacidades inicia una búsqueda por distintos repositorios conocidos por la plataforma (2). Como resultado de la búsqueda se seleccionan un conjunto de capacidades (3). Dentro de este conjunto de capacidades, compatibles con las restricciones proporcionadas, la elección de la capacidad óptima se delega al usuario o a un agente inteligente que toma este tipo de decisiones por el usuario (4). Cuando el componente ha sido resuelto se puede proceder a su ejecución como parte del proceso de ejecución.

Como puede verse, el subsistema de armonización de capacidades funciona como una plataforma middleware orientada a componentes que logra el desacoplamiento entre lógica de proceso y la implementación funcional de un componente dado.

IV. Validación de la Arquitectura

La sección de introducción presentaba los problemas de la creación y el consumo de servicios en el marco del universo inteligente. Esta propuesta intenta definir los mecanismos de creación, ejecución y armonización para que un usuario, sin conocimientos de programación y con una experiencia limitada en informática, pueda diseñar, implementar y, por supuesto, consumir sus servicios siguiendo la filosofía del usuario *prosumer*.

Estos mecanismos han sido analizados utilizando una plataforma de despliegue de servicios que considera al componente como la unidad funcional de la plataforma y participa en los procesos de creación, publicación, búsqueda y ejecución. Según lo revisado, la tecnología OSGi supone una buena candidata para la implementación del sistema, manteniendo el modelo de arquitectura basado en componentes definido en este trabajo.

La utilización de una arquitectura basada en componentes proporciona una ventaja clara en el entorno de creación. Las posibilidades de creación para un usuario no experto crecen considerablemente cuando manejan componentes que tienen una funcionalidad fácil de entender, como provisión de localización y mapas, temperatura, transmisión de video, impresión, etc. Además, tratar directamente con servicios completos no ofrece la flexibilidad y las posibilidades de configuración que pueden lograrse con la inclusión de patrones de combinación de componentes y asistentes de creación de servicios. Estos mecanismos están separados de la lógica de servicio y pueden ser provistos por la interfaz gráfica del subsistema de creación, sin afectar al funcionamiento del motor de creación.

En un nivel inferior se establecen relaciones y correspondencias entre componentes a través de conectores y se realizan comprobaciones de compatibilidad para comprobar la viabilidad de la conexión y también negociaciones entre las entradas y las salidas de los componentes. El resultado de esa negociación será un acuerdo sobre el tipo de datos intercambiados entre esos dos componentes [21]. Este acuerdo queda reflejado en un contrato localizado en un documento y referenciado desde el SDL del servicio. En el subsistema de ejecución existe un elemento que controla que los componentes siguen el contrato firmado.

Toda la información generada durante el proceso de creación (componentes utilizados, personalización de los mismos, conexiones entre componentes, contratos, etc) se almacena en el documento SDL que se utiliza para que la interacción entre subsistemas funcione (ver Fig. 6). Esta información estará constituida por un conjunto de referencias a la colección de contratos, las propiedades de los componentes y los bundles OSGi. Estos tres elementos son publicados junto con el documento SDL para constituir un servicio completo.

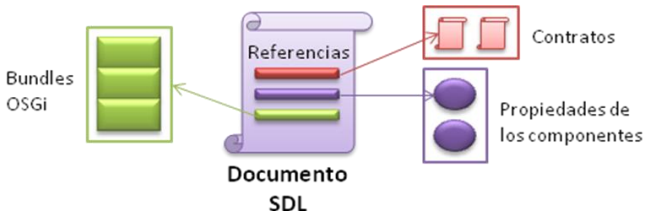


Fig. 6. Documento SDL, generado en el proceso de creación.

En el subsistema de ejecución se proporciona un motor que interpreta el documento SDL y configura los componentes OSGi. A este subsistema se le confía también la tarea de de transmitir al subsistema de armonización de capacidades las propiedades de los componentes que actúan como restricciones para que en el proceso de resolución se selecciones la capacidad óptima para cada componente. El gestor de capacidades proporciona acceso uniforme a las capacidades locales (situadas en el dispositivo móvil), próximas (en el entorno cercano) y remotas.

A modo de validación de la solución propuesta en la sección III, hemos desarrollado un activo experimental que, siguiendo un escenario de creación del servicio *Sport Tracker* estudiado anteriormente, incorpora una interfaz de creación mediante la cual un usuario puede arrastrar e interconectar componentes para crear servicios sencillos. Las acciones del usuario sobre la interfaz de creación se traducen a llamadas a un API que comunica la interfaz gráfica de creación con el motor de generación del documento SDL, el cual almacena la información generada en proceso de creación. Este motor, además, utiliza las preferencias introducidas por el usuario creador (proveedor de Mapas, conexión con el dispositivo GPS, preferencias de consumo y rendimiento) para generar una vista ejecutable del servicio. La vista ejecutable contiene información sobre el orden de los componentes a ejecutar, los tipos de datos que deben intercambiarse y las restricciones para el acceso a capacidades, que serán utilizadas en el proceso de resolución. El uso de la tecnología OSGi viene

justificado por la posibilidad de instalar, desinstalar y ejecutar los componentes de un servicio (implementados como bundles OSGi) según la información contenida en la vista ejecutable.

V. CONCLUSIONES

El futuro universo inteligente abre muchas posibilidades en los campos de la composición, provisión y consumo de servicios. Los usuarios demandan una plataforma en la que un usuario pueda componer y personalizar sus propios servicios a través de su teléfono móvil. Este trabajo ha presentado una arquitectura basada en componentes que puede ser utilizada en este tipo de entornos. Hemos revisado las ventajas de utilizar una arquitectura orientada a componentes en vez de una arquitectura típicamente SOA. Además de las cualidades de los componentes que son conocidas por todos, como la posibilidad de reutilización para distintos entornos, hemos detectado otras razones para utilizarlos que, en general, tienden a ser pasadas por alto:

La utilización de una arquitectura basada en componentes hace el proceso de creación más fácil, gracias a la utilización de herramientas de composición basadas en *workflow*.

Es posible proporcionar algunos mecanismos que ayuden al usuario en el proceso de composición como asistentes y patrones de composición que tienen impacto nulo sobre los niveles inferiores (motor de creación, generador de documentos SDL, conexiones con otros subsistemas, etc). Esta independencia está lograda gracias al desacoplo obtenido al utilizar una metodología de composición donde el elemento fundamental es el componente.

La lógica del servicio, esto es, el conjunto de relaciones entre componentes, está desacoplada de la implementación de cada componente, asociada a las capacidades que son asignadas a los componentes en tiempo de resolución. De esta forma, el principal objetivo del universo inteligente acerca de la posibilidad de interactuar con todos los elementos al alcance del usuario puede ser satisfecho si establecemos un mecanismo de armonización de capacidades, dependiente de las restricciones impuestas por los usuarios pero independiente del tipo de capacidad y de la tecnología utilizada para acceder a esta.

En este trabajo se presenta una propuesta de implementación y un activo experimental como validación de la arquitectura, que proponen soluciones a los problemas detectados, comúnmente encontrados en modelos orientados a componentes: interacción de subsistemas, gestión de componentes, formato de los datos intercambiados y bajo acoplamiento en el proceso de resolución. La arquitectura propuesta se ha validado mediante la implementación de una prueba de concepto de un sistema de creación y composición de servicios que define los mismos mediante la generación de un documento SDL, compatible con distintas reglas de ejecución.

Los siguientes pasos de este trabajo serán la implementación y el prototipado del sistema de provisión y consumo completo y la validación de esta plataforma en un contexto más amplio, describiendo más escenarios. Otra línea de trabajo que estamos llevando a cabo de forma paralela es el diseño de otros subsistemas para que pueda producirse una interacción del sistema global para uso público.

AGRADECIMIENTOS

Agradecemos al programa CENIT y a Telefónica I+D el tener la oportunidad de participar en el proyecto mIO!, que estudia, define y desarrolla tecnologías para prestar servicios en movilidad en el futuro universo inteligente. También estamos agradecidos a todos los miembros del proyecto T2C2, que contribuye al desarrollo de tecnologías que posibilitan la utilización de canales de comunicación donados por los ciudadanos en situación de emergencia.

REFERENCIAS

[1] Information Society Technologies Advisory Group: http://cordis.europa.eu/fp7/ict/istag/home_en.html
[2] Toffler, Alvin. (1980). The Third Wave.
[3] Cloutier, Jean. (1975). La communication audio-scripto-visuelle à l'ère des self-media, L'Ere d'Emerec. P.U.M, Montreal.
[4] Halteren, A.v. and Pawar P. (2006). Mobile Service Platform: A Middleware for Nomadic Mobile Service Provisioning. In: 2nd IEEE International Conference On Wireless and Mobile Computing, Networking and Communications (WiMob 2006), Montreal, Canada.
[5] Belevitch, V.: Summary of the history of circuit theory, In: Proceedings of the IRE, vol 50, Iss 5, pp848-855, May 1962.
[6] K. Czarnecki, U. Eisenecker, Components and Generative Programming. In: Proceedings of the Joint European Software Engineering Conference and ACM SIGSIFT International Symposium on the Foundations of Software Engineering (ESEC/FSE'99), Toulouse, France, 1999, pp.2-19
[7] H.Bruin, H. Vliet, The Future of Component-Based Development is Generation, net Retrieval, In: Proceedings of the 9th IEEE Conference and Workshops on Engineering of Computer-Based Systems, Lund University, Sweden, 2002, pp. 19-22
[8] Zewdie, B.; Carlson, C.R.; Adaptative Component Paradigm for Highly Configurable Business Components. In: 2006 IEEE International Conference on Electro/information Technology. 7-10 May 2006 Page(s): 185 – 190.
[9] Huang, Y., Jieying Li, Haiqiang Dun, Hanpin Wang. (2009). Analyzing Service Composition Patterns in BPEL Artificial Intelligence. In: JCAI '09. International Joint Conference on 25-26 April 2009 Page(s):623 – 627
[10] Yamato, Y., Nakano, Y., Sunaga, H. (2008). Study and Evaluation of Context-Aware Service Composition and Change-Over Using BPEL Engine and Semantic Web Techniques. In: Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE 10-12 Jan. 2008 Page(s):863 – 867
[11] Ma, Z., Leymann, F. (2009). BPEL Fragments for Modularized Reuse in Modeling BPEL Processes. Networking and Services. In: ICNS '09. Fifth International Conference on 20-25 April 2009 Page(s):63 - 68
[12] Web Ontology Language for Services (W3C Submission) http://www.w3.org/Submission/2004/07/
[13] Vaculin, R., Sycara, K. (2008). Semantic Web Services Monitoring: An OWL-S Based Approach. In: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual 7-10 Jan. 2008 Page(s):313 – 313.
[14] Extensible Markup Language (XML), W3C.org http://www.w3.org/XML/
[15] Romero, D. Parra, C., Seinturier, L., Duchien, L., Casallas, R. (2008) An SCA-Based Middleware Platform for Mobile Devices. In: Enterprise Distributed Object Computing Conference Workshops,12th 16-16 Sept. 2008 Page(s):393 – 396.
[16] OSGi Alliance, http://www.osgi.org/Main/HomePage
[17] Yin Qin, Hu Hao, Li Jim, Ge Jidong, Lu Jian. (2005). An approach to ensure service behavior consistency in OSGi. In: Software Engineering Conference, 2005. APSEC '05. 12th Asia-Pacific 15-17 Page(s):8
[18] Diaz Redondo, R.P., Vilas, A.F., Cabrer, M.R., Pazos Arias, J.J., Marta Rey Lopez. (2007). Enhancing Residential Gateways: OSGi Service Composition. In: Consumer Electronics, IEEE Transactions on Volume 53, Issue 1, February 2007 Page(s):87 – 95
[19] Cervantes, H, S. Hall, R. (2003). Automating Service Dependency Management in a Service-Oriented Component Model, In: Workshop on Component Based Software Engineering, May 2003.
[20] Bottaro, A., Gerodolle, A., Lalanda, P. (2007) Pervasive Service Composition in the Home Network. Advanced Information Networking and Applications. In: AINA '07. 21st International Conference on 21-23 May 2007 Page(s):596 – 603.
[21] Ben-Shaul, I., Gidron, Y., Holder, O. (1998). A negotiation model for dynamic composition of distributed applications. In: Database and Expert Systems Applications. Proceedings. Ninth International Workshop on 26-28 Aug. 1998 Page(s):820 – 825

Federación de Redes Personales en Escenarios Nómadas

Luis Sánchez, Jorge Lanza, Luis Muñoz
Departamento de Ingeniería de Comunicaciones
Universidad de Cantabria
Laboratorios de I+D de Telecomunicaciones. Plaza de la Ciencia s/n, 39005, Santander
{lsanchez, jlanza, jchoque, luis}@tlmat.unican.es

***Resumen*- Este artículo presenta la especificación de las soluciones y mecanismos que soportan la creación de una Federación entre Redes Personales situadas en el mismo lugar y que por tanto puedan establecer un enlace directo entre ellas. Las Redes Personales posibilitan que los dispositivos personales de un usuario sean capaces de organizarse de forma autónoma en una red privada y segura, independientemente de donde se encuentren o de la manera en la que acceden a la red. Sin embargo, para poder explotar realmente los beneficios de este concepto, es necesario complementarlo para que sea posible la interacción entre las Redes Personales de diferentes personas. Este concepto de colaboración entre varias Redes Personales recibe el nombre de Federación de Redes Personales. El establecimiento de estas federaciones se puede realizar en múltiples escenarios pero en este artículo nos centraremos en el caso en el que grupos de dispositivos personales de distintos usuarios se encuentren en el mismo lugar, de forma que puedan comunicarse entre ellos de igual a igual.**

***Palabras Clave*- Red Personal, Federación, Asociación segura, Heterogeneidad.**

I. INTRODUCCIÓN

Las comunicaciones personales han experimentado un extraordinario avance en los últimos años. Uno de los paradigmas que han aparecido es el de las Redes Personales (PN, *Personal Network*) [1]. Las PNs permiten al usuario interconectar de manera transparente todos sus dispositivos personales independientemente de cual sea su localización (Ej. a su alrededor, en casa, en el trabajo, etc.). Una PN es una red virtual en la cual los dispositivos de una persona que se encuentran en el mismo lugar se organizan en clusters, que a su vez se interconectan a través de Internet de forma que todos los dispositivos puedan interactuar.

Mientras que las Redes Personales se centran únicamente en la comunicación entre dispositivos personales, es común que la comunicación se extiendan más allá de los dispositivos que pertenezcan a una única persona y que sea necesario establecer una interacción segura entre diferentes personas que tienen intereses comunes. Por lo tanto, es necesario extender el concepto de PN para permitir la posibilidad de acceder a los servicios ofrecidos por los dispositivos de otros usuarios. El concepto de Federación de Redes Personales (PN-F, *Personal Network Federation*) presenta retos aún mayores, ya que las relaciones entre los usuarios tienen que ser gestionadas y soportadas de manera segura evitando que se abran agujeros en la seguridad de la PN a la vez que se permite que usuarios autorizados tengan un acceso controlado a los recursos ofertados por las PNs miembro.

Algunas de las soluciones actuales que pudieran proponerse como respuesta a estos retos como las redes privadas virtuales [2] o las aplicaciones *peer-to-peer* [3] sólo ofrecen soluciones parciales al no ofrecer una autoconfiguración real o seguridad extremo a extremo. Además, por lo general, no soportan el concepto de confianza grupal y la mayoría se centran únicamente en una aplicación *software* específica [4]. Como se describe en [5] y [6], la diversificación que existe hoy en día a nivel de plano de control, exige una configuración manual cuando se trata de la interacción entre redes. Este problema se acentuará en el futuro cuando existan redes con topologías aún más dinámicas y sea necesario integrar redes con tecnologías heterogéneas en un ecosistema más reactivo. Sin embargo, las soluciones que se han propuesto en estos casos se basan en consideraciones demasiado genéricas y se extienden a lo largo de una plétora de tipos de redes diferentes por lo que no ofrecen soluciones prácticas al paradigma de solución centrada en el usuario que se persigue cuando se habla de comunicaciones personales. En [7] se presenta el modelo de la P2P *Wireless Network Confederation* (P2PWNC) en el cual se ofrece acceso a Internet al resto de usuarios a través de un conjunto de dominios administrativos. Los autores pretenden reemplazar al administrador humano de los acuerdos de *roaming* por Agentes de Dominio de forma que se elimina la sobrecarga administrativa. Si bien esta iniciativa investiga varios aspectos críticos, no cumple en su totalidad con los requisitos de las futuras comunicaciones ubicuas ya que se centra demasiado en entornos específicos de redes ad-hoc móviles (MANET). En el ámbito exclusivamente de los servicios Web, en el consorcio OASIS a través de su comité de WSFED [14] se describen los mecanismos para habilitar la federación entre distintos proveedores de servicios Web mediante la gestión de la confianza entre las distintas entidades involucradas. Aún cuando desde esta plataforma se están definiendo los procedimientos para la gestión de las identidades y la confianza así como las estructuras de información para la definición de los servicios compartidos, se circunscribe únicamente a los servicios Web y no contempla los aspectos de conectividad y red que soporten la provisión de servicios. Por tanto, se hace necesario definir una solución integrada que soporte el concepto de Federación de Redes Personales.

El resto del artículo se organiza como se describe a continuación. En la Sección 2 se mostrará la arquitectura de referencia de una federación entre dos PNs. El ciclo de vida

de la PN-F, así como las principales entidades funcionales de la arquitectura serán descritos igualmente. Tal y como se ha mencionado, el soporte de la heterogeneidad y el mantenimiento de la seguridad son los principales retos en el establecimiento de federaciones en entornos nómadas. En la Sección 3 se presentarán las soluciones propuestas para dar respuesta a estos retos. Las Secciones 4 y 5 presentarán la especificación de los mecanismos para crear, formar y usar una PN-F sobre un escenario ad-hoc heterogéneo. Por último, en la Sección 6 se concluirá el artículo resaltando los principales aspectos del trabajo presentado.

II. ARQUITECTURA DE LAS PN-F

Una PN-F se puede definir como la interacción segura entre varias PNs que se organiza de manera automática. Su objetivo es el de permitir la provisión de servicios entre los propietarios de estas redes. Por ejemplo, en un entorno de colaboración profesional, una PN-F estaría formada por aquellos dispositivos de los distintos colegas que son relevantes para el desarrollo del proyecto común. Sólo aquellos recursos que sean necesarios para el proyecto (Ej. archivos, correos electrónicos, agendas, programas, etc.) serán puestos a disposición del resto de usuarios de la PN-F. El resto de recursos (Ej. archivos personales, parte privada de la agenda, etc.) no podrán ser accesibles para tus compañeros o sólo en el marco de otra PN-F que permita su acceso (Ej. familia, amigos, etc.). Por tanto, este concepto se basa fuertemente en el paradigma de confianza grupal. Técnicamente, se establece una red superpuesta que aísla un subconjunto de los recursos ofrecidos por los dispositivos que componen las PNs que forman parte de la PN-F.

Los requerimientos básicos que es necesario soportar por las PN-Fs son: que la comunicación sea segura, que la organización de la red sea automática y transparente para el usuario, que la red sólo este formada por dispositivos de las PNs que pertenecen a la PN-F y que sea posible restringir el acceso de forma que sólo sean accesibles los recursos que, por parte de cada PN, se ofrecen a la federación.

Las circunstancias en las que es posible establecer una federación son muy diversas y por ello se pueden hacer diferentes clasificaciones. Si se tiene en cuenta la duración, se puede pensar tanto en federaciones reducidas (en una conferencia) como muy extensas en el tiempo (en un proyecto); desde el punto de vista del modo de establecimiento, pueden ser reactivas (entre los miembros de un equipo de emergencia) o proactivas (en una familia); por último, atendiendo al entorno en el que se establece, podemos hablar de PN-F ad-hoc (en una sala de reuniones) o basada en infraestructura (PN-F para enseñanza remota). Mientras que las dos primeras categorías obedecen a consideraciones administrativas y de contexto, la última afecta en gran medida a como la PN-F se crea, forma y usa. En el caso de que haya soporte de la infraestructura, los mecanismos utilizados pueden recurrir a entidades remotas que los respalden. Sin embargo, en el caso ad-hoc, no se puede asumir el acceso a esas entidades remotas, sino que hay que afrontar todos los retos con los recursos disponibles localmente en los dispositivos personales que los usuarios de la PN-F tienen consigo. Además, en el caso ad-hoc es necesario tener en cuenta el nivel de conectividad antes de plantear nada más. Por ello, la heterogeneidad en términos de tecnologías de acceso ha de ser tenida en cuenta. Este artículo se concentrará en describir la arquitectura y las soluciones diseñadas para permitir la creación, formación y uso de PN-Fs en situaciones en las que no exista soporte de la infraestructura.

A. *Ciclo de vida de la PN-F*

Antes de continuar con la descripción de la arquitectura de referencia, a continuación se introducen las fases que se han identificado en el establecimiento de una PN-F.

Fase de Participación: El objetivo de esta fase es la toma de acuerdos entre el Creador de la PN-F (el usuario que decide la creación de la federación) y una PN candidata a ser miembro de la federación. La base de estos acuerdos es el intercambio seguro de los diferentes Perfiles en los que se detallan las características de la PN-F.

Fase de Formación: En esta fase se establecen los mecanismos para que cualquiera de las PNs Miembro pueda comunicarse con el resto. Los principales aspectos a resolver en esta fase son los relativos a direccionamiento, enrutamiento y seguridad.

Fase de Uso: Esta fase comprende tanto el descubrimiento como la provisión de servicios ofrecidos por las PNs Miembro. La seguridad ofrecida por las soluciones implementadas a nivel de red permite hacer uso de políticas de acceso a los recursos compartidos.

B. *Entidades funcionales de la PN-F*

La Fig. 1 muestra la arquitectura de referencia así como sus principales entidades funcionales y las relaciones que se establecen entre ellas. Estas entidades funcionales son:

- *Federation Manager* (FM): Es el responsable de gestionar las interacciones entre PNs durante la Fase de Participación. Principalmente se encarga de la gestión de los Perfiles de la PN-F.
- *Secure Context Management Framework* (SCMF) [8]: Se trata de una plataforma distribuida que facilita el acceso a la información de contexto de la PN. Una de sus responsabilidades es almacenar los perfiles de las PN-Fs en las que la PN está involucrada.
- *Service Management Platform* (SMP) [9]: Controla el descubrimiento y acceso a los servicios de la PN. El FM interactuará con ella para la creación del Perfil de Participación de la PN-F. El descubrimiento de servicios se centraliza en el *Service Management Node* (SMN) mientras que la provisión es completamente distribuida.
- *Policy Engine* (PE) [10]: Actúa como interprete y razonador de las reglas declaradas en los Perfiles PN-F para asegurar el mantenimiento del control de acceso.
- *Personal Network Directory Service* (PNDS) [11]: Asume el rol de tercera parte confiable. Puede utilizarse para verificar la identidad de otra PN en cualquiera de las fases de la PN-F así como para albergar los detalles públicos de las PNs y las PN-Fs.

III. SOLUCIONES PARA EL SOPORTE DE LA HETEROGENEIDAD Y EL MANTENIMIENTO DE LA SEGURIDAD

Hasta ahora se ha presentado una vista genérica de la arquitectura de referencia de las PN-F. En esta sección se presentarán la especificación de las soluciones implementadas para la creación, formación y uso de PN-Fs en escenarios ad-hoc.

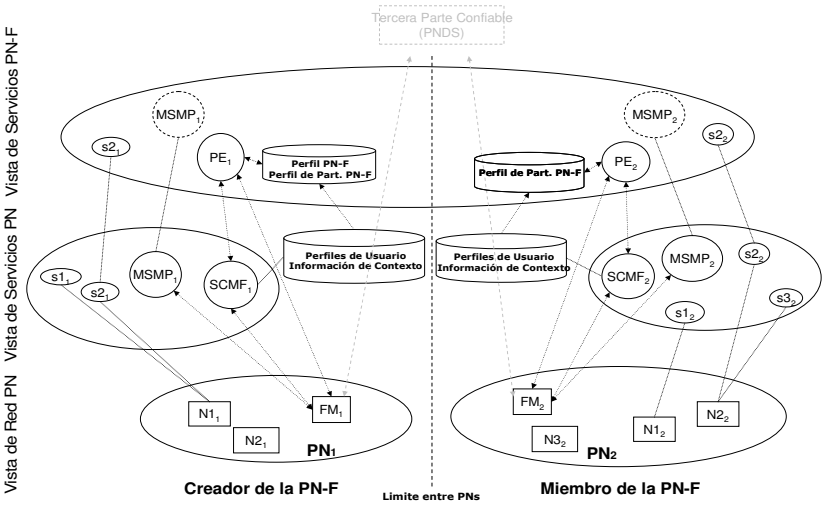


Fig. 1. Arquitectura de referencia de la PN-F

A. *Establecimiento de asociaciones seguras*

En [12] se describe el procedimiento por el cual se asegura la privacidad y la seguridad dentro de una PN. Este mecanismo, denominado *imprinting*, consiste básicamente en el establecimiento de una Asociación Segura entre dos dispositivos personales. Asumiendo que cualquier pareja de dispositivos personales está así asociado (esta asociación se materializa en claves privadas compartidas entre los nodos, establecidas bajo la supervisión del propietario de la PN), la autenticidad, privacidad y la seguridad en general queda asegurada siempre que dos nodos personales quieran comunicarse.

Siguiendo un razonamiento similar, será posible garantizar la seguridad de las comunicaciones entre dos dispositivos que pertenezcan a PNs diferentes si se puede establecer una Asociación Segura, similar a la que se establecía entre nodos de la PN, entre ambas PNs. La clave privada en este caso se empleará para proteger cualquier comunicación en la que intervenga un nodo de cada PN. El resultado de la Asociación Segura es una clave secreta PMK_{A-B} (válida únicamente para las comunicaciones con la otra PN) que ambas PNs almacenarán y asociarán al identificador de la PN correspondiente.

El empleo de estas claves asegura la autenticidad de aquellos nodos que las empleen en los protocolos de autenticación (sólo los nodos de las PNs involucradas en la asociación conocerán PMK_{A-B}) y la privacidad de las comunicaciones estará garantizada al poder cifrar los paquetes intercambiados con claves de sesión derivadas de la clave secreta. La autorización para el acceso a los servicios y recursos podrá basarse en esta base de autenticación segura.

B. *Descubrimiento y autenticación de vecinos*

En el caso ad-hoc, la formación de la PN-F comienza por el descubrimiento y autenticación de los nodos de alguna PN con la que se tenga una Asociación Segura con los que exista la posibilidad de comunicarse directamente. Para ser consciente en todo momento de los nodos vecinos se implementa un proceso de sondeo. Con ello descubriremos tanto los nodos personales (de la propia PN) como los foráneos (de otras PNs). Este proceso consiste en que periódicamente cada nodo enviará un paquete de sondeo de manera que cualquier nodo en su rango de cobertura lo pueda escuchar. De esta manera cada nodo advertirá al resto, tanto de su propia PN como de otras, de su presencia. Este paquete será enviado a través de todas las tecnologías de acceso con las que esté equipado el dispositivo en cuestión. En el caso de recibir uno de estos paquetes de un nodo que pertenezca a otra PN, se devolverá un reconocimiento explicito y se informará al FM propio sobre la presencia de la nueva PN.

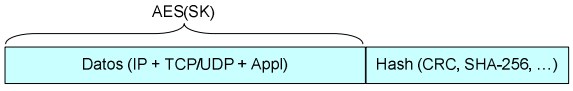


Fig. 2. Formato de la PDU de datos UCL

En el caso de que ya exista una Asociación Segura con la PN a la que pertenece ese nodo, será posible intercambiar una clave de sesión derivada a partir de la PMK_{A-B} y que se empleará para cifrar en los paquetes intercambiados entre esos dos dispositivos.

C. *Soporte de la heterogeneidad y aplicación de las asociaciones seguras*

Poder operar en entornos heterogéneos es fundamental para proveer comunicaciones inter-personales. Esta heterogeneidad se verá reflejada fundamentalmente en el número de tecnologías de acceso diferentes que coexistirán en estos escenarios.

El concepto de aislar las capas superiores de la pila de protocolos de las tecnologías de acceso subyacentes de forma que se ofrezca una capacidad multimodo real se consigue a través de la *Universal Convergence Layer* (UCL) [13]. La UCL actuará principalmente como un habilitador de compatibilidad, tanto hacia delante como hacia atrás, que define un interfaz común único hacia la capa de red a la vez que gestiona varias tecnologías de acceso distintas. En este sentido, la solución adoptada hace posible que los dispositivos personales tengan una única dirección de red independientemente del número de interfaces de acceso que posean. De este modo el protocolo de enrutamiento de capa 3 podrá definir rutas que contengan dominios de acceso diferentes de una manera completamente transparente. La combinación de la UCL con un protocolo de enrutamiento ad-hoc permite hacer una gestión de la heterogeneidad que

aparecerá en los escenarios de establecimiento de PN-Fs en entornos ad-hoc. En este sentido, el protocolo de enrutamiento ad-hoc implementará sus algoritmos de encaminamiento sin importarle sobre que tecnología de acceso se implementan cada uno de los enlaces de la red.

Desde el punto de vista de al seguridad, la UCL también aporta los mecanismos que permiten asegurar la privacidad y autenticidad de las comunicaciones independientemente de cual sea el nivel de seguridad que ofrezca por defecto cada una de las tecnologías de acceso empleadas. La UCL implementa mecanismos de criptografía que usan claves de sesión derivadas de la K_{PN} intercambiada entre ambas PNs.

Tal y como se muestra en la Fig. 2 a cada paquete de datos se le añade una firma para asegurar la integridad y se cifra usando claves de sesión derivadas a partir de la clave secreta compartida por ambas PNs.

IV. FASE DE PARTICIPACIÓN DE LA PN-F

La fase de formación de la PN-F comprende los procedimientos por los cuales se intercambia de manera segura la información que es necesaria para unirse a la federación. En esta fase intervienen el Creador de la PN-F y otra PN que quiera entrar a formar parte de la PN-F.

El Creador de la PN-F generará un Perfil de PN-F en el momento en el que crea la PN-F. Este Perfil de PN-F definirá la identidad de la PN-F y las políticas y reglas que regirán la federación. La información mínima que contendrá el Perfil de PN-F (**PN-F Profile$_{PUBLIC}$**) será:

- PN-F /ID: Un identificador único de la federación.
- El objetivo de la PN-F.
- Condiciones de inicio y reglas de activación y cierre.
- Punto de Contacto (PoC) del Creador: El PN ID del creador así como la dirección del FM.

De manera opcional, el creador puede hacer pública información como:

- Las reglas de participación (Ej. quién más está o puede estar invitado.
- Lista mínima de recursos que deben ser compartidos.

La fase de participación se inicia cuando el Creador de la PN-F hace pública esta información de la federación mediante algún método de difusión. Por ejemplo, una invitación enviada *off-line,* un mensaje destinado a PNs que estén en las inmediaciones o publicándolo en un servidor al que otras PNs tengan acceso.

El siguiente paso será establecer la asociación segura entre la PN del Creador y la PN del candidato que desea entrar a formar parte de la PN-F.

Para iniciar su adhesión a la federación, el candidato editará su Perfil de Participación en la PN-F. Es importante destacar que mientras que el Perfil de la PN-F es común para toda la federación, cada miembro de ésta tendrá su propio Perfil de Participación de la PN-F. Éste consiste básicamente en los recursos que se ponen a disposición de esa federación.

Una vez completado el Perfil de Participación, se lo mandará al Creador. El Creador comprobará si el Candidato cumple las condiciones especificadas en las políticas de la federación y si es así le enviará la parte privada del Perfil de la PN-F (**PN-F Profile$_{PRIVATE}$**). Esta parte privada sólo es conocida por los miembros de la federación y contiene la siguiente información:

- Clave de difusión de la federación: Clave que se usará para proteger las comunicaciones punto-multipunto dentro de la federación.
- Lista de miembros de la federación.
- Lista de servicios disponibles en la federación.

A. *Publicación y Descubrimiento*

Como se ha descrito, el primer paso en la fase de participación es la Publicación y el Descubrimiento de las federaciones. En el caso de que no exista soporte por parte de la infraestructura, es necesario especificar las diferentes formas en las que se puede completar este paso.

En la 0 se muestra la publicación y el descubrimiento de PN-Fs en escenarios donde no existe infraestructura.

En este caso la dirección del PoC contenida en el Perfil de la PN-F no será usable al pertenecer en general a una dirección del FM direccionable globalmente. En un escenario en el cual el acceso a Internet no es posible, esta dirección no tiene utilidad. Por tanto, cuando el FM del candidato recibe la primitiva *PNF_ADVERTISED*, detecta que se trata de un escenario ad-hoc y enviará la primitiva *INIT_JOIN* al nodo que hace de pasarela (GW) de la PN que originó el anuncio.

La primitiva *INIT_JOIN* contiene la siguiente información:

- PN_ID$_X$: El identificador de la PN del Creador de la PN-F para que el GW sepa a quien dirigir los mensajes.
- PN-F_ID: El identificador de la federación al que el usuario se quiere unir.

Esta información se utilizará durante el siguiente paso de la fase de participación, la Autenticación y Establecimiento de Asociación Segura.

B. *Autenticación y Establecimiento de Asociación Segura*

Hasta este punto de la fase de participación, la información intercambiada entre ambas PNs no ofrece ninguna garantía ni en cuanto a su autenticidad ni en lo referente a su privacidad.

Para poder continuar con la fase de participación, es necesario que tanto Creador como Candidato establezcan una relación de confianza mutua a través de una asociación segura entre ambos. Una vez establecida esta asociación (e intercambiadas las claves privadas que resultan de ella), el resto de los pasos pueden realizarse de manera segura.

Como se introdujo en la Sección 3.A., se han identificado dos métodos para hacer el *imprinting* entre dos PNs. El primero se basa en una Infraestructura de Clave Pública (PKI) en la cual una Autoridad de Certificación expide certificados para poder verificar la identidad de las PNs y establecer las Asociaciones Seguras a partir de ellos. El segundo método se propone para los casos en los que no se quiere (o puede) depender de una infraestructura. En esta sección nos centraremos en la descripción del primer caso.

Es importante destacar que este proceso sólo es necesario para la primera vez que dos PNs interactúan. Cualquier interacción posterior estará protegida por la Asociación Segura que se establezca la primera vez. Estas Asociaciones Seguras tienen la característica de perdurar en el tiempo hasta que el usuario decida romperla.

La información contenida en las primitivas *REQ_AUTH* y *AUTH_GRANTED* mostradas en la B. son:

- El certificado de la PN a la que pertenece el emisor.

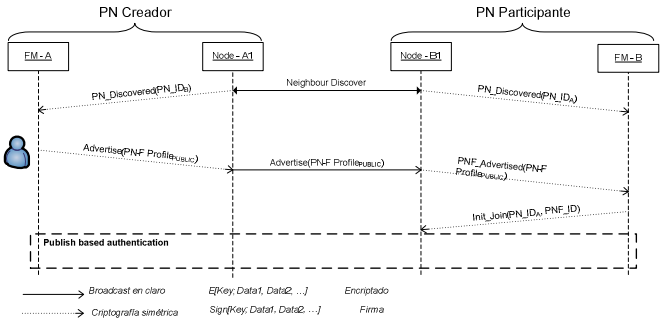


Fig. 3. Publicación y Descubrimiento en escenarios ad-hoc

- La firma del identificador de la federación por la cual se está iniciando el proceso de Asociación Segura. Usando la clave privada correspondiente al certificado incluido en la propia primitiva es posible verificar la autenticidad de la información contenida.

Una vez que se han recibido estas dos primitivas, ambas PNs habrán podido autenticarse mutuamente. Usando la clave pública de ambas PNs (PK_X)se emplea un protocolo de tipo Diffie-Hellman para generar la clave compartida (PMK_{A-B})que sustentará la Asociación Segura entre ambas PN.

C. Unión a la federación

Una vez llegado a este punto en la Fase de Participación, ambas PNs están autenticadas mutuamente y comparten una clave que podrán usar para proteger las comunicaciones entre ellas de forma que sean privadas y permitan autenticar al origen. Sin embargo, el Candidato aún no es Miembro de la federación puesto que no ha enviado su Perfil de Participación al Creador y por lo tanto este no ha autorizado aún su acceso a la PN-F.

El último paso de la Fase de Participación es precisamente el de la adhesión efectiva del nuevo miembro. El Candidato tendrá que generar su Perfil de Participación y enviarlo en una primitiva *JOIN* al Creador.

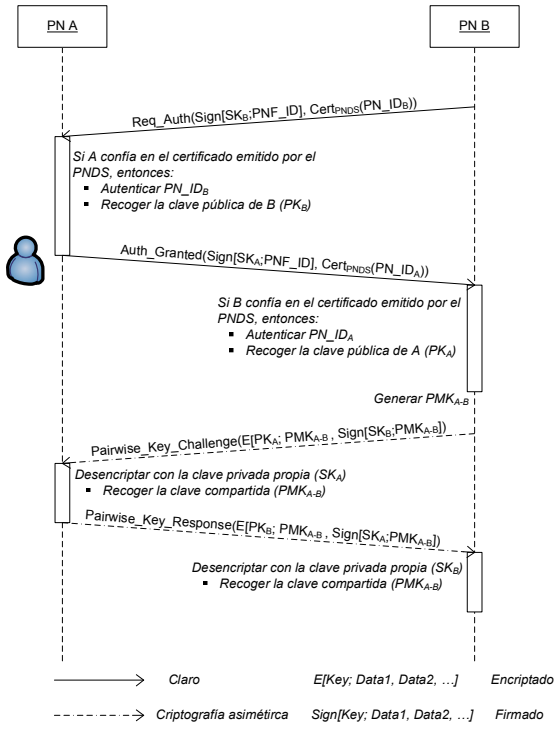


Fig. 4. Asociación segura basada en certificados

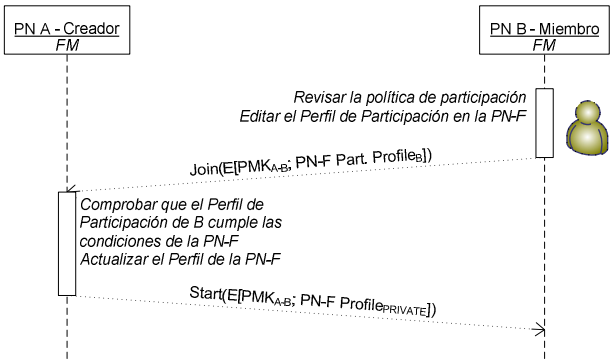


Fig. 5. Mecanismo de unión a la federación

La IV muestra las primitivas que se intercambian en este paso de la Fase de Participación. La información básica que contiene el Perfil de Participación es la siguiente:

- Identificador de la PN-F a la que se corresponde el Perfil de Participación
- Un PoC de la PN que contiene tanto el identificador de la PN como la dirección a la que dirigir futuras peticiones de negociación relativas a la PN-F.
- Los recursos y servicios que se ponen a disposición de la federación por parte de la PN de ese usuario.
- Opcionalmente se pueden incluir reglas y políticas de acceso a dichos recursos.

La definición de los recursos y servicios a compartir y el modo en que se protege su uso, dependerá de la arquitectura propia de dichos servicios y va más allá del alcance de este artículo. En cualquier caso, los perfiles pueden soportar distintas formas de definición.

Una vez que el Creador recibe el mensaje de *JOIN*, comprobará que el Candidato cumple con las reglas establecidas en el Perfil de la PN-F y si es así actualizará la parte privada del Perfil de la PN-F (básicamente añadirá al nuevo miembro a la lista de PNs que forman la federación). En general, si se cumplen las condiciones por parte del Candidato, la respuesta al mensaje de *JOIN* es el mensaje de *START*. No obstante, el envío de este mensaje puede no ser inmediato ya que el inicio de la federación depende, como se ha descrito anteriormente, de unas reglas generales. Por ello, si por ejemplo la federación sólo se iniciará en unas determinadas circunstancias (Ej. fecha y hora concretas), es posible que el envío de la primitiva *START* no se haga hasta que éstas se cumplan. Otra opción posible es que sí se envíe el mensaje de *START*, y sean cada una de las PNs miembro de la federación las que se responsabilicen de hacer cumplir las reglas de inicialización.

V. FASES DE FORMACIÓN Y USO DE LA PN-F

Una vez que la nueva PN ha entrado a formar parte de la PN-F, se puede proceder al establecimiento de los mecanismos de interacción con el resto de miembros de la federación (hasta el momento la interacción se circunscribía únicamente a intercambios con el Creador de la PN-F). Para permitir la comunicación entre nodos pertenecientes a diferentes PNs, durante la Fase de Formación se establece una red superpuesta que incluye a todos los nodos de las PNs que son miembro de la PN-F.

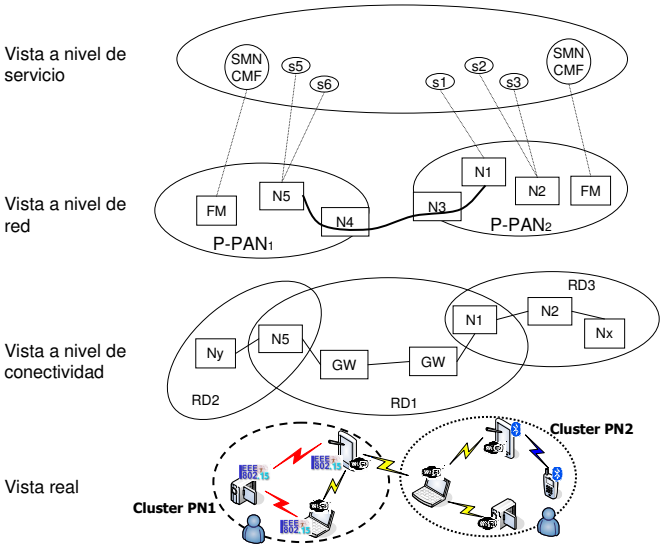


Fig. 6. Vista abstracta de un escenario de PN-F ad-hoc

A. *Descripción del escenario*

La Fig. 6 presenta la vista genérica de un escenario sobre el cual pudiera operar cualquier PN-F ad-hoc. Como se puede ver, clusters de nodos de distintas PNs se comunican entre ellos directamente de manera segura sin necesidad de ayudarse de ninguna entidad externa localizada en la infraestructura. Además, distintas tecnologías de acceso podrán coexistir, por lo tanto existirán a nivel de conectividad diferentes dominios de acceso que pueden forzar a que las comunicaciones consten de múltiples saltos.

B. *Direccionamiento en la PN-F*

Para establecer la red superpuesta a la que nos referíamos con anterioridad, se define un espacio de direccionamiento privado para la PN-F (los detalles de este espacio de direcciones se incluyen en el **PN-F Profile$_{PRIVATE}$**). Cada dispositivo tendrá una dirección IP perteneciente a este espacio de direcciones y cuando quiera comunicarse dentro de la federación utilizará estas direcciones. Este espacio de direcciones es distinto al direccionamiento público de las redes de acceso, al direccionamiento usado para las comunicaciones dentro de la PN y a cualquier otro direccionamiento perteneciente a otra PN-F.

Tanto para el caso de las PNs como las PN-Fs, el direccionamiento en las distintas redes superpuestas se basa en direcciones IPv6 de tipo *site-local* en las que se reservan 40 bits que se dedican a un prefijo que es distinto para cada red superpuesta (uno para la PN y otro para cada PN-F a la que se pertenezca). Esto permite que las comunicaciones en todos estos dominios (público, PN o distintas PN-F) estén aisladas unas de otras a nivel de red.

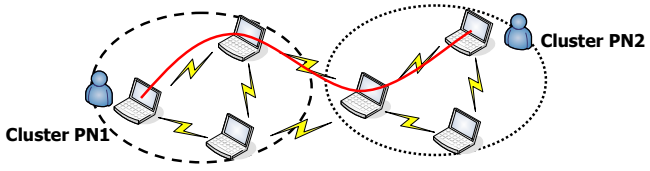


Fig. 7. Establecimiento de red entre nodos de distintos clusters

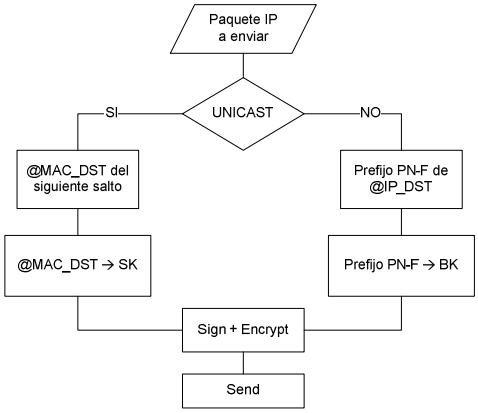


Fig. 8. Proceso de transmisión en la UCL

Tal y como se verá en la Sección 4.C.3, las comprobaciones de seguridad implementadas en la UCL, aseguran que sólo aquellos nodos que pertenezcan a una PN que es miembro de una PN-F, puedan utilizar las direcciones IP de dicha federación. Si cualquier dispositivo no perteneciente a una PN-F tratase de usar ese espacio de direccionamiento, los paquetes serían descartados a nivel UCL. De este modo, todas las comunicaciones en la red superpuesta asociada a la PN-F estarán confinadas únicamente a los miembros de la federación.

C. *Establecimiento de la red superpuesta*

En el escenario ad-hoc, el uso de redes superpuestas hace que la Fase de Formación de la PN-F tenga lugar tanto a nivel de red como a nivel de conectividad.

Los principales requisitos que es necesario soportar son:

- Auto-configuración (o mínima intervención por parte del usuario si así se define en las políticas de la PN-F).
- Independencia de terceras partes que no pertenezcan a alguno de los clusters de nodos personales involucrados.
- Establecimiento de una red superpuesta segura.
- Soporte para la creación espontánea de federaciones.

El primer paso en la formación de la PN-F es el establecimiento de un nivel de conectividad seguro entre los nodos de las distintas PNs que forman la federación. En la Sección 3.B. se describió la forma en la que los dispositivos reconocen a los nodos que tienen a su alrededor.

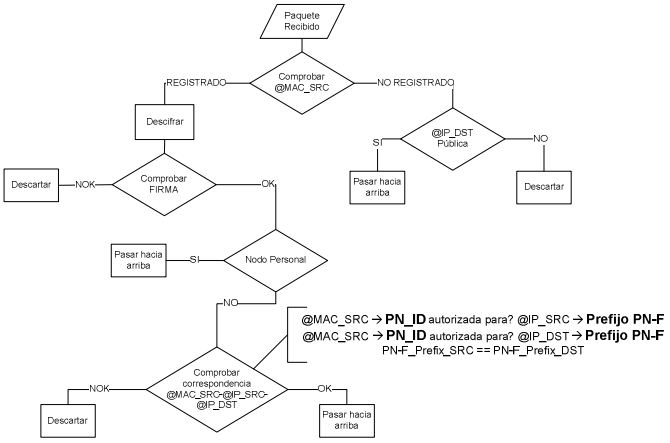


Fig. 9. Proceso de recepción en la UCL

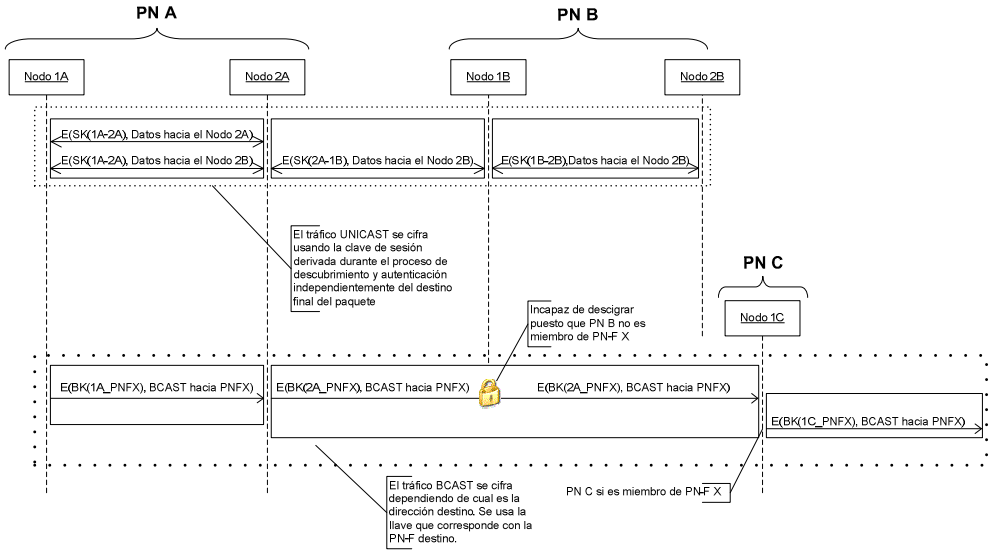


Fig. 10. Detalle del cifrado en las comunicaciones

Una vez autenticados, la información relativa a la presencia de nodos pertenecientes a otras PNs con las que se comparte federación se pasa a los protocolos de encaminamiento que son los únicos responsables del establecimiento de las rutas para la comunicación dentro de la PN-F tal y como se presenta en la Fig. 7.

D. Uso de la PN-F

La Fase de Uso de la PN-F comienza en cuanto uno de los nodos de alguno de los usuarios miembros de la federación hace una petición de un servicio ofrecido por alguno de los nodos de los otros clusters. En esta fase se realiza tanto el descubrimiento de servicios como su provisión.

La Fig. 8 muestra el modo en el que la UCL selecciona la clave que es necesario emplear para proteger cada uno de los paquetes transmitidos. Cuando un paquete IP va a ser transmitido se buscará la clave se sesión de nivel de enlace resultado de la Asociación Segura que se comparte con el nodo que es el siguiente en la ruta hacia el destino final. Si los nodos son personales, esta Asociación Segura es la que tienen por pertenecer a la misma PN, y si pertenecen a PNs distintas, esta Asociación Segura será la que establecieron en su momento la PN tal como se describió en la Sección 3.B.2.

Igualmente, cuando un paquete es recibido, se verifica la información en él contenida para evitar cualquier tipo de ataque por suplantación a la vez que se asegura que sólo los miembros de la PN-F puedan inyectar tráfico en la red superpuesta asociada. En la Fig. 9 se muestra como en los bordes de los clusters se consigue que sólo si la PN que me envía ese paquete pertenece a la federación, se dejará pasar un paquete cuya dirección IP destino pertenezca al espacio de direccionamiento reservado para dicha PN-F.

Así se garantiza que cualquier paquete que llega a las capas superiores esté autorizado para hacerlo. Asumiendo esto, los mecanismos de control de acceso de estas capas, pueden confiar en las direcciones de estos paquetes para permitir o no el acceso según lo indiquen sus propias políticas. En la 0 se detalla la forma en la que van cifrados los paquetes de datos en una comunicación, tanto punto-a-punto (*unicast*) como punto-multipunto (*broadcast*), dentro de la PN-F.

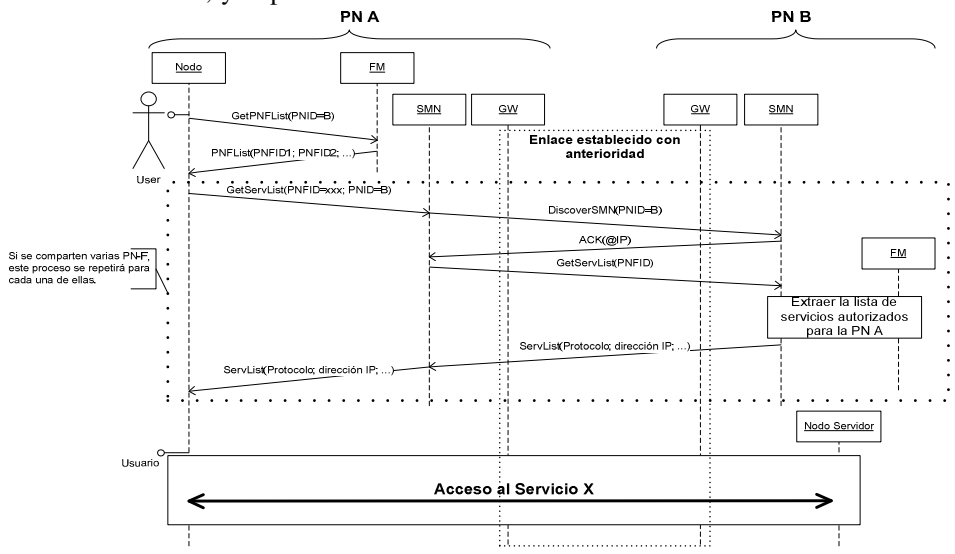


Fig. 11. Descubrimiento y acceso a servicios de una PN-F en un escenario ad-hoc

Por otro lado, es importante mencionar la diferencia de tratamiento del tráfico *unicast* del tráfico *broadcast*. En el primero de los casos, la clave de sesión no depende del destino final del paquete (bien sea en la PN o en alguna PN-F) sino del nodo a quien va dirigida la trama a nivel de enlace. De este modo, en una comunicación multisalto, en cada uno de los saltos se emplea una clave de sesión diferente, pues cada pareja de nodos comparte una clave distinta. En el caso de las comunicaciones *broadcast*, cada nodo empleará una clave propia que si que depende en este caso del destino final. Si los destinatarios son los miembros de una PN-F, la clave a utilizar es distinta a si el paquete sólo deben recibirlo los nodos personales que se encuentren en las proximidades. En cualquier caso como se muestra en la 0 sólo el nodo (o nodos) a los que va destinada la trama podrán descifrar el paquete recibido.

Finalmente, en la Fig. 10 se muestra como se lleva a cabo el proceso de descubrimiento de servicios en la PN-F y su posterior provisión. Cuando el usuario quiere saber que servicios están disponibles dentro de la PN-F, hará una petición al SMN de su cluster. Las peticiones pueden buscar en general todos los servicios disponibles (representado en la Fig. 1) o concentrarse en un servicio con características específicas. Los SMN de los distintos clusters involucrados en la federación se coordinarán para resolver esta petición. Los distintos SMN de los diferentes clusters serán los encargados de responder a la petición únicamente con los servicios que están compartidos en esa PN-F (información recogida en el Perfil de Participación de la PN-F). Cualquier otro servicio no compartido en la federación se mantendrá oculto a las otras PN.

Tras la fase de descubrimiento, el nodo que inició la petición podrá comunicarse directamente con el nodo(s) que ofrezcan el servicio. Los mecanismos de autorización utilizados durante el descubrimiento, no son óbice para implementar otros métodos de control de acceso durante la provisión del servicio.

VI. Conclusiones

En este artículo se ha presentado una especificación detallada de los mecanismos que permiten la creación, formación y uso de Federaciones de Redes Personales en entornos nómadas heterogéneos.

Los principales requisitos en términos de seguridad y autoconfiguración impuestos por el concepto de federación se han descrito teniendo en cuenta el escenario tipo identificado para la formación y uso de PN-Fs. A partir de la identificación de estos requisitos, se han definido los procedimientos correspondientes que soportan las funcionalidades necesarias. En este sentido, se ha descrito como se lleva a cabo el proceso de autenticación mutua y establecimiento de una Asociación Segura entre PNs, y como a partir de ésta, se provee seguridad a nivel de conectividad y se despliega una red superpuesta segura que permite un manejo sencillo del control de acceso a nivel de servicio.

Las características de autoconfiguración y escalabilidad de la solución de red propuesta se heredan de los protocolos de encaminamiento MANET que se utilizan para el establecimiento de rutas entre cualesquiera dos nodos de la PN-F.

Además, se ha implementado un mecanismo para soporte de la convergencia entre diferentes tecnologías de acceso que permite abstraerse de la heterogeneidad en dispositivos multi-interfaz de forma que la red superpuesta pueda establecerse de manera transparente independientemente de cuales sean las tecnologías de enlace que subyacen en la red.

Esta especificación es la base de una implementación que ha llevando acabo sobre dispositivos y redes reales que ha permitido realizar pruebas de concepto que despierten el interés de otros actores de la cadena de valor y ayudará a identificar posibles mejoras.

Agradecimientos

Los autores desean expresar su agradecimiento a todos los socios del proyecto MAGNET Beyond (IST-027396), y especialmente a los del WP2 por su colaboración. Asimismo, los autores desean expresar su agradecimiento al Ministerio de Ciencia e Innovación, por su financiación en el proyecto "Comunicaciones Cognitivas, Cooperativas y Gestión Autónoma de Servicios", C3SEM (TEC2009-14598-C02-01)

Referencias

[1] I.G. Niemegeers and S. Heemstra de Groot, “From Personal Area Networks to Personal Networks: A user oriented approach”, Journal on Wireless and Personal Communications 22 (2002), 175-186.

[2] Charles Scott , Paul Wolfe , Mike Erwin, “Virtual private networks”, O'Reilly & Associates, Inc., Sebastopol, CA, 1998

[3] Sun Microsystems, “JXTATM Technology: Creating Connected Communities”, January 2004

[4] J. Hoebeke, G. Holderbeke, I. Moerman, Bart Dhoedt, P. Demeester “Virtual Private Ad Hoc Networking”, Wireless Personal Communications, Volume 38, Issue 1, June 2006, pp. 125-141

[5] C. Kappler, P. Mendes, C. Prehofer, P. Pöyhönen and D. Zhou, “A Framework for Self-organized Network Composition”, WAC 2004 (IFIP Workshop on Autonomic Communication), Berlin, Germany, October 2004.

[6] L. Fan, N. Akhtar, K. A. Chew, K. Moessner and R. Tafazolli, “Network Composition: A Step towards Pervasive Computing”, 3G 2004, London, UK, October 2004.

[7] Elias C. Efstathiou, George C. Polyzos: “A peer-to-peer approach to wireless LAN roaming”, Proc. 1st ACM Int. workshop on Wireless mobile applications and services on WLAN hotspots, San Diego, CA, 2003.

[8] L. Sanchez, J. Lanza, M. Bauer, R. Olsen, M. Girod-Genet, “A Generic Context Management Framework for Personal Networking Environments”, Proceedings from 1st Workshop on Personalized Networks, San Jose (CA), July 2006

[9] M. Ghader, R. L. Olsen, V. Prasad, M. Jacobsson, L. Sanchez, J. Lanza, W. Louati, M. Girod Genet, D. Zeghlache, R. Tafazolli "Service Discovery in Personal Networks; design, implementation and analysis", 15th IST Mobile & Wireless Summit Communications Summit, Mykonos, June 2006

[10] J. Zeiss, L. Sanchez, S. Bessler, “Policy driven formation of federations between personal networks”, 16th IST Mobile & Wireless Summit Communications Summit, Budapest, July 2007

[11] M. Alutoin, S. Lehtonen, K.Ahola, J. Paananen, “Personal Network Directory Service”, Telektronikk Journal, Vol. 103 No. 1, 2007.

[12] IST-507102 MAGNET/WP4.3/UNIS/D4.3.2/R/PU/002/1.0, “Final version of the Network-Level Security”, March 3, 2005.

[13] L. Sanchez, J. Lanza, L. Muñoz, J. Perez Vila, “Enabling Secure Communications over Heterogeneous Air Interfaces: Building Private Personal Area Networks”, 8th International Symposium on Wireless Personal Multimedia Communications - Aalborg, September 2005.

[14] OASIS Web Services Federation (WSFED) Technical Committee, http://www.oasis-open.org/committees/wsfed/charter.php

Un modelo de datos semántico para catálogos activos de empresas de telecomunicación

Adolfo Ruiz Calleja[1], Guillermo Vega Gorgojo[1], Sergio García Gómez[2],
Miguel L. Bote Lorenzo[1], Juan I. Asensio Pérez[1], Eduardo Gómez Sánchez[1]
[1]Escuela de Telecomunicaciones, Universidad de Valladolid
Paseo Belén 15, 47011 Valladolid, Spain
[2]Telefónica I+D, Boecillo, Valladolid, Spain
adolfo@gsic.uva.es, guiveg@tel.uva.es, sergg@tid.es,
migbot@tel.uva.es, juaase@tel.uva.es, edugom@tel.uva.es
http://gsic.tel.uva.es

***Resumen*—Hoy en día el mercado de las telecomunicaciones está cambiando y la capacidad de proporcionar servicios al usuario final de forma rápida es cada vez más importante. En este escenario, la extensibilidad de los Sistemas de Soporte a Operaciones cobra vital importancia. Para mejorar dicha característica se ha propuesto un nuevo componente, llamado catálogo, cuyo objetivo es identificar y relacionar todas las entidades que maneja el sistema. En el presente artículo, se discuten los beneficios de implementar dichos catálogos utilizando tecnologías semánticas y se propone un modelo de datos para la base de conocimiento del catálogo. La bondad de la propuesta se ilustra por medio de un ejemplo concreto para una empresa de telecomunicación, siendo sus principales beneficios la flexibilidad y extensibilidad de la conceptualización, así como la posibilidad de compartir el catálogo entre diferentes organizaciones.**

***Palabras Clave*—Catálogo, Sistema de Soporte a Operaciones, tecnologías semánticas, ontología.**

I. Introducción

Los Sistemas de Soporte a Operaciones (OSS *Operation Support Systems*) [25] actuales no son lo suficientemente flexibles, lo que provoca que la introducción y modificación de nuevos productos y servicios sea una tarea compleja que requiere mucho tiempo y esfuerzo. Esta limitación se debe fundamentalmente a que el conocimiento sobre la generación de servicios y productos está disperso en los diferentes componentes que forman el OSS. Por esta razón, se ha propuesto la creación de un nuevo componente del OSS, llamado catálogo [17], [24], con la finalidad de recoger dicho conocimiento, eliminándolo del resto de sistemas del OSS y así reducir la complejidad de los datos, lo que redunda en un OSS capaz evolucionar más fácilmente. De hecho, el TeleManagement Forum (TMF) ha lanzado recientemente la Iniciativa de Reunión de Productos y Servicios (PSA, *Product and Service Assembly initiative*) [24], una arquitectura para catálogos que contiene información sobre las entidades del sistema, junto con instrucciones para manejarlas de forma automática. Este tipo de catálogos se denominan "catálogos activos", indicando que soportan las operaciones de crear, leer, actualizar y borrar información, así como otras relacionadas con la gestión de servicios, como la reserva de recursos o la coordinación de eventos [24].

Sin embargo, PSA sólo define una arquitectura de modelo de información y un conjunto de interfaces para el catálogo. Por ello, no es trivial producir datos que puedan ser utilizados a partir de las especificaciones de PSA. De hecho, sólo unos pocos catálogos están disponibles actualmente [5], [26]. Dichos catálogos se centran en proporcionar un vocabulario comprensible, haciendo explícita la relación entre los productos y los servicios que se encuentran en el sistema. De esta forma, toda la información relacionada con la agregación de servicios para generar productos es recogida en un solo componente, teniendo un único punto de control para la gestión de los productos y servicios de la empresa. Dicha información puede ser utilizada, por ejemplo, por el personal de *márketing* para especificar los servicios que se incluyen en cada producto. No obstante, no hay ningún catálogo que considere las relaciones entre los servicios proporcionados a los usuarios y los recursos involucrados en ellos. Tal catálogo podría abarcar otras aplicaciones; por ejemplo, sería posible relacionar los productos comprados por un usuario con los servicios a él proporcionados y con las configuraciones necesarias en los recursos involucrados. Este problema ha sido detectado por los autores cuando se analizaron diversos OSS y se entrevistó a expertos en el dominio, y también ha sido percibido por las patentes [11], [27]. Sin embargo, las soluciones que dichas patentes proponen son sistemas y métodos para la configuración de un grupo de recursos que proveen un servicio, no siguiendo para ello ningún estándar. Además, los autores no tienen constancia de ninguna implementación de dichos sistemas.

Uno de los mayores problemas al diseñar un catálogo para un OSS que incluya productos, servicios y recursos es que los recursos son muy específicos para cada red. Esto hace difícil definir un catálogo que pueda ser reutilizado entre diferentes empresas. Sin embargo, sería interesante la creación de un catálogo de propósito general que pueda ser adaptado a diferentes OSS, de forma que se reduzca el tiempo y el esfuerzo de crear y evolucionar un catálogo. Además, como cierta información puede ser reutilizada, sería posible estandarizar los catálogos de la industria de las telecomunicaciones y federar los catálogos de diferentes compañías, lo cual es uno de los objetivos de PSA [24]. Es evidente que estos objetivos imponen flexibilidad en la base de conocimiento del catálogo, ya que debe ser capaz de adaptarse rápidamente a ambientes heterogéneos y en constante evolución, como un OSS de una Red de Próxima Generación (NGN, *Next Generation Network*) [9]. Las soluciones clásicas, como las

bases de datos relacionales, no proporcionan la flexibilidad requerida. Por ello, el presente artículo propone el uso de tecnologías semánticas para abordar dicho problema, puesto que permiten definir ciertas reglas entre la funcionalidad de los recursos y las características de los servicios y los productos. Así, la flexibilidad del catálogo debería incrementar, puesto que la relación entre los elementos del OSS existe en un metanivel, por lo que elementos semánticamente semejantes pero estructuralmente diferentes, pueden ser transformados automáticamente [20].

Como un primer paso en el desarrollo de un catálogo activo semántico, el presente artículo propone una conceptualización para su base de conocimiento, acorde con los estándares de TMF, y su implementación en una ontología. Un punto importante en dicha conceptualización es la consideración de niveles de abstracción diferentes, definiendo una conceptualización de alto nivel que podría ser compartida entre diferentes empresas y extendida por cada una de ellas para su contexto específico. Así, es posible desarrollar un catálogo compartido, permitiendo el intercambio de información entre diferentes organizaciones, facilitando la cooperación entre diferentes empresas para añadir valor al producto final, que es una de las características más importantes de las redes NGN [9]. Adicionalmente, las tecnologías semánticas proporcionan la extensibilidad necesaria para poder compartir el catálogo.

El resto del artículo se estructura como sigue: la sección II estudia las bondades de las tecnologías semánticas para desarrollar el catálogo. Posteriormente, la sección III explica los principios de diseño más importante del catálogo. La sección IV muestra cómo se conceptualizó la ontología propuesta, mientras que la sección V estudia cómo fue implementada y evaluada. Finalmente, la última sección resume las conclusiones más importantes del artículo, así como las posibles líneas de trabajo futuro.

II. La necesidad de un catálogo semántico

En los últimos años TMF ha propuesto la iniciativa NGOSS (*Next Generation Operations Support Systems*, Sistema de Soporte a Operaciones de Próxima Generación), que proporciona "un entorno de producción más productivo y una eficiente gestión de la infraestructura" [17]. NGOSS está formado por una metodología y cuatro marcos, uno de los cuales es SID (*Shared Information and Data Model*, Información y Modelo de Datos Compartido), un modelo de información que representa las diferentes entidades que aparecen en una empresa de telecomunicación y que puede ser utilizado como un "lenguaje común para desarrolladores e integradores de *software*" [16]. SID es especialmente interesante para el desarrollo de un catálogo de una empresa de telecomunicaciones porque define una conceptualización de los conceptos que aparecen en la empresa y de sus relaciones sin tener en cuenta detalles concretos de sus posibles implementaciones. Otra propuesta similar a SID son los estándares CIM (*Common Information Model*, Modelo Común de Información), desarrollados por DMTF(*Distributed Management Task Force*, Grupo de Trabajo de Gestión Distribuida) [3]. CIM está compuesto por un esquema de datos y una especificación que define los detalles para su integración con otros modelos de gestión. Los objetivos de SID y del esquema de CIM son semejantes: describir conceptos y relaciones que puedan aplicarse a todas las áreas comunes de gestión independientemente de la implementación que se utilice; sin embargo, SID tiene mayor aceptación y actualmente es considerador un estándar de ITU-T[18].

NGOSS también ha detectado la necesidad de extraer el conocimiento de productos, servicios y recursos de los componentes del OSS existentes y recogerlo en un elemento único dentro de la arquitectura del OSS, llamado catálogo. Por eso TMF propuso la iniciativa PSA, definiendo una arquitectura de un catálogo activo y una serie de interfaces para su interoperaibilidad con el OSS y con otros catálogos. Esos catálogos se llaman "activos" porque además de ser un registro de información soportan operaciones sobre el uso y el manejo de productos, servicios y recursos, tales como la reserva de recursos o la validación de servicios [24]. Una aspiración de PSA es estandarizar los catálogos activos de la industria de las telecomunicaciones, permitiendo su federación dentro de la empresa y también con diferentes proveedores de servicio. Dicha federación facilitaría la inclusión de servicios provenientes de terceros en la red, lo que supone una característica importante de las redes NGN [9]. La necesidad de un catálogo también ha sido percibida por diferentes autores, provenientes tanto de la industria como de la academia, incluyendo el Office of Government Commerce, quien publicó ITIL (*Information Technology Infrastructure Library*, Librería de Información sobre Tecnología de Infraestructura), una lista de buenas prácticas para la gestión de servicios de información [13]. No obstante, para compartir información entre catálogos no sólo es necesario tener unas interfaces estandarizadas, sino que se debe compartir un modelo de información, el cual no está definido ni por ITIL ni por PSA. Dicho modelo de información debe estar basado en los estándares existentes, pero ni SID ni el esquema de CIM pueden utilizarse directamente, puesto que para que contengan todos los conceptos necesarios deben ser extendidos. Además, SID especifica una enorme cantidad de conceptos y no es trivial seleccionar cuáles son útiles para la base de conocimiento de un catálogo.

Según PSA, la base de conocimiento de un catálogo activo debe proporcionar información sobre productos, servicios y recursos, así como las relaciones entre dichos conceptos. El principal problema al considerar los recursos es que son muy específicos para cada red y cambian frecuentemente en las redes NGN [9]. Por esa razón la flexibilidad de la base de conocimiento es un requisito imprescindible si se especifican los recursos. Además, como PSA da soporte a la federación de catálogos, su base de conocimiento debe hacer posible el intercambio de información entre diferentes empresas y diferentes componentes del OSS. Por ejemplo, cuando un proveedor de servicio publica un nuevo servicio, otra empresa que desee integrar dicho servico en sus sistemas debe ser capaz de obtener la información sobre los requisitos técnicos que debe cumplir para poder integrarlo. Ese intercambio de información es posible cuando se comparte una conceptualización entre diferentes catálogos, por lo que es imprescindible definir un núcleo para la base de conocimiento del catálogo que pueda ser compartido por diferentes organizaciones y posteriormente extendido por cada una de ellas. Por esta razón, la extensibilidad es otro requisito crítico en la base de conocimiento de un catálogo activo.

En cuanto a catálogos comerciales, los autores sólo tienen

constancia de dos implementaciones con notoria importancia. El primero está incluido en Tribold [26], un sistema de gestión de productos cuyo objetivo es reducir el tiempo y el coste de lanzar un producto al mercado por parte de una empresa de telecomunicación. Tribold utiliza su catálogo como un centro de control centralizado que proporciona un vocabulario de productos y servicios basado en SID. De esta forma Tribold tiene un único punto de control para la gestión de todos los productos y servicios de la empresa que apoya la gestión de productos y la inteligencia de negocio. A pesar de ello, Tribold no contempla la posibilidad de compartir información entre diferentes catálogos, ni tampoco proporciona un modelo de datos que pueda ser modificado de forma sencilla. Otra propuesta interesante es el proyecto SUPER [5], en el que se ha definido un catálogo para la provisión de servicios en la plataforma SUPER. La conceptualización del catálogo también sigue el modelo de SID y está implementada en una ontología con el objetivo de fusionar los estándares con el conocimiento de negocio proveniente de la industria. Sin embargo, dicha conceptualización sólo define los productos y servicios del sistema, mientras que los recursos no están contemplados. El uso de las tecnologías semánticas está motivado para describir los servicios que deben ser implementados y provistos por el sistema y para permitir su integración en la especificación del flujo de trabajo, de forma que las operaciones puedan ser todo lo automáticas que sea posible [14]. Su conclusión más importante es que las tecnologías semánticas hacen más sencilla la inclusión de productos de terceros en el catálogo, y pueden ayudar a abordar los problemas derivados de la heterogeneidad que aparecen de forma natural en el entorno de una empresa de telecomunicaciones. No obstante, el catálogo de SUPER sólo puede usarse cuando se despliegan servicios en la plataforma SUPER, y no aborda el problema de la heterogeneidad de recursos.

Se propone el uso de las tecnologías semánticas para afrontar los requisitos de extensibilidad y flexibilidad del catálogo. Un aspecto importante es implementar la base de conocimiento del catálogo en una ontología, proporcionando una solución flexible para modelar la información necesaria de un dominio, superando la rigidez de otras tecnologías como las bases de datos [4]. De hecho, cuando se incluyen los recursos en el catálogo es posible definir relaciones entre los servicios provistos a un usuario y algunas características de los recursos y, posteriormente, es posible especificar los recursos concretos que satisfacen dichas características. De esta manera, la mayor parte de la información puede ser compartida entre diferentes empresas y puede ser reutilizada si los recursos de una compañía se modifican. A pesar de ello, las tecnologías semánticas son más complejas que las soluciones clásicas, tales como bases de datos o esquemas XML. Esta desventaja es la principal razón por la que las tecnologías semánticas son todavía poco utilizadas en las empresas de telecomunicación [6]. No obstante, la eficiencia de las dichas tecnologías está mejorando e incluso algunas empresas, como Oracle [10], han lanzado sus propios productos comerciales basados en ellas.

Con todo, se propone el desarrollo de una ontología para la base de conocimiento de un catálogo activo que incluya productos, servicios y recursos. Esta ontología debe dar soporte a la comunicación semántica entre diferentes catálogos, así que algunos de sus conceptos deben poder ser compartidos entre terceras empresas. Finalmente, la ontología debe ser lo suficientemente flexible como para satisfacer los cambios que sufren las redes NGN.

III. La arquitectura del modelo de información del catálogo

Para desarrollar la base de conocimiento del catálogo se ha seguido la metodología On-To-Knowledge [19] debido a que es un método simple que está siendo empleado hoy en día en diferentes proyectos. De acuerdo con On-To-Knowledge, se deben estudiar fuentes de diferente naturaleza para distinguir cuáles son los conceptos relevantes que se han de incluir en la ontología. En este caso se estudiaron diferentes fuentes de información, incluyendo estándares de la industria de las telecomunicaciones, literatura publicada al respecto, diversas entrevistas con expertos y el análisis de un OSS real.

Se han seguido los estándares de NGOSS anteriormente citados, con especial interés en SID. Entre otros conceptos, SID distingue entre `products`, `services` y `resources`. `Services` se dividen en aquéllos que son directamente visibles por el consumidor del servicio, `customer facing services`, y aquéllos que no, `resource facing services`. Cualquier producto se puede relacionar con uno o varios grupos de servicios, definiendo los conjuntos de servicios que se agrupan para proporcionar un producto. Además, un servicio se relaciona con los diferentes grupos de recursos que lo pueden proporcionar. No obstante, SID no es adecuado para definir directamente la conceptualización de un catálogo, ya que no proporciona una taxonomía de productos ni servicios, por lo que no es trivial desarrollar una conceptualización que pueda ser utilizada como tal a partir de SID.

Una vez que toda esta información ha sido recogida, se ha propuesto una arquitectura para el modelo de datos que contempla dos gradientes de abstracción. El primer gradiente de abstracción define la arquitectura de cada catálogo y proporciona las relaciones entre diferentes elementos de forma acorde con SID, tal y como se muestra en la Figura 1. El segundo gradiente de abstracción define la relación entre cada catálogo específico y el resto de catálogos que potencialmente podrían aparecer dentro y fuera de la compañía, como muestra la Figura 2. La conceptualización se ha implementado utilizando palabras en inglés debido a que es el idioma en el que está descrito SID.

La Figura 1 muestra la estructura de más alto nivel del catálogo. Siguiendo esta estructura, un `product specification` está compuesto por uno o múltiples `customer facing services specification`.
Tanto el concepto `product` como `customer facing service` abstraen todos los detalles tecnológicos y de implementación y sólo se centran en el comportamiento que dichos conceptos tienen de cara a los usuarios. Cualquier `customer facing service specification` se relaciona con al menos un grupo de `resource facing service specification`, definiendo así el agrupamiento de servicios de red que hacen posible proveer el servicio al usuario. Como puede haber

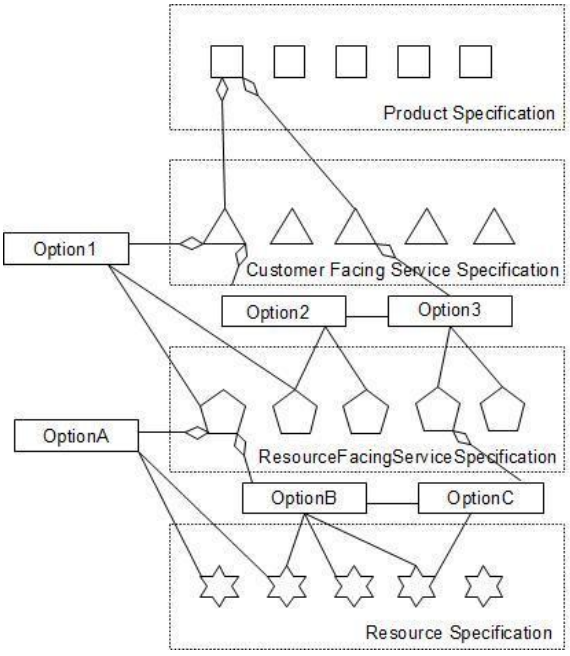


Fig. 1. Conceptos principales y sus relaciones en la arquitectura del catálogo.

múltiples opciones tecnológicas para proporcionar un mismo servicio a un usuario, un `customer facing service specification` puede relacionarse con diferentes grupos de `resource facing service specification` (definidos en la Figura 1 por los conceptos `Option 1`, `Option 2` y `Option 3`). Del mismo modo, un `resource facing service specification` puede estar relacionado con uno o varios grupos de `resource specification`, dependiendo del tipo de recursos que puedan proporcionar el servicio (conceptos `Option A`, `Option B` y `Option C` en la Figura 1).

En este punto se deben resaltar algunos aspectos. En primer lugar, esta estructura es suficientemente general como para poder ser compartida por cualquier empresa de telecomunicación, debido a que no impone ninguna arquitectura tecnológica o empresarial y sólo define los conceptos que una empresa puede manejar. Además, siguiendo dicha estructura, cualquier producto, servicio o recurso puede ser definido. Eso no implica que se deba considerar cualquier concepto posible, pero se debe poder extender la conceptualización para definir la especificación de cualquier elemento, dependiendo de las necesidades particulares de la empresa. Finalmente, puede haber relaciones entre las diferentes opciones que enlazan los distintos niveles. Dichas relaciones permitirán hacer explícitas las dependencias tecnológicas entre las diferentes decisiones a tomar cuando se proporciona un servicio.

A partir de dicha estructura se ha desarrollado el núcleo del modelo del catálogo compartido, que puede ser entendido como una ontología de dominio [7]. Este núcleo debe ser extendido por cada compañía para desarrollar ontologías de aplicación [7] que se correspondan con el modelo del catálogo y que proporcionen todos los conceptos y axiomas necesarios para cada organización. Finalmente, este modelo se puede poblar para definir el catálogo de la empresa, el que variará con el tiempo. De esta manera, se han definido tres niveles de abstracción que se muestran gráficamente en la Figura 2.

El núcleo del modelo proporciona una conceptualización de dominio compartida, permitiendo que cada compañía seleccione los conceptos que necesite y posteriormente añada conceptos más específicos, desarrollando su propio modelo de catálogo. Posteriormente, los modelos pueden ser instanciados y a partir de ellos se pueden especificar diferentes catálogos, facilitando de esta manera su evolución. Nótese que si bien los catálogos de ambas compañías parecen muy diferentes, ambos comparten algunos conceptos, puesto que los conjuntos de conceptos que cada empresa tomó de la conceptualización compartida no son disjuntos, por lo que puede darse la comunicación semántica entre ambas compañías.

IV. Conceptualización de la ontología

Siguiendo la metodología On-To-Knowledge se ha conceptualizado un modelo de información a partir de la arquitectura propuesta en la sección anterior. Partiendo de SID, la primera tarea fue seleccionar qué conceptos eran adecuados para ser utilizados en un catálogo. Posteriormente, algunos conceptos se definieron utilizando las fuentes de información anteriormente citadas. Se debe tener en cuenta que la conceptualización no intenta ser completa, sino definir unos principios de diseño, de forma que pueda ser extendido posteriormente adaptándola a cada contexto concreto. Concretamente, sólo se han considerado productos de usuarios domésticos, que se han relacionado exclusivamente con los servicios que son provistos directamente por una empresa de telecomunicación, tales como una conexión de datos y el acceso a la red. Otros servicios, como provisión de contenidos, no han sido especificados en el catálogo a pesar de que se podría extender para contemplarlos.

En la Figura 3 se observan algunos conceptos del núcleo del modelo de catálogo. Los conceptos que ya están definidos en SID se representan enmarcados en un rectángulo, mientras que el resto ha sido definido por los autores. La taxonomía de `product specification` no se considera explícitamente en la figura, pero se pueden entender como agrupaciones de `customer facing service specification`, tal y como se explicó en la sección anterior.

SID determinad que un `customer facing service` es "una abstracción que define las características y el comportamiento de un servicio concreto tal y como lo ve el usuario" [22]. En otras palabras, un `customer facing service` es lo que el usuario disfruta, esto es, el servicio que es dado al usuario abstrayendo todos sus detalles tecnológicos. SID distingue entre `simple` y `composite customer facing services`. Los servicios simples son atómicos y puede ser agregados para formar un servicio compuesto que será comprensible por el usuario. Un producto está compuesto por un conjunto de `customer facing services`, ya sean simples o compuestos.

Se han definido seis categorías principales de `customer facing service specification`: `UserEquipmentSpec`, relacionado con los servicios que proporciona el equpamiento en las pertenencias del usuario; `AccessSpec` incluye el acceso a la red; `CommunicationSpec` se relaciona con los diferentes medios de comunicación a los que el usuario puede tener acceso; `ContentDeliverySpec`, donde se incluyen los

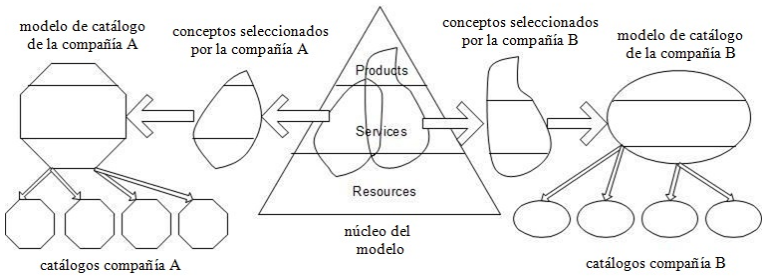


Fig. 2. Representación gráfica del núcleo, modelos y catálogos.

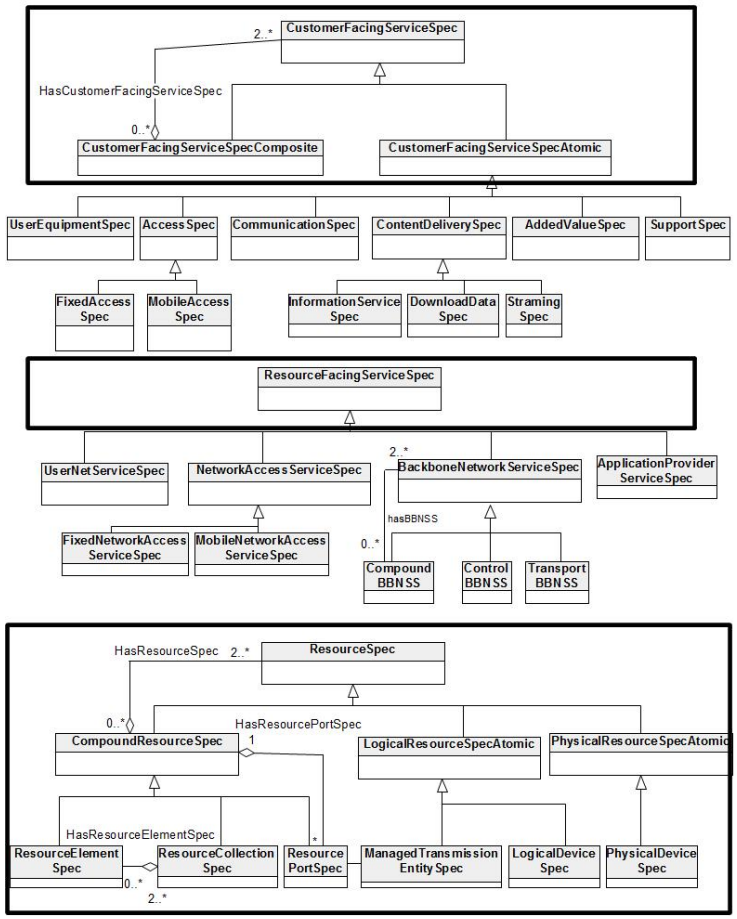


Fig. 3. Los conceptos de alto nivel del núclo del catálogo.

conceptos relacionados con la provisión de contenidos, tanto si son bajo demanda como *broadcast*; `AddedValueSpec` especifica servicios que proporcionan un valor añadido a los servicios de comunicación; finalmente `SupportSpec` está relacionado con los servicios de soporte que se proporcionan al usuario.

Por otra parte, los `resource facing service` son "abstracciones que definen las características y el comportamiento de un servicio particular que no es visto ni comprado directamente por el usuario" [22], es decir, que servicios que proporciona la red al usuario para satisfacer las necesidades de los productos por él adquiridos, sin importar si el usuario es consciente de ellos o no. SID distingue entre `simple` y `composite resource facing service specifications`, de manera que se puede definir una jerarquía de servicios de red. No obstante, para nuestros propósitos se han considerado cuatro categorías de `resource facing services specifications`: `UserNetServiceSpec` incluye las especificaciones de servicios relacionads con la red propia del usuario; `NetworkAccessServiceSpec` incluye los servicios relacionados con tecnologías que permiten comunicar al usuario con la red de `backbone` de la empresa de telecomunicaciones; `BackboneNetworkServiceSpec` se relaciona con cualquier servicio de la red de `backbone`; `ApplicationProviderServiceSpec` se relaciona con los servicios que permiten el acceso a la red de un proveedor de servicio.

Finalmente, resource es definidos en SID como una "entidad que es manejables en sí misma y que da lugar a un producto" [23]. Como la conceptualización de recursos está mucho más detallada que la de servicios, no ha sido necesario crear nuevos conceptos, sino simplemente seleccionar aquéllos que son útiles en un catálogo. Resource specification ha sido dividido en tres categorías principales: PhysicalResourceSpec es una clase abstracta que representa las especificaciones de "elementos *hardware* que pueden ser manejados", mientras que LogicalResourceSpec representa las especificaciones de "conceptos lógicos y servicios que pueden ser manejados y que están relacionados con un elemento como un todo". ResourceCompoundSpec se utiliza para describir especificaciones de "entidades manejables que son colecciones de otras entidades manejables".

Una vez que se conceptualizó el núcleo del modelo de catálogo se particularizó para adaptarlo a las necesidades de un OSS concreto, y así diseñar el modelo de catálogo proporcionando un vocabulario más específico al OSS. Por ejemplo, el concepto TransportBBNSS fue extendido definiendo dos subconceptos: ATMConnection y GBEthernetConnection. Dichos conceptos están relacionados con las alternativas tecnológicas que un OSS puede contemplar al proporcionar un servicio de transporte de datos en la red *backbone* de la empresa.

A modo de ilustración, se ha diseñado un modelo de información para un catálogo concreto, tal y como muestra la Figura 4. Este ejemplo sólo contempla la especificación de producto Speedy3Mb, que es un producto doméstico que proporciona conexión a Internet, 10 cuentas de correo electrónico, almacenamiento web, soporte, *software* antivirus y acceso a algunos contenidos. Todos estos servicios son los customer facing service specifications definidos en el ejemplo, los cuales están relacionados con los conceptos definidos en el núcleo del modelo del catálogo. Con el ánimo de hacer la Figura 4 más legible, sólo se han hecho explícitas las relaciones de dos de estos servicios con sus resource facing service specifications correspondientes. Como ejemplo, 3MbFixedAccessSpec tiene dos opciones que lo relacionan con servicios ADSL y VDSL. Nótese que los conceptos ADSL2+ y VDSL son particularizaciones de ADSL2+AccessServiceSpec y VDSL–AccessServiceSpec, que fueron definidos en el modelo de catálogo (véase la Figura 4). Finalmente, el concepto ADSL2+ está relacionado con dos grupos diferentes de recursos, algunos relacionados con los conceptos definidos en SID, tal como TrailTerminationPortSpec, y otros definidos en el modelo de catálogo, tal como DSLAMSpec.

V. Implementación de la ontología y prueba de concepto

Para implementar la ontología anteriormente descrita se debe seleccionar un metalenguaje . En este caso, se escogió OWL-DL [2] puesto que proporciona la expresividad necesaria para implementar un catálogo activo mientras que la decidibilidad de la conceptualización está garantizada. Además, al ser un metalenguaje muy utilizado hoy en día, OWL-DL está muy documentado y existen numerosas herramientas que le dan soporte. Protégé Ontology Editor 3.3.1 [8], es un editor ampliamente utilizado y fue seleccionado para facilitar la codificación de la ontología. Además, el razonador RacerPro 1.9.2 [15] se ha usado para clasificar la ontología y comprobar su consistencia, utilizando la interfaz DIG [1].

Durante el proceso de formalización se han seguido las buenas prácticas publicadas en [12], donde se indica que las clases deben relacionarse con los conceptos más generales (los que aparecen en el núcleo del catálogo y en el modelo del catálogo), mientras que los individuos deben representar a los más específicos (los conceptos del catálogo). La implementación de la ontología se dividió en tres ficheros: el primero implementa el núcleo del modelo del catálogo, el segundo lo extiende y define el modelo del catálogo y el tercero implementa el catálogo en sí. De esta forma los tres niveles de abstracción pueden extenderse de forma independiente tan sólo con la restricción de asegurar la consistencia entre ellos. Esto redunda en una mayor flexibilidad de la conceptualización, ya que cualquier capa puede ser modificada fácilmente sin necesidad de cambiar las demás, permitiendo que diferentes modelos de catálogos compartan un mismo núcleo y que diferentes catálogos particularicen un mismo modelo. Otra ventaja es que es posible compartir el núcleo del modelo entre diferentes empresas mientras que el modelo de catálogo se mantiene en privado.

De acuerdo con la metodología On-To-Knowledge, la ontología debe ser evaluada una vez que ha sido formalizada. Se ha llevado a cabo una evaluación preliminar, mezclando una evaluación centrada en el usuario, en la que se estudia si la aplicación satisface a los usuarios, y una evaluación centrada en la tecnología, donde se estudian las propiedades tecnológicas de la ontología [21].

Tal y como recomienda On-To-Knowledge, la evaluación centrada en el usuario consiste en estudiar si la ontología satisface una serie de preguntas de competencia. Concretamente, se pidió a dos expertos del dominio, externos a los autores, que propusieran algunas preguntas que debería responder el catálogo en un escenario real. Dichas preguntas fueron posteriormente traducidas de lenguaje natural a nRQL [15], un lenguaje comprensible por RacerPro. Las preguntas se relacionaban con dos escenarios diferentes: una situación en la que el personal de *marketing* consulta a la ontología qué servicios incluye un producto, y otro escenario en el que un sistema de provisión inquiere sobre la configuración que deben tener los recursos para proporcionar un servicio a un cliente. Un ejemplo de una pregunta de competencia es "¿Puede conectarse un enlace VDSL a una red *backbone* con tecnología ATM?". En vocabulario definido por la ontología, se pregunta si existe alguna relación de imposibilidad entre los conceptos CFSSpec2RFSSpec que relacionan los customer facing service specifications con VDSL y aquéllos que los relacionan con ATM. Dicha pregunta fue traducida como:

```
 (retrieve (?y) (and (?y meta:Impossibi
lity) (?x VDSL meta:isRelatedToRFSS)
(?z ATM meta:isRelatedToRFSS)
(?y ?x meta:hasCFSS2RFSS)
(?y ?z meta:hasCFSS2RFSS)))
```

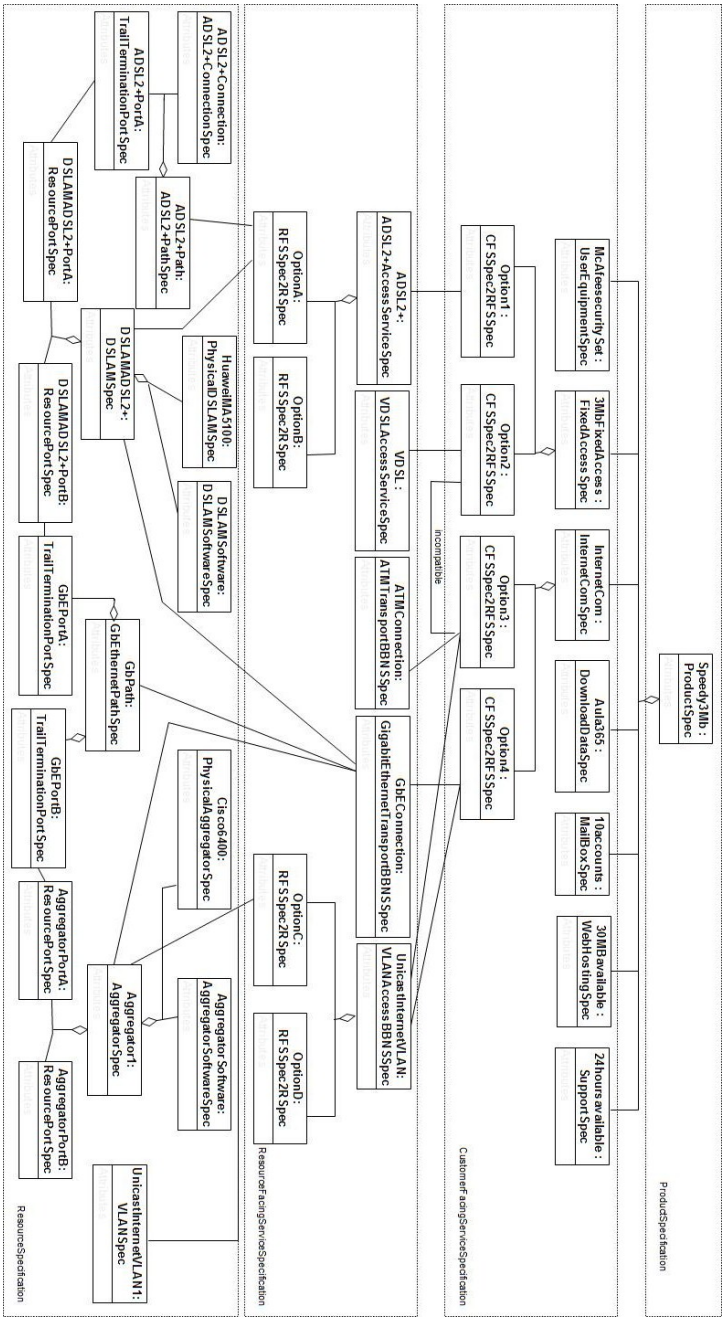


Fig. 4. Ejemplo de un modelo de información para el catálogo de una empresa de telecomunicaciones.

En este caso, el sistema devuelve el concepto `notVDSLandATM`, una instancia del concepto `Impossibility`. Dicha imposibilidad se muestra en la Figura 4 como una relación entre los conceptos `Option2` y `Option3`. De esta forma se hace explícito que ATM y VDSL son tecnologías incompatibles cuando se proporciona un servicio.

Por otro lado, la evaluación centrada en la tecnología debe mostrar la flexibilidad y extensibilidad de la ontología. Para evaluar estas características se supone una situación en la que una nueva especificación de un elemento se incluye en el sistema, concretamente se debe definir el concepto `agregador Cisco 10000`. Para ello se editó la ontología y se definió un nuevo concepto del tipo `PhysicalAggregatorSpec` y otro del tipo `AggregatorSpec`, definiendo el *hardware* del agregador y el agregador como un todo respectivamente. Posteriormente, se consideró otro concepto para permitir la relación entre los nuevos conceptos creados y los `resource facing service specifications` previamente existentes. Así, al proporcionar conexión a Internet, el sistema permitirá dos opciones: una de ellas utiliza un CISCO 6400 y la otra un CISCO 10000. Se puede observar que con tan sólo crear tres conceptos, y sin necesidad de modificar los previamente existentes, es posible insertar la especificación de un nuevo elemento en el catálogo, relacionándolo con el resto de conceptos.

VI. Conclusiones y trabajo futuro

La creación de catálogos se ha propuesto recientemente en la industria de las telecomunicaciones, con el objetivo de

recoger el conocimiento sobre productos, servicios y recursos en un único componente del OSS. De esta manera, dicho conocimiento puede extraerse de los sistemas existentes, de forma que se reduzca su complejidad. Recientemente, se han propuesto algunos catálogos con el objetivo de mejorar la gestión de los procesos de negocio; sin embargo, ninguno de ellos tiene en cuenta las especificaciones de recursos, y por tanto no puede proporcionar una visión global de todas las entidades que toman parte en la provisión de un producto. El presente artículo propone la creación de un catálogo de productos, servicios y recursos utilizando tecnologías semánticas. A pesar de que las tecnologías semánticas sean relativamente complejas, la extensibilidad que proporcionan hace de ellas una solución adecuada para cumplir con la necesidad de compartir el catálogo entre diferentes empresas. Además, la posibilidad de definir restricciones en un nivel de abstracción mayor aumenta la flexibilidad del catálogo, lo que supone un requisito crítico cuando se trabaja con redes NGN.

El presente artículo supone un primer paso en el desarrollo de un catálogo semántico, presentando una conceptualización para la base de conocimiento de un catálogo y su implementación en una ontología. La conceptualización se basa en SID, un estándar actualmente en uso, esperando que así se facilite la integración del catálogo en el OSS y su distribución entre diferentes organizaciones. Para favorecer este último aspecto la conceptualización de la base de conocimiento define tres niveles de abstracción diferentes, permitiendo la federación de catálogo por parte de terceros. Esta conceptualización ha sido implementada y se ha llevado a cabo una prueba de concepto. A pesar de que se trata de una evaluación preliminar, se han logrado algunos resultados prometedores, puesto que se ha mostrado que la ontología es capaz de responder a algunas preguntas de competencia hechas por expertos externos a los autores y que se puede incluir nuevas especificaciones de elementos de forma sencilla.

Como se ha tomado la ontología On-To-Knowledge, se debe proceder de forma cíclica sobre el diseño y la evaluación de la ontología para refinarla. El trabajo futuro se centrará en desarrollar un primer prototipo del catálogo e integrarlo en un OSS real para dar soporte al sistema de provisión. Esta experiencia mostrará si la ontología es capaz de adaptarse a las necesidades de un OSS real y proporcionará una información muy útil para la mejora de la ontología. Posteriormente, debe comprobarse si la ontología da soporte a la comunicación semántica entre diferentes organizaciones.

VII. Agradecimientos

El trabajo publicado en el presente artículo ha sido financiado por el proyecto Euricles, el cual supuso una colaboración entre Telefónica I+D (TID) y la Universidad de Valladolid. Los autores agradecen la ayuda por parte del personal de TID, especialmente a Mario López-Gallego, de TID Valladolid, y Francisco Javier Zorzano-Mier, de TID Madrid.

Referencias

[1] S. Bechhofer. The DIG Description Logic Interface: DIG/1.1. Technical report, University of Manchester, febrero 2003. URL = http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-81/bechhofer.ps, última visita abril de 2009.

[2] S. Bechhofer, F. van Harmelen, J. Hendler, I. Horrocks, D. L. McGuinness, P.F. Patel-Schneider, and L.A. Stein. OWL Web Ontology Language Reference. Recommendation, W3C, febrero 2004. URL = http://www.w3.org/TR/owl-ref/, última visita abril de 2009.

[3] Distributed Management Task Force, Inc. Common Information Model (CIM) Standards. URL = http://www.dmtf.org/standards/cim/, última visita abril de 2009.

[4] D. Florescu. Managing semi-structured data. *Queue*, 3(8):18–24, 2005.

[5] J. Frankowski, H. Kupidura, P. Rubach, and E. Szczekocka. Business process management for convergent services provisioning using the SUPER Platform. In *International Conference on Intelligence in service delivery Networks (ICIN)*, Bordeaux, France, October 2008.

[6] J. Frankowski, P. Rubach, and E. Szczekocka. Collaborative Ontology Development in Real Telecom Environment. In W. Abramowicz and L. Macaiaszek, editors, *1st International Working Conference on Business Processes and Services Computing (BPSC 07)*, pages 40 – 53, 2007.

[7] N. Guarino. Formal Ontology and Information Systems. In *Proceedings on Formal Ontology in Information Systems (FOIS ´98)*, pages 3 – 15. IOS Press, 1998.

[8] H. Knublauch, R. W. Fergerson, N. F. Noy, and M. A. Musen. The Protégé OWL plugin: An open development environment for semantic web applications. In *Proceedings of the Third International Semantic Web Conference (ISWC 2004)*, LNCS 3298, pages 229–243, Hiroshima, Japan, noviembre 2004.

[9] C.S. Lee and D. Knight. Realization of the Next Generation Network. *IEEE Communications Magazine*, 43(10):34 – 41, 2005.

[10] C. Murray. Oracle Database. Semantic Technologies Developer's Guide. Technical report, Oracle, noviembre 2009. URL = http://download.oracle.com/docs/cd/E11882_01/appdev.112/e11828.pdf, última visita abril de 2009.

[11] B. Naughton, S. Osborne, G. Senior, and P. Kitteringham. Service assembly and delivery. Patent, International Publication Number WO 2008/068524 A2, junio 2008.

[12] N. F. Noy and D. L. McGuinness. Ontology development 101: A guide to creating your first ontology. Technical Report SMI-2001-0880, Stanford Knowledge Systems Laboratory, marzo 2001.

[13] Office of Government Commerce (OGC). ITIL Version 3 Lifecycle Process Model. Technical report, Office of Government Commerce (OGC), junio 2007. URL = http://www.best-management-practice.com/ITILV3ProcessModel, última visita abril de 2009.

[14] Daniel Pop, Teodor-Florin Fortis, and Viorel Negru. Ontology-Based Modeling and Execution of Workflows for Virtual ISP. In *CISIS '08: Proceedings of the 2008 International Conference on Complex, Intelligent and Software Intensive Systems*, pages 1007–1011, Washington, DC, USA, 2008. IEEE Computer Society.

[15] Racer Systems GmbH & Co.KG. RacerPro user's guide. Technical Report 1.9, Racer Systems GmbH & Co.KG, diciembre 2005.

[16] J. P. Reilly. *Getting Started with the SID. A SID Modeler´s Guide*. The Lean Corporation, 2007.

[17] J. P. Reilly and M. J. Creaner. *NGOSS distilled*. The Lean Corporation, 2005.

[18] D. Sidor and K. Johannessen. ITU-T Recommendation M.3190 Shared Information and Data Model (SID). Recommendation, ITU-T, julio 2008. Prepublished recommendation.

[19] S. Staab, R. Studer, H. P. Schnurr, and Y. Sure. Knowledge processes and ontologies. *IEEE Intelligent Systems*, 16(1):26–34, 2001.

[20] S. Stein, C. Stamber, M. El Kharbili, and P. Rubach. Semantic business process management: An empirical case study. In M. Turowski K. Loos, P. Nüttgens and D. Weth, editors, *Proceedings of the MobIS 2008 Workshops*, pages 165–177, noviembre 2008.

[21] Y. Sure, S. Staab, and R. Studer. Methodology for development and employment of ontology based knowledge management applications. *ACM SIGMOD Record*, 31(4):18 – 23, 2002.

[22] TeleManagement Forum. Shared Information/Data Model (SID). Addendum 4S0. Service Overview Business Entity Definitions, 2004.

[23] TeleManagement Forum. Shared Information/Data Model (SID). Addendum 5LR. Logical Resource Business Entity Definitions, 2004.

[24] TeleManagement Forum. Product and Service Assembly Catalyst: Interface Implementation Specification, 2007.

[25] K. Terplan. *OSS Essentials: Support System Solutions for Service Providers*. John Wiley, 2001.

[26] Tribold. Tribold 3.0 white paper. URL = http://www.tribold.com/index.cfm, última visita abril de 2009.

[27] B. Watson-Luke and D. J. Cooke. System and method for managing OSS component configuration. Patent US 2005/0114642 A1, mayo 2006.

Adaptación del Simulador OPNET para Aplicaciones de Control Industrial con Tecnología 802.11

J. Jiménez, R. Estepa, F.R. Rubio, F. Gómez-Estern, A. Estepa
Área de Telemática, Escuela Superior de Ingenieros
Universidad de Sevilla
C/ Camino de los Descubrimientos s/n., 41092 Sevilla (España).
E-mail:{juanjimenez,rafa}@trajano.us.es, {fabio,rubio}@us.es, aestepa@trajano.us.es

***Resumen*—El control de procesos industriales mediante redes 802.11 se incluye en el área WNCS (Wireless Network Control System), que experimenta en la actualidad una gran expansión. La falta de herramientas de simulación apropiadas para combinar ambos entornos, las redes de telecomunicación y control de sistemas, es una de las lagunas que dificultan la validación de las incipientes contribuciones en este campo. El objetivo de los autores es conseguir un simulador unificado para control industrial con tecnología inalámbrica 802.11. Para ello se desarrollan módulos que amplían el conocido simulador OPNET al campo del control de sistemas, permitiendo así el análisis del rango de trabajo de los parámetros implicados en la tecnología 802.11 cuando se aplica al control de procesos industriales. Así mismo se presenta una primera aproximación al dimensionamiento de este tipo de escenarios, determinando mediante simulación las condiciones más apropiadas para el uso de la tecnología 802.11 en el lazo de control.**

I. Introducción

El control de procesos industriales presenta como característica unos requisitos muy estrictos de tiempo (retardo), pérdida de paquetes y consumo de energía. A su vez, el tráfico generado por las aplicaciones (normalmente sensores o equipos embebidos) suele ser tráfico periódico que representa uno o varios valores (llamados variables de control) con sus correspondientes marcas de tiempo. Dicha información llega por una red o bus de campo hasta el punto de acceso (PA), que la reenviaría hasta el controlador. Es habitual en bastantes escenarios que el número de sensores sea muy superior al número de actuadores, por lo que en nuestro caso supondremos que el controlador genera información de control hacia los actuadores, enviándola por una red cableada. Esta hipótesis permite simplificar el estudio a un escenario con tráfico homogéneo, ya que si se considera el tráfico desde el AP hacia los sensores, se introduce un factor de heterogeneidad de tráfico que complica la interpretación de los resultados.

En la actualidad existe una clara tendencia a utilizar redes inalámbricas para el control de procesos industriales. Como principal ventaja de esta alternativa tenemos la eliminación de costes de cableado que presentan las soluciones como Profibus, ModMus, FoundationFieldbus, etc. Existen varias tecnologías candidatas a ser utilizadas para tal propósito, entre las que destacan: 802.11, ZigBee, y BlueTooth. En [1] se analizan en detalle desde el punto de vista de los requisitos del control de procesos concluyendo que 802.11y ZigBee son las tecnologías más adecuadas para esta tarea. Esta conclusión también se comparte en [2]. Todo esto unido a las mejoras que aporta la reciente norma 802.11n (transmisión MIMO e incremento en las velocidades) y el hecho de que las fábricas presentan cada vez más infraestructuras 802.11 para tráfico de gestión (almacenes de paletización automática, acceso a SAP, etc.) que podrían ser reutilizadas para el control de procesos hacen de la tecnología 802.11 una seria candidata a ser utilizada en este campo.

Existe una gran cantidad de trabajos que tratan el uso de redes 802.11 para el tráfico en tiempo real. Entre ellos podemos destacar [3], [4], [5] donde se analiza el rendimiento de red en términos de caudal y retardo en función del tráfico ofrecido, estableciendo sus límites de funcionamiento. Sin embargo, en la mayoría de estos trabajos se suponen fuentes de tráfico Poissonianas, mientras que muchas aplicaciones de tiempo real (control industrial, VoIP, etc.) generan su tráfico de forma periódica. Además, los trabajos anteriores establecen unos tamaños de paquete (entre 512 y 1024 bytes) mucho mayores que los utilizados habitualmente por las aplicaciones de tiempo real mencionadas anteriormente (usualmente entre 4 y 80 bytes). En 802.11 el uso de paquetes pequeños tiene un impacto muy negativo sobre el rendimiento debido a la sobrecarga de cabeceras e información de control. Esto provoca que en escenarios exigentes compuestos por un gran número de sensores (varias decenas) con tasas de muestreo muy elevadas (del orden de 100ms.), la capacidad 802.11b no sea suficiente y haya que recurrir a 802.11g o incluso 802.11n. Este fenómeno supone una motivación extra para este trabajos ya que todos los trabajos mencionados anteriormente utilizan el estandar 802.11b.

Sobre el consumo energético en redes 802.11 podemos encontrar trabajos como [6], [7], [8] donde se realizan análisis basados en los modelos anteriores para obtener el consumo de las estaciones. Estos estudios parten de las mismas hipótesis anteriormente citadas.

En el campo del control de procesos industriales bajo redes 802.11 existen algunas aportaciones recientes de gran interés como [9], dónde se realiza una estimación de interferencias en redes 802.11 basado en filtros de Kalman para situaciones de congestión y [10] cuyo trabajo propone el ajuste dinámico del número máximo de retransmisiones y de los parámetros del controlador para tener un control de calidad.

Uno de los inconvenientes para el estudio conjunto de control y redes es que las herramientas de simulación de cada

ámbito han evolucionado de forma separada. Tal es así, que actualmente no existe ningún simulador que integre con éxito ambas disciplinas. En el campo del Control suele utilizarse Matlab, dónde existe un módulo llamado TrueTime [11] que permite utilizar redes Zigbee y 802.11. Lamentablemente, Truetime no es un simulador de redes completo y tan sólo es útil para ciertos escenarios de red. Una de sus limitaciones más notables es que no es extensible a redes que incluyan protocolos de capas superiores (encaminamiento, transporte y aplicación), sólo implementa el estándar 802.11b y no soporta el modo infraestructura. Estas dos últimas limitaciones hacen de Truetime una herramienta poco adecuada para el objetivo de nuestro estudio.

En el campo de las redes suelen utilizarse simuladores como NS2 u OPNET. La principal ventaja de este último es su arquitectura altamente modular que facilita su extensión, que proporciona una interfaz de desarrollo muy intuitiva y que tiene una curva de aprendizaje más rápida que NS2). También ofrece funcionalidades avanzadas para el análisis de resultados como representaciones de gráficos y tratamiento estadístico de datos. Sin embargo, OPNET no ha sido diseñado específicamente para su uso en el control.

Disponer de una herramienta de simulación única para el diseño de sistemas WNCS (Wireless Network Control System) permite establecer relaciones entre las variables de control y de red de manera detallada. Además, disponer de un modelo de red preciso puede ser muy útil a la hora de diseñar estrategias de control. Las alternativas disponibles para ello pasan por la extensión de OPNET o Truetime para el soporte de sistemas de control y red, o bien una cosimulación dónde se el simulador de red se integre con otro de control (típicamente MATLAB).

La cosimulación implica un mayor consumo de recursos que además, limita y ralentiza la obtención de resultados en simulaciones con cargas de trabajo altas (escenario con varias decenas o centenas de sensores). En caso de que el tamaño del escenario lo permita, una cosimulación usando OPNET y MATLAB puede ser una estrategia muy recomendable ya que permite al primero se encargue sólo de la simulación de la red y al segundo de los cálculos y el diseño de leyes de control. Para aquellos escenarios donde no sea viable la cosimulación, es necesario escoger una opción alternativa. Teniendo en cuenta la buena precisión del modelado de redes 802.11 que ofrece OPNET, afrontar una extensión de Truetime con el objetivo de obtener un nivel de fidelidad similar supone una tarea mucho más costosa que adaptar OPNET a la simulación de sistemas de control, puesto que en OPNET es posible programar leyes de control utilizando librerías en C++ que integran muchas de las funciones necesarias.

Este trabajo tiene un doble objetivo. Por un lado, se presentará la adaptación de OPNET al entorno del control automático, concretamente al WNCS para la tecnología 802.11, lo que exige el desarrollo de módulos de sistemas dinámicos, control y cómputo del consumo de energía. Como segundo objetivo, este trabajo pretende analizar las peculiaridades de la tecnología 802.11 cuando se aplica a requisitos de retardo, pérdidas y consumos de energía propios del campo de control de procesos, intentando establecer los límites en el rango del número máximo de estaciones permitidas y frecuencia de muestreo de la señal para los sensores. Se analizarán además los comportamientos del retardo, pérdidas y energía para diversos valores de tamaños de buffer o tamaños de paquete. Todo ello permitirá establecer el rango de trabajo de esta tecnología para este campo y conocer mejor su dinámica a fin de elaborar con posterioridad un diseño conjunto que permita optimizar tanto la ley de control como los parámetros de la red 802.11 como pueden ser tamaño de paquete, tamaño de buffer, número máximo de reintentos, etc.

El artículo se organiza de la siguiente manera; en la sección II se describe la adaptación de OPNET para su uso en sistemas WNCS. La sección III ofrece los resultados obtenidos mediante simulación donde se exploran los límites de la 802.11 para su uso en aplicaciones WNCS según varios parámetros como el número máximo de sensores, consumo energético, tamaño de los buffers, etc. La sección IV presenta los resultados de un caso práctico de uso en WNCS en un sistema de primer orden con control proporcional. Finalmente la sección V resume las conclusiones y avanza las líneas futuras del trabajo.

II. Adaptación de Opnet para su uso en el control de procesos industriales

Esta sección presenta los cambios realizados en la versión 14.5 de OPNET para su uso en WNCS.

II-A. Creación de un Módulo de Control

El módulo desarrollado permite la simulación de un sistema dinámico discreto en el tiempo, que puede describirse mediante las siguientes ecuaciones en el espacio de estado:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + Du(k) \end{aligned} \quad (1)$$

Donde A, B, C y D son matrices fijas de dimensiones apropiadas, $x(k) \in \Re^n$ es el vector de estado, $y(k) \in \Re^p$ el vector de salida y $u(k) \in \Re^m$ es el vector de control. Las condiciones iniciales del sistema vendrían fijadas por $x(0)$. Para modelar un sistema de este tipo, debemos implementar diversas entidades en OPNET: Nodo Planta, Módulo de Control y Módulo de Envío del Sensor.

El *Nodo Planta* ejecuta las dos ecuaciones anteriores, actualizándolas en función de un tiempo de muestreo predeterminado, que será configurable. El modelo de este nodo se refleja en la Fig. 1. donde se recogen todos los estados y transiones del sistema.

1. *Reposo (Idle)*: El sistema no evoluciona mientras se encuentre en este estado. Se permanece en él hasta que se inicia un nuevo muestreo del sistema o se reciba una señal de control $u(k)$.
2. *Recepción (Receive)*: Se salta a este estado cada vez que se reciba una nueva señal de control. Esta señal de control puede proceder de la misma estación en la que se ha implementado el sistema dinámico (control local) o de una estación diferente (control a través de red). Es posible que en el momento de recepción de la señal de control no coincida con un nuevo instante de muestreo, de manera que $u(k)$ será almacenada y sólo se aplicará al sistema cuando corresponda. Por tanto, tras recibir $u(k)$ se regresa al estado de reposo y se espera hasta el momento de actualización del sistema.

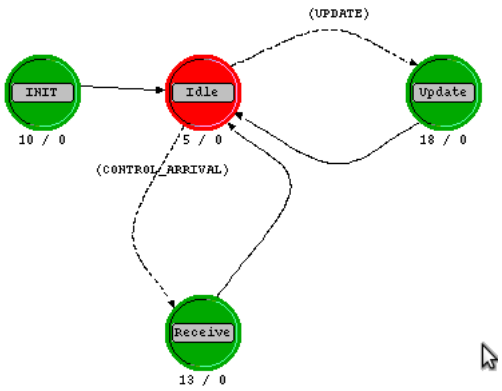


Figura 1. Diagrama de estado del Nodo Planta

3. *Actualización (Update)*: Este estado se ejecuta con una periodicidad igual al periodo de muestro del sistema y es el encargado de implementar las ecuaciones de evolución del sistema. Tras ejecutar el paso del sistema de $y(k)$ a $y(k+1)$, envía la muestra a la capa de transporte de la estación para que esta se encargue de enviarla a su destinatario, es decir, la estación controladora (en caso de que el controlador se encuentre en una estación distinta). Finalmente vuelve al estado de reposo y espera un nuevo instante de actualización.

El *Módulo de envío* de datos se conecta con la capa de envío de tráfico de una estación 802.11 para formar un sensor, que busca el valor de la señal $y(k)$ de la planta cada cierto tiempo, fijado por la frecuencia de muestreo de la planta configurada para dicho sensor (f_s), y envia dicho valor en un paquete IP/UDP hacia el controlador, ubicado en el punto de acceso.

El Módulo de Control se ubica en el nodo punto de acceso, conectado a su capa de aplicación. Se encarga de recibir la señal $y(k)$ y enviar a la planta (vía Ethernet) el valor de la señal de control correspondiente: $u(k) = -K \cdot y(k)$. El control implementado es un sencillo control proporcional, que permite estabilizar a un sistema de primer orden. El parámetro K es configurable y en su lugar se puede implementar cualquier tipo de control.

II-B. Creación de Módulo de consumo de Energía

El consumo energético de una estación inalámbrica depende del estado en el que se encuentre ésta en cada momento. En el módulo desarrollado se distinguen entre los estados de reposo, transmisión, recepción y colisión, con consumos diferentes en casa uno de ellos. Para obtener el consumo de total de energía por estación hacemos uso de la relación:

$$E = P_{idle} \cdot T_{idle} + P_{tx} \cdot T_{tx} + P_{rx} \cdot T_{rx} + P_{col} \cdot T_{col} \quad (2)$$

donde E representa la energía consumida (en Julios), P_{tx}, P_{rx}, P_{idle} y P_{col} son los consumos asociados a cada estado y T_{idle}, T_{tx}, T_{rx} y T_{col} son los tiempos que pasa la estación en cada estado.

El módulo permite como parámetros fijar los consumos de potencia en cada estado y nos proporciona como estadístico la energía consumida en el terminal hasta un instante de tiempo determinado. Los consumos de potencia utilizados para las simulaciones han sido obtenidos de [6]. Para caracterizar el consumo de forma precisa debe ser posible identificar su modo de operación en todo momento e ir acumulando el periodo de tiempo que un terminal pasa en cada uno de los distintos estados de consumo a lo largo de la simulación. El modelo de consumo desarrollado en OPNET divide el consumo total en cuatro estados de gasto energético:

1. *Reposo (Idle)*: Es el estado de menor consumo. La estación se limita a escuchar el medio y permanece aquí hasta que comience una nueva transmisión o se reciba una nueva trama.
2. *Transmisión (Txon)*: Se entra al comienzo de cada nueva transmisión, pasando al estado de reposo una vez finalizada. Es el estado con mayor consumo asociado.
3. *Recepción (Rxon)*: Al detectarse el inicio de una nueva trama el modelo salta a este estado y permanece en él hasta que finaliza la recepción (pasando después al estado de reposo) o hasta que se detecta una colisión (pasando al estado colisión). El consumo en éste estado es menor que en transmisión y mayor que en reposo.
4. *Colisión (Collision)*: El modelo permanecerá en este estado mientras dure la colisión. Una vez finalizada pasa al estado de reposo. El consumo es el mismo que en el estado de recepción.

El módulo desarrollado debe recibir información de la capa física para poder conocer el estado del canal en todo momento, lo que a su vez le permite determinar el estado de consumo energético. Esta es la razón por la que el módulo de energía es conectado a los módulos de transmisión y recepción de la capa física tal y como se muestra en la Fig. 2.

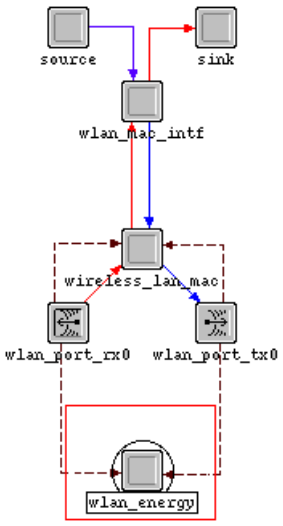


Figura 2. Diagrama de módulos de medición del consumo

III. LÍMITES DE 802.11 PARA EL USO EN APLICACIONES DE CONTROL DE PROCESOS

En este apartado planteamos el siguiente escenario: un cierto número de nodos (representan sensores) N que varía desde 10 hasta 50, situados equidistantes a 50 m. del punto de acceso y que se encuentran enviando datos de una señal muestreada de forma periódica (con frecuencia f_s) al controlador integrado en la estación que representa al punto de acceso. El tamaño

de los paquetes es de longitud fija de 40 bytes (incluyendo cabeceras IP, UDP y de aplicación), lo que deja 12 bytes para el envío de una muestra y su correspondiente marca de tiempo. Es habitual en bastantes escenarios que el número de sensores sea muy superior al número de actuadores, por lo que en nuestro caso supondremos que el controlador genera información de control hacia los actuadores, enviándola por una red cableada.

Consideraremos que la relación señal a ruido es de 30dB (en ese rango no existen problemas de descodificación) y que la infraestructura 802.11 está configurada con los parámetros típicos para aplicaciones de gestión (capa física 802.11g a 2,4 GHz, 54 Mbps y los valores por defecto con respecto al límite máximo de retransmisiones, tamaños de ventana, etc.) El tamaño del buffer para el nivel de aplicación es de 256.000 bits, permitiendo el encolado de 21 paquetes de 1.500 bytes o de hasta 800 paquetes de pequeño tamaño (40 bytes).

III-A. Número máximo de sensores en función de la frecuencia de muestreo

Las Figs. 3 y 4 presentan los resultados de simulación relativos al comportamiento de las pérdidas de paquetes y el retardo respectivamente.

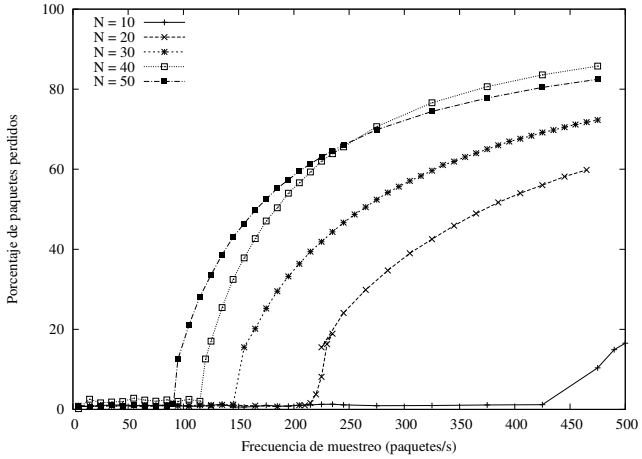


Figura 3. Porcentaje de pérdidas de paquetes en función de la tasa de muestreo para distinto número de nodos (buffer grande)

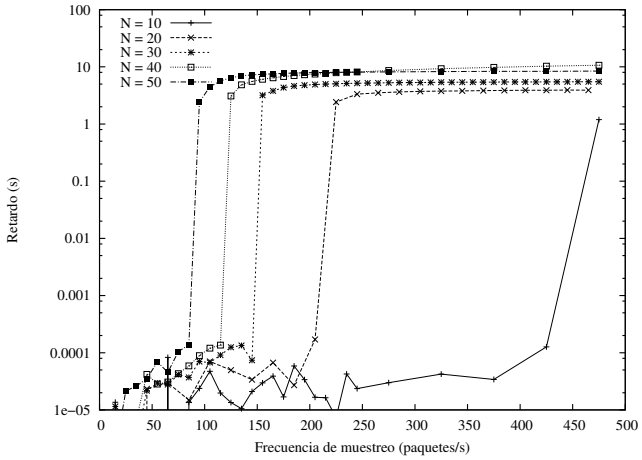


Figura 4. Retardo sufrido por los paquetes en función de la tasa de muestreo para diferente número de sensores (buffer grande)

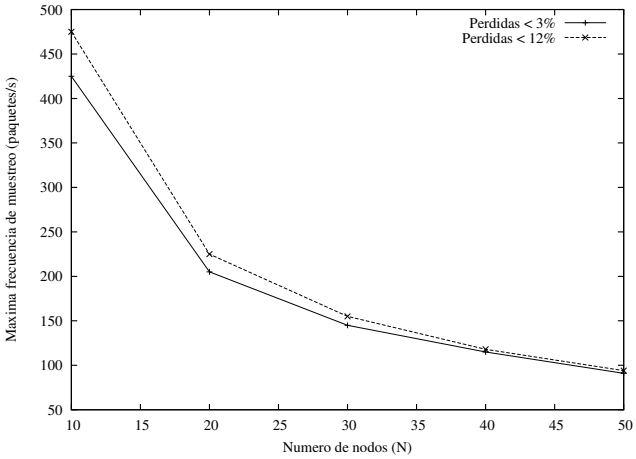


Figura 5. Frecuencia máxima de muestreo en función del número de sensores para obtener valores de pérdidas menores del 3 % y 12 %

Podemos distinguir en ambas figuras dos zonas de trabajo bien diferenciadas: zona de baja carga, donde la red es capaz de adsorber el incremento de carga que se produce con el aumento de la frecuencia de muestreo y zona de saturación dónde los valores de retardo y pérdidas de paquetes comienzan a subir de forma abrupta (exponencial en el retardo). El límite que separa ambas zonas se sitúa en torno a 90, 120, 150, 230 y 480 paquetes por segundo en la frecuencia de muestreo para 50, 40, 30, 20 y 10 sensores respectivamente. Con respecto al retardo podemos apreciar que en la zona de baja carga éste se sitúa por debajo de 1ms, lo que permite sin duda su utilización en aplicaciones de control, ya que la frecuencia máxima de muestreo tratada (500 paquetes por segundo) implica un retardo de 2 ms. entre envío de paquetes. En la zona de saturación, el retardo hace inviable el uso de esta tecnología para este tipo de aplicaciones. Estos valores tan altos de retardo se explican porque la configuración por defecto de ciertos parámetros como el número máximo de reintentos o el tamaño del buffer se encuentran optimizados para el envío de datos sin requisitos de tiempo real, por lo que toman valores grandes que perjudican el retardo en beneficio de un menor número de paquetes perdidos (que se suelen retransmitir con TCP).

Las Figs. 5 y 6 muestran los valores límite en cuanto a número de sensores o estaciones y frecuencia de muestreo de las mismas a fin de conseguir un cierto valor de retardo y pérdidas de paquetes válidos para gran número de aplicaciones de control.

Tal y como se aprecia en la Fig. 6, en el caso del retardo, las diferencias entre valores son mínimas, ya que al entrar en zona de saturación el incremento de retardo es muy grande.

III-B. Estudio del Consumo de Energía de la interfaz WiFi

Los dispositivos 802.11 consumen energía tanto en estado de transmisión como en el estado de escucha y en el de recepción de información. El consumo de energía del interfaz WiFi de un nodo (sensor) se muestra en la Fig. 7, donde se puede apreciar un incremento lineal del consumo en la zona de baja carga de tráfico. Las distintas pendientes en función del número de dispositivos (N desde 10 hasta 50) se explican por el hecho de que cuantas más estaciones mayor número de tramas 802.11 debe decodificar una estación (correspondientes

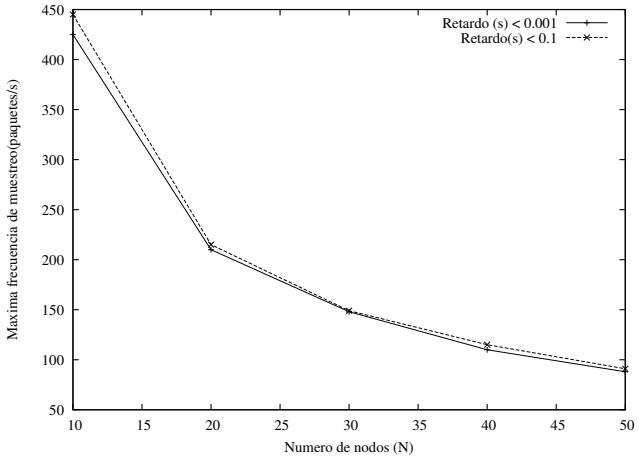


Figura 6. Frecuencia máxima de muestreo en función del número de sensores para obtener valores de retardo menores que 0.1 s. y 1 ms.

al tráfico del resto de las estaciones). Al llegar a la zona de saturación el número de tramas enviadas se estabiliza en torno al caudal del tráfico en saturación, por lo que la energía consumida ya no se incrementa a pesar de que el tráfico ofrecido sea mayor.

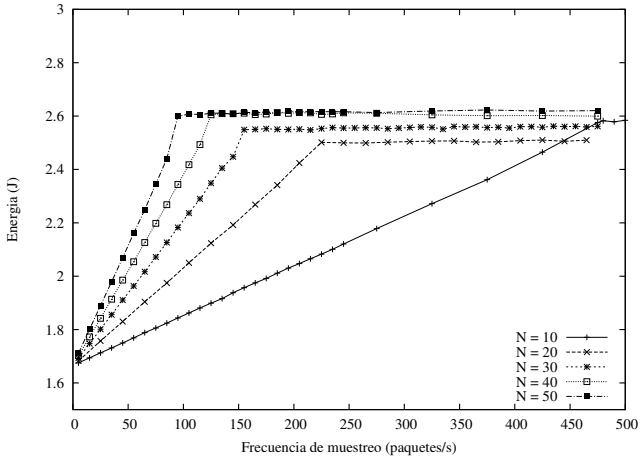


Figura 7. Consumo de energía del interfaz WiFi en función de la frecuencia de muestreo de los sensores para diferente número de sensores

Se puede apreciar en la Fig. 7 que conforme se acerca a la zona de saturación la pendiente se incrementa ligeramente, lo que se explica por el incremento en el número de retransmisiones.

III-C. Influencia del Tamaño del Buffer

En los resultados anteriores se puede apreciar cómo el retardo sube bruscamente al entrar en la zona de saturación debido a que el tamaño del buffer utilizado en el nivel de aplicación permitía un gran número de paquetes en cola (para 40 bytes/paquete permitía hasta 800 paquetes). A fin de evaluar el efecto que un buffer de menor tamaño tiene en los parámetros: retardo, tasa de pérdidas de paquetes y energía consumida, se ha reducido el tamaño del buffer de 256.000 bits a 19.200 bits (lo que permite un máximo de 60 paquetes en cola). Los resultados se muestran en la Figs. 8 y 9. Como cabe esperar, los retardos de saturación han disminuido notablemente (casi un orden de magnitud) con respecto al caso de colas grandes.

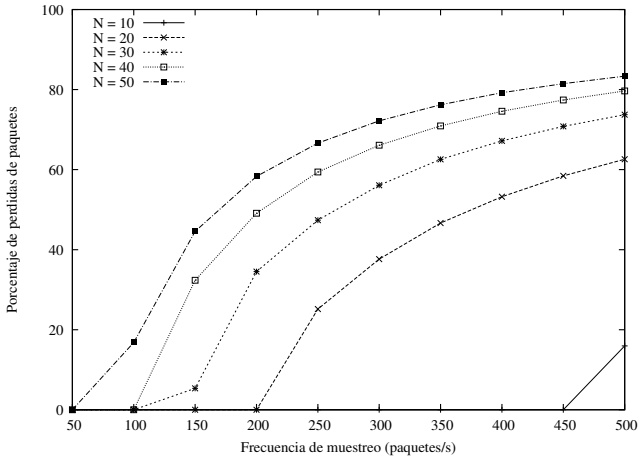


Figura 8. Porcentaje de pérdidas de paquetes en función de la tasa de muestreo para diferente número de sensores

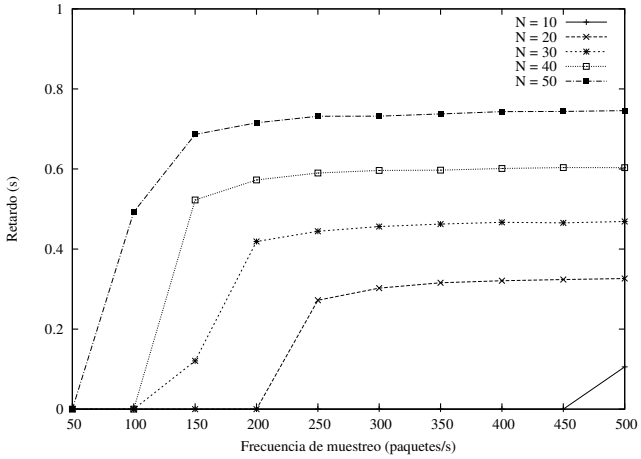


Figura 9. Retardo sufrido por los paquetes en función de la tasa de muestreo para diferente número de sensores

Contrariamente a lo que ocurre con el retardo, la tasa de pérdidas de paquetes se mantiene aproximadamente igual, resultado que aparentemente no tiene sentido. Sin embargo dicho resultado puede explicarse debido a que el tráfico inyectado a la red es de tasa constante, por lo que el efecto de un buffer en régimen permanente es nulo. El buffer puede acomodar pequeñas diferencias entre tráfico ofrecido y tráfico que puede cursar la red durante un breve periodo de tiempo, pasado el cual las pérdidas aparecen irremediablemente. Por ello podemos concluir que para aplicaciones de control industrial el tamaño de los buffer de nivel de aplicación debe ser muy reducido, estando en consonancia con el máximo número de retransmisiones permitido en la red.

Sin embargo, tal y como se aprecia en la Fig. 10, el consumo de energía cuando el tamaño del buffer es pequeño presenta un comportamiento similar al que registran tamaños de cola grandes, pues el consumo en saturación y zona de baja carga resultan aproximadamente igual en ambos casos.

No obstante, aparece una diferencia grande en la zona de comienzo de la saturación. En el caso de buffer de pequeño tamaño no existe un incremento de la pendiente cuando nos acercamos a la zona lineal.

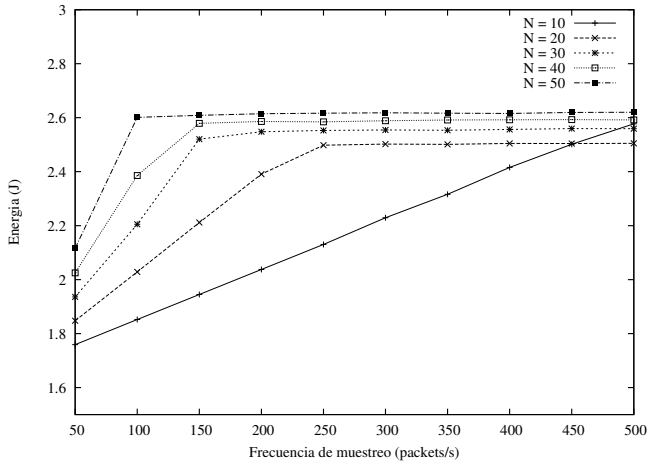


Figura 10. Consumo de energía del intefaz WiFi en función de la frecuencia de muestreo para diferente número de sensores

III-D. Influencia del Tamaño de los paquetes

El tamaño de los paquetes es un parámetro crucial para el rendimiento de un sistema 802.11. Paquetes pequeños disminuirán el retardo de acceso al medio pero impedirán un buen aprovechamiento del canal. Contrariamente, paquetes de gran tamaño aprovecharán al máximo el canal (desplazando el punto de saturación hacia mayores tasas de muestreo) pero incrementarán el retardo de acceso. En las aplicaciones de control el tamaño de los paquetes es normalmente pequeño y (del orden de 40 bytes) pues se utiliza para enviar el valor de una o varias variables de control con sus correspondientes marcas de tiempo. Además, el tamaño de los paquetes suele ser constante, lo que favorece el rendimiento del canal.

En las Figs. 11-14 podemos ver el retardo y la tasa de pérdidas para N=10 y 50 sensores para diversos valores de la frecuencia de muestreo, tomando siempre tres puntos de referencia: uno en zona de baja carga, uno en zona de transición hacia la saturación y otro en zona de saturación.

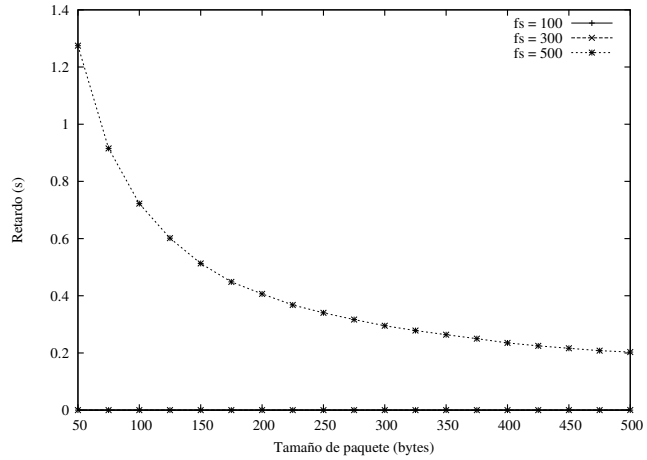


Figura 11. Retardo en función del tamaño del paquete para $N = 10$

El tamaño de los paquetes también tiene una influencia notable en el consumo de energía de la interfaz WiFi. En la Figs. 15-18 se puede apreciar cómo varía el consumo de energía en una estación (sensor) para distintos valores de tamaño del paquete y número de sensores.

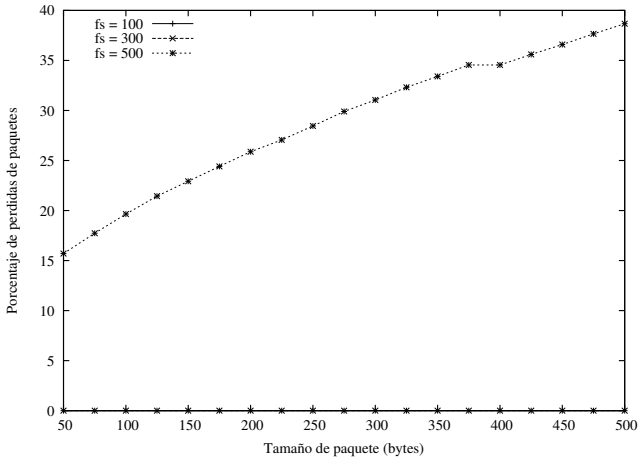


Figura 12. Porcentaje de pérdidas en función del tamaño del paquete para N=10 sensores

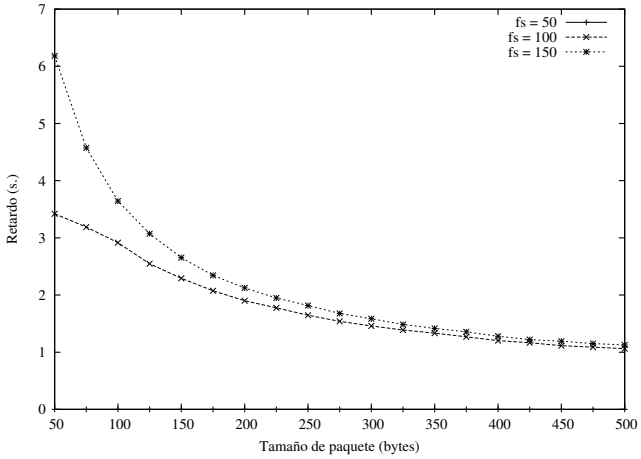


Figura 13. Retardo en función del tamaño del paquete para N=50 sensores

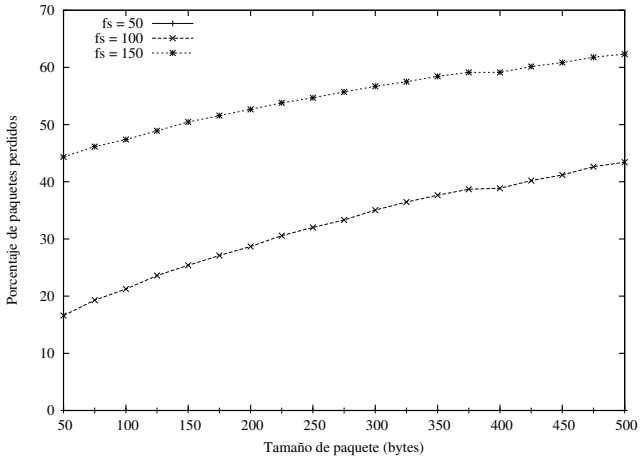


Figura 14. Porcentaje de pérdidas en función del tamaño del paquete para $N = 50$ sensores

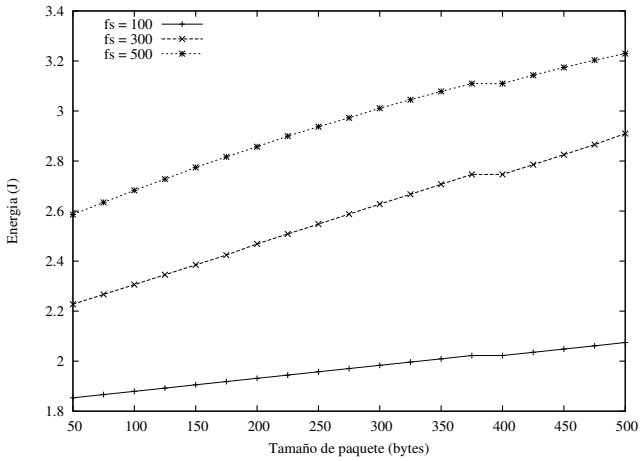


Figura 15. Energía en función del tamaño del paquete para $N = 10$ sensores

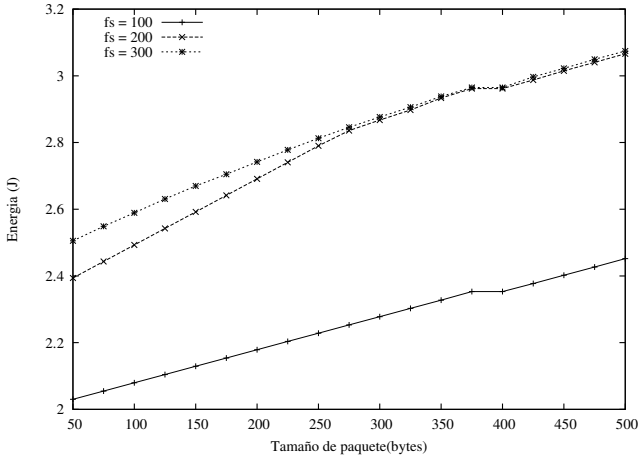


Figura 16. Energía en función del tamaño del paquete para $N = 20$sensores

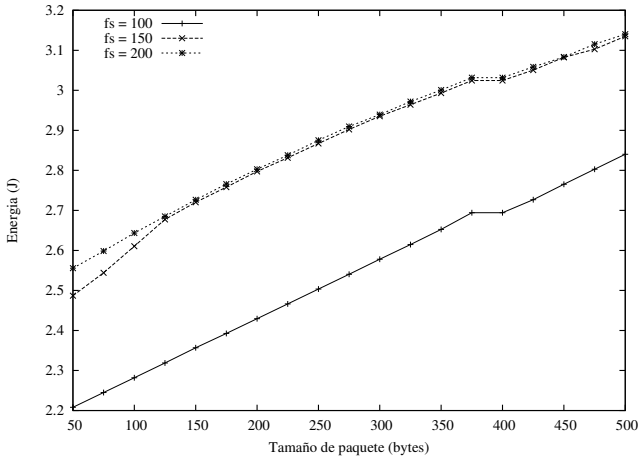


Figura 17. Energía en función del tamaño del paquete para $N = 30$ sensores

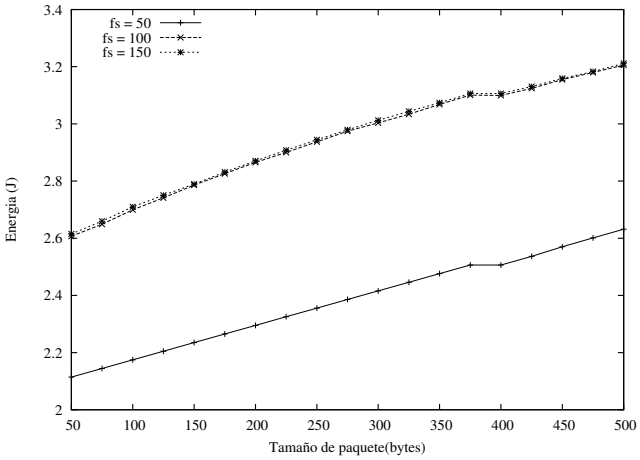


Figura 18. Energía en función del tamaño del paquete para $N = 50$ sensores

Teniendo en cuenta que la carga útil transmitida en las gráficas anteriores se multiplica por 10 (de 50 a 500 bytes/paquete), podemos apreciar cómo el consumo de energía por byte transmitido se reduce drásticamente cuando incrementamos el tamaño de los paquetes. En el caso de N=10 terminales vemos que el incremento en la energía consumida por terminal para ambos casos (50 y 500 bytes/paquete) se sitúa entre un 10 % para zona de baja carga ($f_s = 100$) y un 24 % en zona de saturación ($f_s = 500$). Para un número de terminales mayor ($N = 50$), el incremento de energía sería entorno al 24 % tanto en zona de saturación como en baja carga. Se puede observar también que el incremento en el tamaño del paquete anticipa el punto de saturación de la energía consumida tanto más cuanto mayor es el número de terminales. Esto resulta lógico, pues la energía gastada en recibir paquetes de otros terminales se incrementa con el tamaño del paquete.

IV. RESPUESTA EN UN SISTEMA DE CONTROL PROPORCIONAL DE PRIMER ORDEN

Se pretende aplicar en el escenario bajo estudio un sistema de control de primer orden con control proporcional. En la Fig. 19 se puede apreciar el modelo equivalente en MATLAB, donde la referencia a conseguir es $r = 10$, los valores de A, B, C y D escalares son de 0.8, 1, 0.16 y 0.2 respectivamente, lo que equivale a la función de transferencia inestable $G(z) = -0{,}1z/(z-1{,}1)$. La constante de proporcionalidad K vale -2 en nuestro caso y el sistema en estado inicial $x(0)$ es igual a 0.

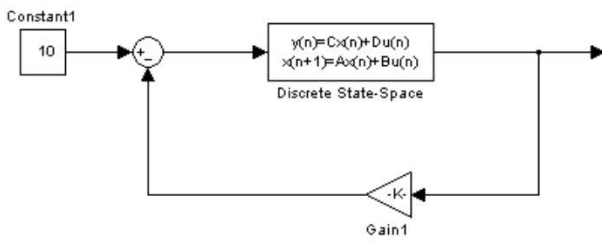


Figura 19. Modelo equivalente del sistema de control

La Fig.20 refleja la evolución del sistema cuando se ejecuta el control para $N = 30$ en la zona de baja carga ($f_s = 50$) y en

la zona de saturación ($f_s = 300$). En el primer caso (retardo ¡0.1), se puede apreciar como el sistema tiende a la referencia $r = 10$, mientras que en el segundo caso el sistema evoluciona hacia infinito. En el Nodo de Control implementado el tiempo de ejecución de las ecuaciones del sistema es de $0{,}001s$. Para distintos valores de N se obtienen resultados similares,

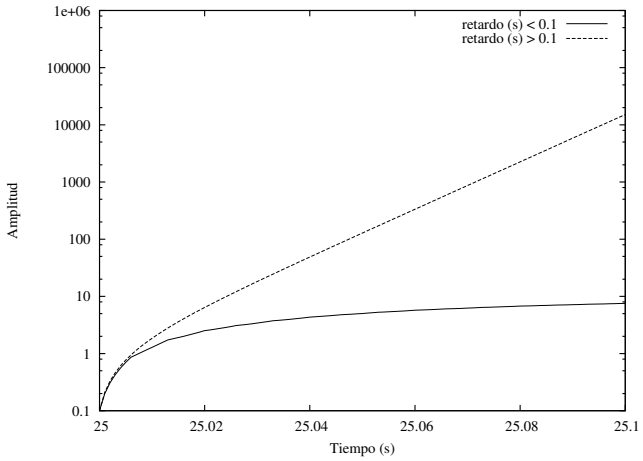


Figura 20. Respuesta temporal del sistema de control

distinguiéndose claramente una buena calidad de control en la zona de baja carga y un pésimo control en la zona de saturación. Estos resultados tan dispares se explican por el gran tamaño de cola utilizado en la simulación.

V. CONCLUSIONES Y LÍNEAS DE AVANCE

Las aportaciones realizadas por este trabajo suponen un primer avance en la línea del control de sistemas utilizando redes con tecnología 802.11 para la transmisión de información entre sensores y controlador. En el trabajo se realiza una adaptación del simulador OPNET para la ejecución de simulaciones en el campo WNCS, basada en la programación de tres nuevos módulos orientados al control de procesos y cómputo de energía. Las redes 802.11 presentan multitud de parámetros que influyen en la eficiencia, como el tamaño de cola, tamaño de paquete, este trabajo analiza el comportamiento de la red en el entorno de trabajo del control de procesos, delimitando los valores de retardo, pérdidas y consumo de energía para diverso número de sensores y frecuencias de muestreo de los mismos. También se presentan curvas que pueden ser utilizadas para el dimensionamiento, pues definen el máximo número de sensores posibles en función de la frecuencia de muestreo para ciertos valores de retardo y pérdidas.

Del análisis realizado puede concluirse que para el control de procesos el tamaño del buffer de aplicación debe ser pequeño si se quiere utilizar el control en zona de saturación; esto además permite reducir los consumos de energía en la zona cercana a la saturación. El tamaño de los paquetes afecta de forma severa al consumo de energía por lo que habría que intentar diseñar algoritmos de control que permitieran la llegada de varias muestras en el mismo paquete a fin de permitir un mayor número de sensores asociados a un punto de acceso. Por último, el consumo de energía depende en gran medida del número de sensores, debido principalmente al gasto en recepción de tramas pertenecientes a otras estaciones, lo que sugiere del uso de mecanismos a nivel de aplicación para poner los terminales en modo *sleep* entre el envío de dos tramas consecutivas. Como última conclusión podemos señalar que es posible utilizar OPNET para simular sistemas de control mediante redes 802.11 y que la implementación realizada resulta eficiente, pues el incremento en el tiempo de simulación no se incrementa significativamente.

Como líneas de avance se pueden plantear futuras investigaciones en el campo de optimización energética conjunta, diseñando estrategias de control que permitan minimizar el consumo para conseguir cierto nivel de calidad en la respuesta del sistema. Algunas de esas estrategias pasan por controlar algunos parámetros claves en el rendimiento de 802.11 como son: el tamaño de ventana de contienda, el número de reintentos, la tasa de transmisión o la potencia de transmisión. El uso de sensores con distintas frecuencias de muestreo (caso heterogéneo) también plantea importantes líneas de avance, así como un estudio a mayor nivel de profundidad de los tamaños de cola en el nivel de aplicación y los modelos matemáticos que definen el comportamiento del sistema en la zona cercana a la saturación, lo que permitiría el co-diseño de estrategias de control que tuvieran en cuenta parámetros de red. Por último es posible ampliar el tipo de sistemas dinámicos y leyes de control implementadas.

AGRADECIMIENTOS

Este trabajo ha sido financiado en parte gracias al proyecto CICYT DPI2007-64697, y al proyecto European Commission (EC) (FeedNetBack Project, grant agreement 223866).

REFERENCIAS

[1] A. Willig, K. Matheus, and A. Wolisz, "Wireless technology in industrial networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, 2005.

[2] F. De Pellegrini, D. Miorandi, S. Vitturi, and A. Zanella, "On the use of wireless networks at low level of factory automation systems," *IEEE Transactions on Industrial Informatics*, vol. 2, no. 2, pp. 129–143, 2006.

[3] H. Zhai, X. Chen, and Y. Fang, "How well can the IEEE 802.11 wireless LAN support quality of service?" *IEEE Transactions on Wireless Communications*, vol. 4, no. 6, pp. 3084–3094, 2005.

[4] D. Malone, K. Duffy, and D. Leith, "Modeling the 802.11 distributed coordination function with heterogenous finite load," in *Workshop on Resource Allocation in Wireless Networks, Trento, Italy*. Citeseer, 2005.

[5] E. Ziouva and T. Antonakopoulos, "CSMA/CA performance under high traffic conditions: throughput and delay analysis," *Computer Communications*, vol. 25, no. 3, pp. 313–321, 2002.

[6] M. Ergen and P. Varaiya, "Decomposition of energy consumption in ieee 802.11," in *IEEE International Conference on Communications, 2007. ICC'07*, 2007, pp. 403–408.

[7] S. Chang, W. Stark, and A. Anastasopoulos, "Energy-delay analysis of MAC protocols in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 2841–2845, 2008.

[8] M. Carvalho, C. Margi, K. Obraczka, and J. Garcia-Luna-Aceves, "Modeling energy consumption in single-hop IEEE 802.11 ad hoc networks," in *Thirteenth International Conference on Computer Communications and Networks (ICCCN'04)*. Citeseer, 2004.

[9] G. Bianchi and I. Tinnirello, "Kalman filter estimation of the number of competing terminals in an IEEE 802.11 network," in *IEEE INFOCOM*, vol. 2. Citeseer, 2003, pp. 844–852.

[10] A. Panousopoulou, G. Nikolapoulos, and A. Tzes, "Experimental controller tuning and QoS optimization of a wireless transmission scheme for real-time remote control applications," in *2004 IEEE International Conference on Industrial Technology, 2004. IEEE ICIT'04*, vol. 2, 2004.

[11] M. Andersson, D. Henriksson, A. Cervin, and K. Arzen, "Simulation of wireless networked control systems," in *44th IEEE Conference on Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC'05*, 2005, pp. 476–481.

Sistemas Avanzados de Reputación para Redes Móviles Ad-hoc Cooperativas

Alberto Rodriguez-Mayol, Javier Gozalvez
Ubiquitous Wireless Communications Research Laboratory
Uwicore, http://www.uwicore.umh.es
Universidad Miguel Hernández
Avda. de la Universidad s/n, 03202, Elche (España)
f.rodriguez@umh.es, j.gozalvez@umh.es

***Resumen*- MCN-MR (*Multi-hop Cellular Network – Mobile Relay*) es una novedosa tecnología que ha sido propuesta para ser empleada en los sistemas *Beyond 3G* o *4G* por su capacidad para proporcionar homogeneidad en la calidad de servicio de toda el área de cobertura. Para ello, es necesario que los nodos cooperen en la retransmisión de los paquetes de otros usuarios, dado que el egoísmo de los nodos puede tener un efecto muy perjudicial en la conectividad *multi-hop* de las redes MCN-MR. En trabajos anteriores se han propuesto distintos tipos de protocolos basados en reputación para contrarrestar el egoísmo de los nodos en redes móviles *ad-hoc*. Sin embargo, la evaluación de su rendimiento en condiciones realistas de simulación demuestra que tienden a sobrestimar el comportamiento egoísta de los nodos. De esta forma, la disponibilidad de rutas *multi-hop* válidas se ve reducida. En este contexto, este trabajo propone y evalúa dos técnicas que corrigen el funcionamiento inexacto de la técnica *watchdog* empleada para observar el comportamiento de los nodos.**

***Palabras Clave*- Redes celulares *multi-hop*; egoísmo; técnicas basadas en reputación; *watchdog*; MANET**

I. INTRODUCCIÓN

Una de las características más distintivas y exigentes de las futuras redes *Beyond 3G* será la provisión de niveles homogéneos de Calidad de Servicio (QoS, *Quality of Service*) en toda el área de cobertura [1]. Las redes celulares convencionales han alcanzado una cobertura universal, pero son incapaces de proporcionar niveles homogéneos de QoS en toda el área de la celda y velocidades de transmisión altas en zonas alejadas de la estación base (BS, *Base Station*), debido al decrecimiento exponencial del nivel de señal con la distancia. Para superar esta limitación, los operadores pueden aumentar la densidad de BS, que a su vez incrementaría la complejidad de la planificación y el coste de despliegue y mantenimiento de la red, además del rechazo social existente en contra de la instalación de nuevos emplazamientos de antenas. Por otro lado, se ha propuesto un nuevo paradigma de redes de comunicaciones, denominadas *Multi-hop Cellular Networks* (MCN) [2], que combinan las transmisiones en modo *ad-hoc* y en modo celular, para incrementar las tasas de transmisión y proporcionar niveles de QoS homogéneos en toda la celda. En las redes MCN, las transmisiones celulares de un solo salto de larga distancia son sustituidas por una combinación de múltiples transmisiones *ad-hoc* y una última conexión celular de corta distancia con la BS. La transmisión en modo *multi-hop* celular permite extender las altas tasas de transmisión de las proximidades de la BS a las zonas del borde de la celda, además de mejorar la capacidad, la cobertura y la utilización de la energía [3].

Se han identificado dos modalidades de redes MCN. En la modalidad de retransmisión fija (MCN-FR, MCN-*Fixed Relay*), se emplean estaciones repetidoras fijas para reducir la distancia de retransmisión entre la BS y los usuarios situados en el borde de la celda. Para alcanzar el rendimiento esperado, las antenas retransmisoras deben estar situadas en emplazamientos con buenas condiciones de propagación con la BS, especialmente de visibilidad directa (LOS, *Line Of Sight*). Las redes MCN-FR tienen una complejidad de diseño relativamente baja, pero requieren la instalación de nuevas antenas con el consecuente coste económico y social [3]. Por otro lado, las redes de retransmisión móvil (MCN-MR, MCN-*Mobile Relay*) tienen una mayor flexibilidad, dado que emplean los equipos de los usuarios (UE, *User Equipment*) como estaciones retransmisoras. Sin embargo, deben superarse ciertos desafíos para conseguir los beneficios esperados de las redes MCN-MR. Uno de estos desafíos es asegurar la cooperación de los usuarios en el proceso de retransmisión de los paquetes [4]. El comportamiento egoísta de los nodos puede estar motivado por distintas causas, tales como el agotamiento de la batería del terminal, la sobrecarga en el canal, la desconfianza hacia la tecnología MCN-MR, etc. y puede provocar un importante deterioro del rendimiento de la red. En este contexto, el objetivo de los protocolos de prevención de egoísmo (SPP, *Selfishness Prevention Protocols*) es incentivar a los nodos a cooperar en las funciones de la red y evitar los ataques intencionados de nodos maliciosos.

Trabajos anteriores en el área de redes MANET (*Mobile Ad-hoc NETworks*) han abordado el problema del descarte de paquetes, en el que algunos nodos se niegan a retransmitir los paquetes originados por otros nodos, incluso después de haber accedido a retransmitirlos en la fase de búsqueda y establecimiento de rutas *multi-hop* [5]. En [5] se establecen tres grupos para categorizar las diferentes estrategias de SPP propuestas en la literatura: basadas en reputación, basadas en crédito y basadas en teoría de juegos. Las estrategias basadas en crédito utilizan una moneda real o virtual para pagar por la retransmisión de los paquetes realizada por otros nodos. El crédito se utiliza para compensar la utilización de los recursos de otros nodos en el proceso de retransmisión, y puede ser obtenido retransmitiendo los paquetes de otros nodos o simplemente se puede comprar con una moneda real. Algunas de las desventajas de los esquemas basados en crédito son la

falta de escalabilidad, la necesidad de una entidad central confiable o de un hardware de seguridad a prueba de ataques y falsificaciones [5]. Por otro lado, los modelos de teoría de juegos empleados en SPPs simulan un juego en el que cada nodo puede escoger retransmitir o no los paquetes de otros nodos en función de distintos parámetros. Permiten estudiar de manera analítica la estabilidad de los puntos de equilibrio y de las soluciones a los problemas planteados con diferentes estrategias. Sin embargo, muchas propuestas basadas en teoría de juegos no reflejan adecuadamente la influencia de algunos parámetros importantes de los sistemas reales. Alternativamente, en el presente trabajo se emplean protocolos basados en reputación, que por lo general emplean la técnica *watchdog* propuesta en [6] para observar el comportamiento de otros nodos, que será explicada más adelante. Estas observaciones se registran en una tabla de reputación que cuantifica la predisposición de cada nodo conocido a cooperar en la retransmisión. La información de la tabla de reputación se emplea en el proceso de descubrimiento y establecimiento de ruta para seleccionar una ruta sin nodos egoístas. Los esquemas de reputación son completamente distribuidos y obtienen un buen rendimiento de red [4]. Sin embargo, un estudio previo [7] mostró que la evaluación de los esquemas de reputación en condiciones de simulación simplistas puede proporcionar resultados inexactos y demasiado optimistas sobre su funcionamiento y rendimiento. En particular, [7] demostró la importancia del impacto sobre el rendimiento esperado de las técnicas SPP basadas en reputación de factores como las condiciones de propagación radio y la posible sobrecarga del canal. Tomando como punto de partida estas observaciones, en este trabajo se proponen dos nuevas estrategias para mejorar el rendimiento de esquemas basados en reputación en redes MCN-MR y se evalúa su funcionamiento en un escenario realista de simulación.

El resto del trabajo se estructura del siguiente modo. Los protocolos basados en reputación se presentan en la sección II, así como una descripción de la técnica *watchdog*. La sección III presenta las mejoras propuestas en este estudio. La sección IV introduce la plataforma de simulación implementada y la sección V discute el rendimiento conseguido con las técnicas propuestas. Finalmente, las conclusiones se presentan en la sección VI.

II. Protocolos de Prevención de Egoísmo Basados en Reputación

Los SPPs empleados para contrarrestar los ataques de descarte de paquetes tienen como objetivo detectar y aislar a los nodos egoístas para incentivarlos a cooperar. Los métodos basados en reputación se componen de dos módulos: detección y reacción. El módulo de detección de cada nodo vigila el comportamiento de otros nodos, es decir, si transmiten o no los paquetes que deben retransmitir, usando el mecanismo *watchdog* de detección explicado en la siguiente sección II.A. El módulo de reacción mantiene una tabla de reputación donde a cada nodo se le asigna un nivel de reputación basado en las observaciones del módulo de detección. La información de dicha tabla se emplea en el protocolo de enrutamiento para evitar y aislar a los nodos egoístas conocidos en futuros establecimientos de ruta. En la literatura se han propuesto otros métodos de detección de egoísmo, tales como el protocolo TWOACK [8], o el sistema propuesto en [9]. TWOACK propone que la retransmisión correcta de cada paquete sea confirmada al nodo precursor por parte del nodo sucesor mediante el envío de un paquete ACK (*ACKnowledgment*) de confirmación hacia atrás a través del nodo retransmisor (ver Figura 1). Esta estrategia introduce una sobrecarga de comunicación muy alta por la necesidad de confirmar cada paquete. Mediante otro enfoque, [9] plantea que los mensajes ACK empleados en protocolos como TCP (*Transmission Control Protocol*) para la confirmación extremo a extremo de la correcta transmisión de un paquete se utilicen para vigilar el comportamiento de los nodos. Sin embargo, dicho sistema no permite distinguir cuál es el nodo egoísta entre todos los que participan en una ruta *multi-hop* sospechosa. Por ello, en este trabajo se ha escogido como técnica de detección el sistema *watchdog*.

A. Técnica de detección watchdog

La técnica de detección *watchdog* [6] se basa en la confirmación pasiva de la retransmisión de los paquetes mediante la observación de los paquetes transmitidos por el nodo retransmisor, como se muestra en la Figura 1.

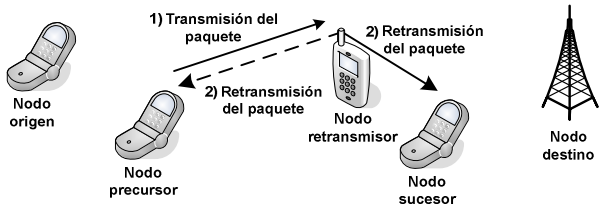


Fig. 1. Funcionamiento de la técnica de detección *watchdog*.

En la Figura 1, el nodo origen ha establecido una ruta *multi-hop* hacia el nodo destino para transmitir sus paquetes de datos. La ruta se ha establecido empleando un protocolo de enrutamiento *multi-hop* cualquiera. Los paquetes de datos se transmiten de manera consecutiva salto por salto siguiendo la secuencia *nodo origen – nodo precursor – nodo retransmisor – nodo sucesor – nodo destino*. En la figura, un paquete se transmite primero desde el nodo precursor al nodo retransmisor. En el nodo precursor, un buffer de paquetes almacena una copia temporal del paquete transmitido, que debe ser retransmitido por el nodo retransmisor. A cada paquete almacenado se le asigna un '*timeout* de paquete', que marca el tiempo máximo que puede tardar el nodo retransmisor en transmitir el paquete. En caso de que dicha transmisión se realice en el tiempo establecido y sea escuchada por el nodo precursor, se asume que el nodo retransmisor ha cooperado correctamente, lo cual se conoce como una 'detección de retransmisión'. El nodo precursor busca la copia del paquete escuchado en el buffer y la borra. En caso de que el paquete retransmitido no sea escuchado correctamente por el nodo precursor dentro del tiempo establecido, entonces se supone que el nodo retransmisor ha actuado de manera egoísta, es decir, que ha descartado el paquete. Esto se conoce como una 'detección de descarte'. Dependiendo del tipo de SPP, las detecciones de descarte y de retransmisión modifican el nivel de reputación del nodo en la tabla del nodo precursor. Un parámetro importante en el proceso de detección *watchdog* es el *timeout* de paquete, que es el tiempo máximo establecido para que el nodo retransmisor retransmita el paquete. El valor de este parámetro no está especificado en el trabajo [6]. Un valor

demasiado grande del *timeout* de paquete incrementa el tiempo necesario para detectar a los nodos egoístas, y por tanto aumenta la cantidad de paquetes que estos nodos descartan antes de ser detectados, mientras que un valor demasiado pequeño puede impedir que los nodos no egoístas tengan tiempo suficiente para llevar a cabo la retransmisión. Para ajustar correctamente este parámetro, los autores llevaron a cabo algunas simulaciones preliminares. Los resultados obtenidos mostraron que la mayoría de los paquetes eran correctamente retransmitidos 50ms después de que el nodo precursor los transmitiera. Por consiguiente, el *timeout* de paquete fue fijado en 50ms en el presente trabajo. Otro parámetro definido en la implementación de la técnica *watchdog* en este trabajo es el intervalo de comprobación de buffer, que representa el intervalo entre instantes consecutivos en los cuales se rastrea el buffer y se borran aquellos que hayan caducado durante el intervalo anterior, actualizando consecuentemente la tabla de reputación. Este parámetro se ha fijado a 25ms, de acuerdo a resultados obtenidos en simulaciones previas de optimización.

La técnica *watchdog* de detección se utiliza en la mayoría de los SPPs basados en reputación. Sin embargo, tal y como los autores demostraron en [7], los errores de propagación radio y las colisiones de paquetes debidas a la sobrecarga en el canal pueden deteriorar notablemente el rendimiento de la técnica *watchdog* y su capacidad para detectar con exactitud a los nodos egoístas. En el ejemplo de la Figura 1, las colisiones en los paquetes podrían impedir que el nodo precursor observara correctamente la retransmisión del paquete por parte del nodo retransmisor. La referencia [9] aduce que las colisiones de paquetes no afectan notablemente a la capacidad de detección de *watchdog*, incluso con una carga de tráfico muy alta. Sin embargo, esta conclusión fue extraída a partir de un *testbed* con 4 nodos, lo cual puede limitar la generalidad de esta afirmación. En caso de que el nodo precursor no escuche la retransmisión del paquete, registrará una detección de descarte incorrecta. Si persisten de manera repetida las detecciones de descartes incorrectas hacia un nodo determinado, será acusado incorrectamente de comportarse egoístamente, por lo cual será evitado en futuros establecimientos de ruta, además de ser aislado y penalizado en la retransmisión de sus propios paquetes. Las acusaciones incorrectas además reducen la disponibilidad de rutas seguras, ya que algunas de las rutas que son descartadas por contener algún nodo supuestamente egoísta son en realidad rutas válidas. Por rutas seguras se entiende aquellas rutas que se suponen válidas porque en ellas no participa ningún nodo que haya sido acusado previamente de egoísta. En este contexto, este trabajo presenta dos mejoras aplicables a cualquier SPP que emplee la técnica de detección *watchdog* con el objetivo de reducir el número de acusaciones incorrectas para mitigar sus efectos negativos.

B. Protocolo de prevención de egoísmo de Marti

El SPP implementado en este trabajo fue propuesto por Marti [6]. El protocolo de Marti se compone de dos módulos: *watchdog* y *pathrater*, que pueden asimilarse a un módulo de detección y otro de reacción, respectivamente. En el módulo *watchdog*, cada nodo precursor usa la técnica *watchdog* para observar el comportamiento de los nodos retransmisores. El módulo *watchdog* cuenta el número de veces que un nodo retransmisor ha descartado paquetes. Cuando el número de detecciones de descarte supera un cierto umbral, denominado 'umbral máximo de faltas', el nodo retransmisor es acusado de egoísta. El valor exacto del umbral de faltas no fue especificado en [6]. Mientras que un valor demasiado alto del parámetro incrementa el número de paquetes que los nodos egoístas descartan antes de ser detectados, un valor demasiado bajo incrementa el número de acusaciones incorrectas hacia nodos no egoístas que son tomados por egoístas debido a los errores de propagación o a las colisiones de paquetes. Los autores realizaron simulaciones previas para encontrar un valor de compromiso entre ambas tendencias, escogiéndose finalmente el número 5. El *pathrater* en cada nodo usa la información proveniente del *watchdog* y del protocolo de enrutamiento para seleccionar aquella ruta con más probabilidad de ser confiable, es decir, aquella cuyos nodos tengan una mayor reputación promedio. El *pathrater* mantiene la tabla de reputación a partir de la información del *watchdog* y del protocolo de enrutamiento, para todos aquellos nodos con los que interacciona. Todos los valores numéricos de lo parámetros en esta implementación han sido escogidos de acuerdo a [6], excepto aquellos cuyo valor no había sido especificado en dicho trabajo, como se menciona en el texto. Cuando el *pathrater* detecta por primera vez a un nodo, le asigna de forma automática un nivel de reputación de 0.5. El *pathrater* incrementa la reputación de todos los nodos que participan en rutas activas en 0.01 en períodos fijos de 200ms. Este período se denomina 'intervalo de incremento de reputación'. Una ruta activa es aquella a través de la cual se ha recibido o transmitido un paquete durante el último intervalo de incremento de reputación. Se establecen dos distintas categorías de nodos: neutrales y egoístas. La máxima reputación que puede alcanzar un nodo neutral, es decir, que no ha sido acusado de actuar de manera egoísta, es 0.8. Por encima de ese valor, la reputación del nodo no es incrementada aunque así se tuviera que hacer según la regla de las rutas activas. La reputación de un nodo retransmisor del cual se detecta el descarte de un paquete se reduce en 0.05. El valor mínimo de la reputación de un nodo neutral es 0, valor que se mantiene mientras el nodo no pase a ser egoísta. Como se mencionó antes, un nodo es acusado de ser egoísta cuando supera el umbral máximo de faltas. Cuando un nodo es acusado de egoísta, su reputación se fija a un valor muy negativo, -100. Este nivel negativo se mantiene por un período de tiempo, el tiempo de aislamiento, cuyo valor no fue especificado en la implementación original, pero que en este trabajo se ha fijado a 500s. Después de este período, el aislamiento del nodo se desbloquea y su reputación vuelve a un valor de 0.5, para permitir que el nodo pueda optar por cooperar. El protocolo de Marti también introduce mensajes de acusación que permiten al nodo precursor advertir al nodo origen sobre la presencia de un nodo egoísta en la ruta. No obstante, estos mensajes pueden ser falsificados y además pueden aumentar la carga de señalización. Durante los procesos de descubrimiento y establecimiento de ruta, el protocolo de enrutamiento selecciona una ruta que no contenga nodos egoístas, según la tabla de reputación. Las peticiones de retransmisión de paquetes provenientes de nodos acusados de egoístas no son aceptadas por el *pathrater*.

III. Mecanismos de Mejora de SPP Basados en Reputación

Para mitigar los efectos negativos de la inexactitud de la técnica *watchdog* causada por errores en el canal radio o por colisiones de paquetes, este trabajo propone y evalúa dos mejoras de la técnica original de Marti que pueden ser adaptadas para aplicarse en cualquier SPP que utilice la técnica *watchdog* para la vigilancia de los nodos.

A. *Warning Mode* (WM)

El modo WM (*Warning Mode*) tiene como objetivo reducir el número de acusaciones falsas causadas por errores en el canal radio o por colisiones de paquetes. WM introduce una categoría intermedia, la de nodo 'sospechoso', entre un nodo marcado como neutral y un nodo marcado como egoísta. En la implementación original de Marti, cuando el nodo retransmisor, que está siendo observado por el nodo precursor, muestra un comportamiento egoísta durante un cierto período de tiempo, es acusado de egoísta directamente, y todos los enlaces en los cuales participa el nodo en cuestión son deshechos, dado que se supone que el nodo no va a retransmitir ninguno de los paquetes. No obstante, es importante señalar que estas acusaciones pueden ser incorrectas debido a errores de transmisión radio experimentados en el nodo precursor o en el nodo retransmisor. En este contexto, en el modo WM, cuando el número de faltas excede el umbral máximo de faltas, el nodo retransmisor se marca primero como sospechoso, y sus enlaces son temporalmente deshechos. Los nodos sospechosos pueden participar en las tareas de enrutamiento otra vez, dado que podría tratarse de una acusación incorrecta. Sin embargo, se aplican restricciones adicionales sobre los nodos sospechosos para evitar un aumento de los paquetes descartados por nodos egoístas reales. Específicamente, los nodos tratarán a los nodos sospechosos como si fueran nodos neutrales, con dos excepciones. En primer lugar, el *timeout* del que dispone el nodo para retransmitir el paquete se reduce en un factor α. En este trabajo, el factor α se ha fijado a 0.5, pero podría ser optimizado. Además, el número máximo de faltas se reduce a 1, en vez de 5, para los nodos sospechosos. De esta forma, si el nodo precursor detecta una única falta más por parte de un nodo sospechoso, lo acusará definitivamente de egoísta. Por otro lado, si un nodo precursor detecta que un nodo sospechoso coopera de nuevo, entonces su reputación se incrementa para darle la oportunidad de recuperarse del nivel previo de baja reputación, que puede haber sido provocado por errores radio o colisiones de paquetes.

Los potenciales beneficios de la técnica WM provienen del hecho de que los errores en el canal radio y las colisiones de paquetes pueden producir un incremento perjudicial del número de acusaciones incorrectas en la implementación original del protocolo de Marti. Las acusaciones incorrectas tienen muchos efectos negativos. Algunos nodos cooperativos son acusados y aislados de manera injusta. El aislamiento de nodos cooperativos les obstaculizará a la hora de encontrar rutas *multi-hop* hacia la estación base. Además, dado que los nodos egoístas son evitados en las rutas *multi-hop*, el número de rutas *multi-hop* potencialmente válidas se reduce erróneamente. Esto resulta en que algunas rutas *multi-hop* válidas serán infrautilizadas, mientras que otros nodos estarán sobrecargados por las peticiones de retransmisión de paquetes. Por el contrario, con la técnica WM, los nodos sospechosos tienen una oportunidad extra para recuperarse de una injusta mala reputación. En caso de que dicho nivel de reputación fuera provocado por colisiones de paquetes o por errores de transmisión radio, la participación de los nodos sospechosos se reestablece correctamente cuando las condiciones en el canal mejoran. En cambio, si el nodo sospechoso es realmente egoísta, el número de paquetes de datos adicionales que serán descartados será mínimo, dado que será detectado y aislado rápidamente debido a las condiciones de vigilancia estrictas establecidas en WM para los nodos sospechosos.

B. *Reset Failure Mode (RFM)*

El objetivo del modo RFM es el de contrarrestar las acusaciones incorrectas que pueden estar provocadas en el momento en que un enlace entre dos nodos se deshace debido a la movilidad de los nodos, al desvanecimiento o a otros efectos del canal radio. La capa MAC (*Medium Access Control*) es responsable de detectar las caídas de los enlaces e iniciar un proceso de 'caída de enlace', para informar al protocolo de enrutamiento. Sin embargo, antes de que el proceso se inicie, algunos de los paquetes transmitidos por el nodo precursor al nodo retransmisor pueden no haber sido retransmitidos correctamente por éste. Por consiguiente, las copias de los paquetes en el buffer de paquetes del nodo precursor caducarán, y la reputación del nodo retransmisor será injustamente rebajada.

En el modo RFM, si se detecta la caída de un enlace, se trata de restablecer la reputación inicial del nodo retransmisor implicado, pues su reputación puede haberse visto afectada por detecciones de descarte incorrectas. Para ello, la reputación del nodo se reajusta a 0.5, que es la reputación inicial asignada a un nodo que interacciona por primera vez con otro. Además, el número de faltas se reinicia a 0, dado que se supone que estas faltas han sido provocadas por la caída del enlace y no por el posible comportamiento egoísta del nodo. Por último, se borran las copias de los paquetes en el buffer del nodo precursor que están pendientes de ser retransmitidas por el nodo retransmisor, dado que éste no será capaz de retransmitirlas. Debe tenerse en cuenta que sólo se aplican estas reglas en el modo RFM cuando el nodo retransmisor es todavía un nodo neutral para el nodo precursor. Si es acusado de ser egoísta antes de que se dispare el proceso de 'caída de enlace', la reputación y las faltas del nodo retransmisor no son alteradas.

Un posible inconveniente de RFM es que la restauración de la reputación por caídas de enlaces puede incrementar la reputación de nodos egoístas verdaderos, es decir, que en verdad actúan egoístamente. Esto podría ocurrir en el caso de que se detecte una caída de enlace y que el nodo retransmisor implicado sea realmente un nodo egoísta que todavía no ha sido catalogado como tal. En este caso, la reputación del nodo se vería injustamente aumentada. No obstante, es importante notar que esto ocurre sólo en transmisiones *multi-hop* con enlaces con una vida media reducida, lo cual debería ser evitado empleando protocolos de enrutamiento *multi-hop ad-hoc* eficientes. Con estos protocolos eficientes, la vida media de los enlaces es mayor que el tiempo necesario para detectar el comportamiento egoísta de un nodo, en escenarios con una movilidad baja-media, en la cual las redes MCN con retransmisión móvil son más viables.

C. Coste y complejidad

Las propuestas WM y RFM son fáciles de implementer, puesto que solo requieren ligeras modificaciones de la implementación original del SPP que se ejecuta en paralelo. Además, RFM introduce un mínimo coste computacional, debido a la utilización de funciones sencillas como la restauración del nivel de reputación, el reseteo del número de faltas y el borrado de copias de paquetes en el buffer de paquetes. Sin embargo, es importante comentar que la técnica WM incrementa el número de establecimientos de ruta en aproximadamente un 40% en comparación con el protocolo original de Marti, y también por tanto la carga de señalización asociada al proceso de descubrimiento de rutas. Se podría conseguir una importante reducción de la carga de señalización de los procesos de enrutamiento inducida por la técnica WM incrementando el tiempo de aislamiento empleado para castigar a los nodos egoístas, lo cual se investigará en futuros trabajos.

IV. Plataforma de Evaluación

A. Escenario de simulación

Se han llevado a cabo simulaciones a nivel de sistema que emulan el funcionamiento de una red inalámbrica *multi-hop* empleando la plataforma de simulación ns2 y la extensión de *Rice Monarch Project* para redes móviles [11]. El entorno de simulación consiste en un escenario tipo Manhattan de 1350x1350m^2, en el cual los nodos se mueven siguiendo el modelo de *Random Walk Obstacle* [12] y que se comunican con la BS situada en el centro del escenario a través de transmisiones *multi-hop*. Los nodos se distribuyen de manera uniforme inicialmente. La densidad de los nodos es de 1 por cada 80 metros de calle, para asegurar el establecimiento de rutas *multi-hop*. Las sesiones de tráfico consisten en transmisiones de tráfico *web* con 5 páginas en promedio por sesión, un tiempo de lectura entre descargas consecutivas de páginas de 30s, 25 objetos por página y un tiempo entre paquetes de 0.028s, tal y como especifica [13]. Con objeto de demostrar los efectos de posibles situaciones de sobrecarga en el canal, un 15% de los nodos en promedio mantiene sesiones activas de tráfico simultáneamente. El interfaz radio *ad-hoc* empleado es el del estándar 802.11a en la banda de 5.8GHz con un nivel de potencia de transmisión de 17dBm.

B. Protocolo de enrutamiento

La comunicación *multi-hop ad-hoc* entre los nodos y la BS se establece utilizando el estándar para redes *mesh* del IEEE 802.11s [14]. El protocolo HWMP (*Hybrid Wireless Mesh Protocol*) es el protocolo de enrutamiento obligatorio definido en el estándar, aunque se especifica que los proveedores pueden optar por operar también usando protocolos alternativos. HWMP combina el protocolo de enrutamiento reactivo AODV (*Ad-hoc On-demand Distance Vector*) [15] con un protocolo de enrutamiento proactivo en árbol. Para evitar una excesiva carga de señalización provocada por la utilización de un protocolo proactivo en un entorno móvil, en este trabajo se ha empleado una versión modificada del protocolo AODV que se comenta a continuación.

El protocolo de enrutamiento AODV solamente busca y establece una ruta cuando un nodo tiene datos para transmitir y no conoce la ruta hacia el nodo destino. En este caso, envía mensajes RREQ (*Route REQuest*) en modo *broadcast*, que son a su vez difundidos por sus nodos vecinos. Cuando el nodo destino recibe el mensaje RREQ, responde con un mensaje RREP (*Route REPly*) en modo *unicast* dirigido al nodo origen para confirmar el establecimiento de ruta. En el protocolo AODV original los nodos intermedios de la ruta, i.e. los nodos entre el nodo origen y el nodo destino, sólo procesan la primera de las réplicas del RREQ que reciben y descartan el resto de réplicas provenientes de rutas alternativas con una mayor latencia. Por consiguiente, la ruta *multi-hop* seleccionada entre el origen y el destino resulta ser la de menor latencia, que generalmente coincide con la que tiene menor número de saltos. En la versión implementada de AODV, los nodos intermedios pueden procesar múltiples réplicas de los mensajes de enrutamiento, para poder emplear la información de reputación en la métrica de selección de ruta. De esta manera, se procesan todos los paquetes y son aceptados aquellos que combinan una ruta libre de egoístas y con una menor latencia. Además, los mensajes de enrutamiento en la versión modificada de AODV incluyen la información de la identidad de todos los nodos participantes en la ruta, necesaria para averiguar si una ruta tiene nodos egoístas o no. Es importante señalar que estas características de la versión de AODV implementada están incluidas en el protocolo de enrutamiento DYMO (*Dynamic MANET On-demand*) [16], que es una versión mejorada del protocolo AODV.

C. Modelo de propagación radio

Para el cálculo del *pathloss* se emplea el modelo de canal para escenario urbano micro-celular propuesto en [17], que utiliza expresiones de *pahtloss* diferentes cuando existen condiciones de visibilidad (LOS *Line Of Sight*) o de no visibilidad (NLOS *Non Line Of Sight*) entre emisor y receptor. El modelo de propagación implementado modela de manera realista el canal radio, al considerar además los efectos del desvanecimiento lento y el desvanecimiento multicamino. El efecto de desvanecimiento multicamino, provocado por la recepción de múltiples réplicas de la señal transmitida en el receptor, se modela según una distribución Ricean en condiciones LOS y según distribución Rayleigh en condiciones NLOS. El desvanecimiento lento, provocado por obstáculos entre emisor y receptor, se modela con una distribución lognormal con una desviación estándar de 3dB y 4dB respectivamente para LOS y NLOS. Además, para la autocorrelación espacial característica del desvanecimiento lento se emplea el modelo de Gudmunson [18].

V. Evaluación de Resultados

Las propuestas de este trabajo tienen como fin mitigar los efectos negativos de la inexactitud del mecanismo de detección *watchdog* empleado por la mayoría de los SPPs basados en reputación, cuando se consideran condiciones realistas de simulación. Con las mejoras presentadas se disminuye el número de acusaciones incorrectas, lo cual incrementa el rendimiento general y la conectividad de la red, debido a la mayor disponibilidad de rutas *multi-hop* conocidas sin nodos egoístas.

La Figura 2 representa algunas estadísticas de rendimiento en cuanto a la recepción y al descarte de paquetes con las técnicas analizadas en este trabajo. El PDR (*Packet Delivery*

Ratio) es un parámetro del rendimiento de la red que mide el porcentaje de paquetes correctamente recibidos del total de paquetes transmitidos. Otros valores estadísticos son el porcentaje de paquetes descartados intencionadamente por nodos egoístas, el porcentaje de paquetes descartados por la inexistencia de rutas sin nodos egoístas conocidos y descartados por caídas de enlaces. Cada grupo de barras en la Figura 2 corresponde a un porcentaje diferente de nodos egoístas. Cada una de las tres barras dentro de un grupo corresponde a una técnica diferente (Marti, RFM y WM). Los números inscritos en el gráfico indican el porcentaje de incremento del PDR conseguido por las propuestas, comparado con el conseguido por la técnica original de Marti. La capacidad para distinguir con exactitud los nodos egoístas de los cooperativos con las técnicas propuestas permite obtener un incremento notable del PDR. Esto se debe al incremento del número de rutas válidas disponibles, especialmente en el caso de la propuesta WM. El incremento del número de rutas válidas disponibles con las técnicas propuestas puede apreciarse en el descenso del porcentaje de paquetes descartados debido a la inexistencia de rutas válidas conocidas ('Sin ruta' en la leyenda). El coste de esta mejora es un aumento leve de aproximadamente un 5% en el porcentaje de paquetes descartados por nodos egoístas en el modo WM. La razón de este incremento está implícita en el funcionamiento de la técnica WM. Cuando el comportamiento egoísta de un nodo retransmisor se detecta, primero se marca como un nodo sospechoso, antes de ser finalmente marcado como egoísta y aislado si continúa descartando paquetes durante el tiempo que esté marcado como sospechoso. No obstante, como se muestra en la Figura 2, el incremento en el número de paquetes descartados por los nodos egoístas, no tiene un gran impacto sobre el PDR. Además, debe señalarse que en los sistemas basados en reputación que utilizan la técnica *watchdog* para observar la retransmisión de los paquetes, la determinación del valor óptimo del umbral máximo de faltas constituye un compromiso entre la rapidez en la detección de nodos egoístas y la tasa de error de las acusaciones de egoísmo. Aunque en este trabajo el valor óptimo de dicho parámetro ha sido fijado mediante simulaciones preliminares, es inevitable que exista un cierto porcentaje de paquetes descartados, ya que la técnica de *watchdog* se basa precisamente en detectar esos descartes de paquetes. Además, un nodo egoísta que ha sido descubierto en una zona determinada del escenario de la red, puede esquivar el aislamiento aprovechándose de la movilidad de los nodos, cambiando su localización. Frente a estos inconvenientes inherentes a las redes MANET y los sistemas basados en *watchdog*, la reducción del porcentaje de paquetes descartados es un importante objetivo en el diseño de SPPs que será tenido en cuenta en futuros trabajos, a través de un mayor intercambio de información de reputación entre los distintos nodos de la red, que permita aislar a los nodos egoístas de manera efectiva.

El incremento del PDR con las técnicas propuestas se debe al descenso del número de acusaciones incorrectas y a la capacidad de seleccionar rutas *multi-hop* sin nodos egoístas. El número de acusaciones incorrectas, representado en la Figura 3(a), se refiere al número de ocasiones en las que un nodo retransmisor no egoísta fue acusado de actuar egoístamente debido a la acumulación de detecciones de descarte incorrectas provocadas por errores de propagación radio y colisiones de paquetes (ver sección II.A). El resultado más destacable es el importante descenso del número de acusaciones incorrectas conseguido con la propuesta WM (mayor del 95%), con respecto a la técnica original de Marti. Esta reducción se debe al funcionamiento de la categoría de nodo sospechoso introducida por la técnica WM, como se explicó en la sección III.A. Los nodos retransmisores que se marcan como sospechosos tienen otra oportunidad de recuperar una buena reputación antes de ser acusados finalmente de actuar de manera egoísta. Además, cabe la posibilidad de que un nodo sospechoso no vuelva a interactuar otra vez con el nodo precursor que le marcó como sospechoso. En ambos casos, no se llega a realizar finalmente la acusación. La razón del descenso del número de acusaciones incorrectas en el caso de la técnica RFM es que cuando se detecta la caída de un enlace antes de que el nodo retransmisor sea acusado de comportarse egoístamente, su reputación es restaurada. De esta forma, se reduce el efecto negativo de los niveles de reputación de las caídas de los enlaces radio.

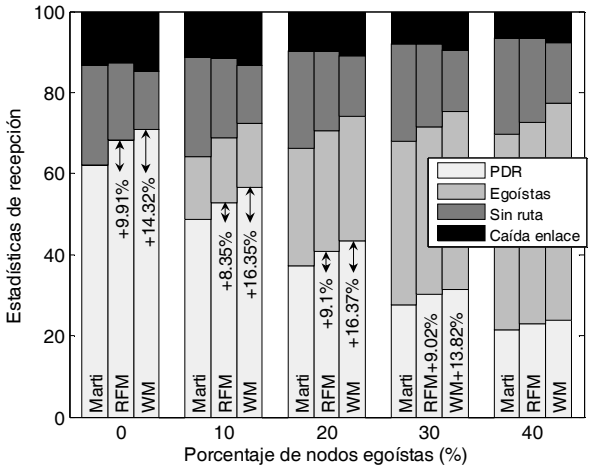


Fig. 2. Estadísticas de recepción de paquetes para las mejoras propuestas.

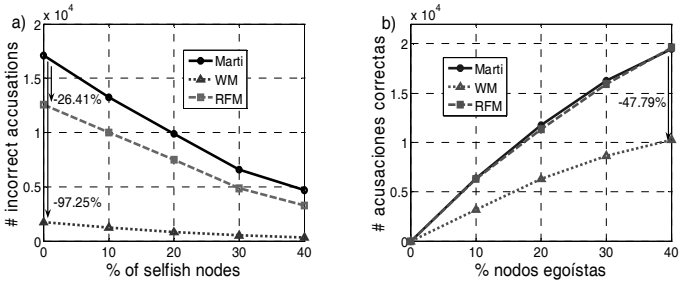


Fig. 3. Número de acusaciones incorrectas (a) y correctas (b)

El número de acusaciones correctas es un parámetro de rendimiento que refleja el número de ocasiones en que un nodo egoísta es acusado. Un mayor número de acusaciones correctas contribuye a incrementar el número de rutas *multi-hop* sin nodos egoístas. La Figura 3(b) refleja que este parámetro se mantiene constante para la técnica RFM respecto a la técnica de Marti, lo que confirma que el proceso de restauración de la reputación en la técnica RFM no beneficia a los nodos egoístas, dado que son acusados rápidamente antes de que un posible evento de caída de enlace sea iniciado. Por otro lado, en la técnica WM se detecta un descenso del número de acusaciones correctas de aproximadamente un 45%, a pesar de que los resultados mostrados en la Figura 2 se aprecia que este descenso no tiene un impacto apreciable sobre el PDR de la técnica WM. Esto

se debe a que, como se ha comentado, los nodos que son marcados como sospechosos posiblemente no vuelven a interactuar con el nodo precursor y por tanto no son finalmente acusados, pero tampoco tienen ocasión para descartar más paquetes.

La Figura 4(a) muestra el número de ocasiones en las que se estableció una ruta *multi-hop* con nodos egoístas, lo cual se conoce como establecimientos de ruta incorrectos. Por otro lado, la Figura 4(b) representa el número de establecimientos de ruta correctos, es decir, de rutas sin nodos egoístas. Se aprecia un incremento notable del número de establecimientos de ruta correctos e incorrectos con la técnica WM. Esto se debe a su propio funcionamiento. En caso de que se observe a un nodo retransmisor actuando de manera egoísta, antes de ser acusado definitivamente, se marca como sospechoso y los enlaces a través del mismo se rompen. Los nodos sospechosos pueden participar otra vez en los procesos de descubrimiento y establecimiento de rutas. Este modo de funcionamiento implica un incremento en el número de rutas establecidas, tanto correctas como incorrectas. Sin embargo, el aumento del número de rutas incorrectas no afecta al PDR apreciablemente, como se muestra en la Figura 2, debido a que los nodos sospechosos son vigilados estrictamente en la técnica WM. La técnica RFM mantiene el mismo número de rutas incorrectas establecidas respecto al protocolo de Marti, e incrementa en un 14% aproximadamente el número de rutas correctas. Esta mejora se debe al hecho de que la técnica RFM reduce el número de acusaciones incorrectas pero mantiene el número de acusaciones correctas, como se aprecia en las figuras anteriores.

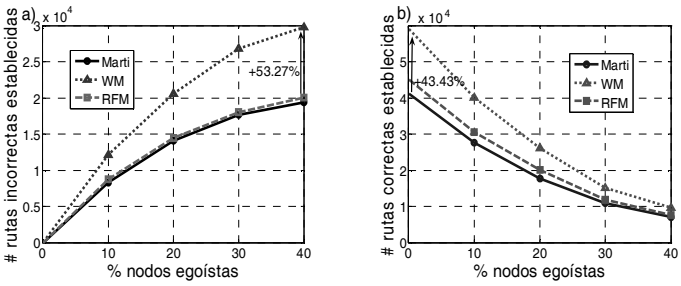


Fig. 4. Número de establecimientos de ruta incorrectos (a) y correctos (b)

En los SPPs basados en reputación, las peticiones de descubrimiento y de establecimiento de ruta son descartadas si el nodo que las recibe detecta que alguno de los nodos que participa en la ruta *multi-hop* es egoísta. El número de rutas correctas descartadas, representado en la Figura 5(a), se refiere al caso en el que realmente ningún nodo egoísta participaba en la ruta denegada. Se aprecia que tanto la técnica WM como la técnica RFM consiguen un notable descenso del número de rutas correctas descartadas, especialmente en el caso de WM. Esto conlleva a una reducción del porcentaje de paquetes descartados por la inexistencia de rutas sin nodos egoístas conocidos y al aumento del PDR que fue comentado en la Figura 2. La reducción del número de rutas correctas negadas se debe una reducción paralela del número de acusaciones incorrectas, tal como se señaló en la Figura 3. Es importante destacar que tanto WM como RFM mantienen un número de rutas incorrectas descartadas similar al del protocolo de Marti, como se muestra en la Figura 5(b). Esto significa que reducir el número de rutas correctas descartadas, lo cual incrementa la disponibilidad de rutas sin nodos egoístas, no se consigue al precio de reducir también el número de rutas incorrectas descartadas, lo cual aumentaría el porcentaje de paquetes descartados por nodos egoístas y reduciría por consiguiente el PDR.

La utilización simultánea de las técnicas WM y RFM propuestas es posible, ya que han sido implementadas de manera modular. Los resultados preliminares obtenidos al respecto indican que al ser ejecutadas simultáneamente, se obtiene un mayor incremento del número rutas correctas disponibles, con una mejora del PDR mayor que la conseguida con las técnicas empleadas por separado. Sin embargo, los resultados completos no han podido ser incluidos en la presente comunicación debido a restricciones temporales.

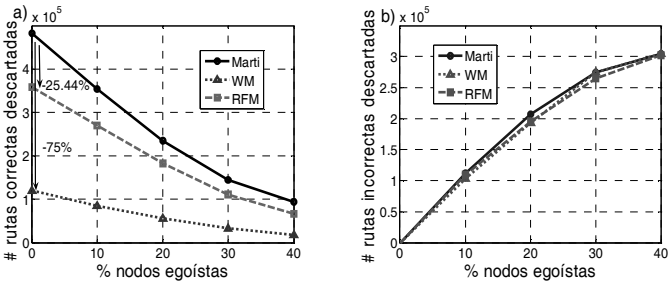


Fig. 5. Número de rutas (a) correctas e (b) incorrectas descartadas

VI. CONCLUSIONES

Este trabajo ha presentado dos técnicas de mejora del mecanismo básico de detección *watchdog* empleado en la mayoría de los protocolos de prevención de egoísmo para redes móviles cooperativas basados en reputación. Los SPPs basados en reputación tienen como objetivo detectar y aislar a los nodos egoístas que no participan en la retransmisión de los paquetes de otros nodos, pero que se benefician de la retransmisión de sus propios paquetes por parte de otros nodos. Resultados anteriores demostraban la inexactitud de la técnica *watchdog* en la detección de nodos egoístas y sus efectos negativos sobre el rendimiento de SPPs basados en reputación cuando se evaluaban en condiciones de simulación realistas. La técnica de *watchdog* sobrestima el egoísmo de los nodos al confundir las colisiones de los paquetes y los errores del canal radio con descartes intencionados de paquetes de datos. Para mitigar las consecuencias de esta inexactitud, este trabajo propone dos técnicas que mejoran la capacidad de los SPPs para detectar correctamente a los nodos egoístas y reducen el número de acusaciones incorrectas. Como se ha mostrado, las técnicas propuestas incrementan la disponibilidad de rutas *multi-hop* libres de nodos egoístas y por consiguiente aumentan también el PDR y la conectividad de las redes cooperativas *multi-hop*.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el Ministerio de Ciencia e Innovación, el Ministerio de Industria y Comercio y fondos FEDER a través de los proyectos TEC2008-06728 y TSI-02400-2008-113 y por la Generalitat Valenciana a través de la ayuda con referencia BFPI/2007/269.

REFERENCIAS

[1] Recommendación ITU-R M.1645 – "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000".

[2] Y. Lin y Y. Hsu, "Multi-hop Cellular: a new architecture for wireless communications," *Libro de Actas del IEEE Computer Communications (INFOCOM)*, pp. 1273-1282, Mar. 2000, Israel.

[3] X. J. Li, B.-C. Seet y P. H. J. Chong, "Multihop cellular networks: Technology and economics," *Computer Networks*, Elsevier, vol. 52, No. 9, pp. 1825-1837, Jun. 2008.

[4] S. Buchegger, J. Mundinger y J.-Y. Le Boudec, "Reputation systems for self-organized networks," *IEEE Technology and Society Magazine*, vol. 27, núm. 1, pp. 41-47, Primavera 2008.

[5] Y. Yoo y D.P. Agrawal, "Why does it pay to be selfish in a MANET?," *IEEE Wireless Communications Magazine*, vol. 13, núm. 6, pp. 87-97, Dic. 2006.

[6] S. Marti, T. J. Giuli, K. Lai y M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," *Libro de Actas del International Conference on Mobile Computing And Networking ACM (MobiCOM 2000)*, pp 255-265, 2000.

[7] A. Rodriguez-Mayol y J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks," *Libro de Actas del European Wireless Conference EW2010*, Abr. 2010.

[8] K. Balakrishnan, J. Deng y V.K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," *Libro de Actas del IEEE Wireless Communications and Networking Conference* WCNC 2005, vol. 4, pp. 2137-2142, Mar. 2005.

[9] M.T. Refaei, Y. Rong, L.A. DaSilva y H. Choi, "Detecting Node Misbehavior in Ad hoc Networks," *Libro de Actas del IEEE International Conference on Communications ICC 2007*, pp. 3425-3430, Jun. 2007.

[10] S. Buchegger, C. Tissieres y J.Y.Le Boudec, "A test-bed for misbehavior detection in mobile ad-hoc networks," *Libro de Actas del IEEE Workshop on Mobile Computing Systems and Applications WMCSA,* pp.102 – 111, Dic. 2004.

[11] Rice Monarch Project "Wireless and mobility extensions to ns-2," http://www.monarch.cs.rice.edu/cmu-ns.html

[12] K. Maeda, A. Uchiyama, T. Umedu, H. Yamaguchi, T. Higashino, "Urban pedestrian mobility for mobile wireless network simulation," *Ad Hoc Networks, Elsevier*, vol. 7, núm. 1, pp. 153–170, 2009.

[13] UMTS 30.03 v3.2.0 TR 101 112 "Selection procedures for the choice of radio transmission technologies of the UMTS," ETSI, Apr. 1998.

[14] IEEE P802.11s/D2.0, borrador de corrección del estándar IEEE 802.11: Mesh Networking, *IEEE Standard*, 2007.

[15] C. Perkins y E. Royer, "Ad hoc On-Demand Distance Vector Routing," *Libro de Actas del IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA), pp. 90-100, 1999.

[16] I. D. Chakeres y C. E. Perkins, "Dynamic MANET on-demand (DYMO) Routing," draft-ietf-manet-dymo-05, Internet Draft, Jun. 2006.

[17] WINNER, "DI. 1.1. WINNER II interim channel models," *Public Deliverable*, http://www.ist-winner.org/

[18] M. Sepulcre y J. Gozalvez, "On the importance of radio channel modeling for the dimensioning of wireless vehicular communication systems," *Libro de Actas del International Conference on ITS Telecommunications 2007*, ITST '07, pp 1–5, Jun. 2007.

Transmisión eficiente de datos multimedia en redes inalámbricas de sensores

Jose F. Mingorance Puga, Gabriel Maciá-Fernández, António Grilo and Nestor M. C. Tiglao
Universidad de Granada - CITIC, Instituto Superior Técnico (Lisboa - Portugal)

***Resumen*—La transmisión de información multimedia para múltiples aplicaciones requiere prestaciones de tiempo real. Estas prestaciones implican la necesidad de recibir a tiempo la información para que ésta pueda ser útil para la capa de aplicación. La recuperación de pérdidas a través de la retransmisión de los datos perdidos es una alternativa que puede introducir retardos inaceptables. Por esta razón, muchos autores proponen transmitir la información mediante capas de transporte sin función de recuperación de errores y, en su lugar, se usan códigos de error FEC y técnicas similares para maximizar la recuperación de datos en el receptor. No obstante, en las Redes Multimedia Inalámbricas de Sensores (WMSN), debido a la alta tasa de error en el canal, estos mecanismos no son suficientes para proporcionar una calidad de señal aceptable y, por tanto, se necesitan protocolos de transporte fiables adaptados a estos requisitos. En este artículo se proponen algunos mecanismos para mejorar las transmisiones multimedia en WMSN cuando se usan protocolos de transporte fiables. Estos mecanismos consisten en asignar una cantidad de tiempo para enviar una cierta cantidad de información, estimando si las condiciones del canal permiten o no completar la transmisión. Si es improbable que se complete la transmisión, entonces se detiene la misma, ahorrando de este modo una importante cantidad de energía y recursos en los sensores y la red.**

Se evalúa esta aproximación modificando el comportamiento de un protocolo fiable previamente propuesto (DTSN). La nueva aproximación, M-DTSN, mejora la flexibilidad de DTSN controlando el compromiso entre la calidad de la información transmitida y las restricciones de tiempo para datos multimedia en tiempo real, con un cierto grado de tolerancia a pérdidas. Los resultados de la simulación demuestran que las ventajas de M-DTSN para la transmisión de datos multimedia son bastante significativas cuando se comparan con el protocolo original DTSN.

***Index Terms*—Redes de sensores, transmisión multimedia, capa de transporte.**

I. Introducción

Las redes multimedia de sensores (WMSN) son redes de sensores que tienen capacidad para trabajar con información multimedia. Están compuestas por sensores multimedia, capaces de capturar y transmitir información multimedia. Por ejemplo, estos sensores podrían ser cámaras trabajando en entornos de vigilancia de baja resolución. Las WMSN presentan algunos retos que son comunes a todas las redes de sensores (escasos recursos como memoria, consumo de energía, capacidad de la CPU, etc.). Debido a estas limitaciones, es esencial maximizar el tiempo de vida de los sensores reduciendo la cantidad de información que atraviesa la red. Además, las WMSN tienen ciertas características que las hacen diferentes de las WSN tradicionales. Deben ser capaces de funcionar con ciertos requisitos de calidad de servicio que son específicos del tráfico multimedia. Más concretamente, deben ser capaces de adaptar su capacidad de transmisión a las particularidades de la información multimedia.

En este trabajo consideramos solamente aquella información multimedia que requiere prestaciones de tiempo real para su transmisión. Sin pérdida de generalidad, nos centraremos en la transmisión de vídeo, ya que constituye un flujo típico de datos en tiempo real. La información de vídeo está compuesta por una secuencia de imágenes, normalmente codificadas siguiendo un estándar (como MPEGv2). Las técnicas de codificación de vídeo escalables permiten al transmisor trabajar con múltiples resoluciones de vídeo codificando una imagen con una capa base y una o más capas adicionales. Los codificadores de vídeo son capaces de separar la información crítica de una imagen –la capa base– para presentar una imagen a baja resolución, y la información complementaria –las capas adicionales– que permiten reconstruir imágenes en alta resolución. La cantidad de información multimedia requerida por el receptor determina los parámetros usados en la transmisión por los codificadores, por ejemplo, tamaño de la imagen, resolución máxima, número de capas adicionales, periodo de muestreo de imágenes, etc.

Además de la capacidad del receptor, la capacidad de la red en el caso de WMSN también es una limitación importante en cuanto a la máxima resolución de vídeo permitida durante una transmisión. La existencia de enlaces de baja calidad, principalmente debida a los reducidos recursos de energía y potencia instalados en los sensores, supone un reto para el diseño de protocolos de transmisión en redes de sensores. Además, cuando hay información multimedia implicada, la existencia de retardos y jitter es un problema tradicional tratado por muchos investigadores. Debido a la existencia de estos entornos propensos a errores, las últimas investigaciones apuntan que es recomendable el uso de protocolos de transporte fiables para obtener una calidad aceptable[1], [2]. Estas contribuciones se han centrado principalmente en el diseño de protocolos de transporte optimizados para conseguir tasas de retransmisión y recuperación rápida de errores, ofreciendo a la capa de aplicación un mayor rendimiento, lo que permite usar una resolución más alta para la información multimedia. A pesar de ello, hasta donde llega nuestro conocimiento, todas las contribuciones consideran la capa de transporte como un sistema monolítico intentando comportarse lo mejor posible por sí misma.

J. F. Mingorance Puga (jose.mingorance@gmail.com) y G. Maciá-Fernández (gmacia@ugr.es) pertenecen a la Universidad de Granada, Dpto. Teoría de la Señal, Telemática y Comunicaciones, CITIC, España. António Grilo (antonio.grilo@inesc.pt) es miembro de INESC-ID/INOV e IST, Lisboa, Portugal. Nestor M.C. Tiglao (nmctiglao@yahoo.com) es miembro de EEEI, Universidad de Filipinas, Diliman, Quezon City, Filipinas.

En este artículo exploramos cómo las capas de transporte en WMSN podrían hacer uso de cierta información sobre las características de los datos multimedia a ser transmitidos con el fin de mejorar la calidad de la red percibida por la capa de aplicación. En particular, analizamos algunas características útiles de la información multimedia y descubrimos que es posible explotar el conocimiento sobre la tasa de muestreo de la información multimedia para permitir un aumento considerable en la calidad observada por los receptores. La idea básica para nuestra aproximación es la siguiente. Consideremos un ejemplo simple, consistente en una transmisión entre dos nodos en una WMSN, y supongamos que la unidad de información mínima para un receptor es una imagen. El receptor es capaz de presentar la imagen si ésta llega antes de un instante dado. Entonces, si el transmisor fuera capaz de estimar si la trama no va a llegar a tiempo al receptor (antes del instante de presentar la trama al usuario) no merecería la pena seguir transmitiendo la imagen. Nuestra propuesta aprovecha esta idea y, en esta línea, se sugieren algunos mecanismos para mejorar el rendimiento de las transmisiones multimedia.

Aunque nuestra aproximación podría funcionar sobre otros protocolos de transporte fiables, hemos elegido el *Distributed Transport Protocol for Sensor Networks*, DTSN [3], con el fin de implementarla y evaluarla. Se propone, por tanto, una versión modificada de este protocolo, denominada Multimedia DTSN, M-DTSN. La razones por las que se elige DTSN es que es un protocolo de transporte fiable y está especialmente diseñado para redes inalámbricas de sensores. En el artículo se evalúa en profundidad este protocolo mediante simulación, obteniendo resultados muy prometedores.

El artículo está organizado de la siguiente manera. En la Sección II proporcionamos algunos fundamentos sobre el protocolo DTSN, con el fin de clarificar las modificaciones sugeridas en nuestra aproximación. Después se describe la propuesta en la Sección III. A continuación, se evalúan y se discuten en profundidad los resultados obtenidos por M-DTSN en la sección IV. Finalmente, algunos trabajos relacionados se describen en la Sección V y las conclusiones se presentan en la Sección VI.

II. Fundamentos de DTSN

DTSN [3] fue concebido para la transferencia de datos con fiabilidad extremo a extremo al estilo TCP. DTSN usa peticiones selectivas de retransmisiones (ARQ) y confirmaciones negativas (NACK). Las confirmaciones positivas (ACK) también se usan para evitar situaciones de bloqueo que no pueden detectarse únicamente con NACK. Los mensajes NACK y ACK se envían por el receptor únicamente si el emisor lo solicita mediante una petición explícita de confirmación, EAR. Esta solicitud puede ir insertada (piggy-backing) en un paquete de datos que envíe el emisor.

En DTSN, una sesión es una relación unívoca entre emisor/receptor identificada por la tupla `<dirección emisor, dirección receptor,identificador aplicación, número de sesión>`. La sesión se inicia automáticamente cuando el primer paquete se procesa, y termina cuando expira el temporizador de actividad (si no quedan confirmaciones pendientes). Se escoge un número aleatorio para el número de sesión que diferencia sin ambigüedad sucesivas sesiones que comparten los mismos extremos e identificadores de aplicación. El procesamiento de un paquete con la misma tupla `<dirección emisor, dirección receptor,identificador aplicación>` pero diferente número de sesión provoca que la sesión anterior se destruya y una nueva comience.

En una sesión, los paquetes se numeran secuencialmente. La ventana de confirmación (AW) se define como el número de paquetes que la fuente transmite antes de generar un mensaje EAR. El búffer de salida en el emisor consiste en una ventana deslizante que puede albergar más de una AW. El tamaño del búffer de salida y de la AW depende de las restricciones de memoria de cada nodo.Para minimizar el número de retransmisiones extremo a extremo, los nodos intermedios son capaces de almacenar en caché un número de paquetes de acuerdo a una cierta probabilidad. Ante la recepción de un NACK, si alguno de los paquetes que se solicitan en el NACK se encuentran en la caché de un nodo intermedio, éste puede retransmitirlos hacia el receptor. Después de eliminar del NACK los números de secuencia de los paquetes retransmitidos, el NACK sigue su camino hacia el emisor.

III. Mecanismos de Transmisión Multimedia

En esta sección introducimos nuestra aproximación para mejorar la eficiencia durante la transmisión de información multimedia en una WMSN. Consideremos un escenario compuesto de un transmisor enviando información multimedia con destino un receptor a través de una WSN. Nuestra hipótesis es que en la capa inferior a nuestra solición habrá un protocolo de transporte fiable para la transmisión. Aunque hemos elegido DTSN, nuestros resultados no están ligados a él, y pueden generalizarse a otros protocolos de transporte fiables.

Se consideran tres factores en nuestro escenario de estudio: (*i*) los flujos multimedia tienen restricciones temporales, (*ii*) los sensores están limitados en cantidad de energía permitida para las transmisiones y (*iii*) la fiabilidad de la capa de enlace/MAC normalmente no es suficiente para asegurar el nivel requerido de entregas exitosas; incluso, el uso de códigos FEC no es una solución satisfactoria en nuestro escenario. Bajo estas hipótesis, si la capa de transporte en un sensor dado es informada sobre las necesidades de la capa de aplicación, nuestra consideración es que es posible mejorar considerablemente las transmisiones requeridas. A continuación explicamos como puede conseguirse esta mejora.

Los receptores multimedia presentan limitaciones debido a la restricción temporal inherente a la información recibida. Algunas están relacionadas con la cantidad de retardo permitido y el jitter máximo tolerado durante la transmisión. Además, el receptor debería obtener también información del transmisor como un promedio de la tasa de trafico requerida; p.ej., considerando un streaming de vídeo, las imágenes deberían llegar a una tasa que vendrá en cierta forma determinada por la tasa de muestreo de la señal de vídeo.

Consideremos un escenario en el que un receptor de vídeo reproduce un flujo de vídeo compuesto por una secuencia de

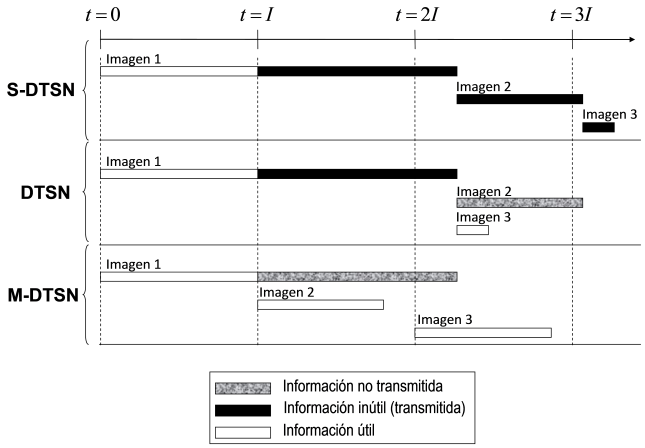


Figura 1: Diagrama mostrando la recepción de tramas en el receptor y la cantidad de información útil/inútil según la perspectiva del receptor, para tres estrategias de transmisión diferentes: S-DTSN, DTSN y M-DTSN

imágenes. Asumamos también que el tamaño de todas las imágenes es igual, y sea su valor S. Además, consideremos que el receptor necesita obtener al menos una imagen cada cierto tiempo, llamado *intervalo de imagen, I* para poder ser capaz de reproducir la secuencia de vídeo. Transmisor y receptor se encuentran localizados en una red inalámbrica de sensores separados por un cierto número de saltos H.

En este escenario, estamos interesados en un mecanismo de transmisión que mejore la efectividad alcanzada por los protocolos actuales de transporte. Para permitir una comparación de nuestra aproximación con el comportamiento de otros protocolos, nos centraremos en DTSN y clarificaremos cuáles son sus diferencias en la transmisión de información respecto a nuestra propuesta.

Consideremos el escenario de ejemplo mostrado en la Figura 1. Tres tramas consecutivas son enviadas desde un transmisor hacia un receptor. Aunque las tres tramas tienen el mismo tamaño, S, la cantidad de tiempo empleada para su transmisión no es la misma, ya que éste depende de las condiciones de la red: calidad del enlace, número de saltos, número de retransmisiones, etc. El tiempo empleado para la recepción de cada una de las tramas se muestra en las barras horizontales de la Figura 1. La misma representación se hace para tres estrategias de transmisión diferentes: S-DTSN, DTSN y M-DTSN. Estas estrategias se explican a continuación. M-DTSN es nuestra propuesta. Las otras dos se presentan para comparar M-DTSN con dos aproximaciones más sencillas.

DTSN simple, S-DTSN, es la estrategia más simple en el uso de DTSN. La capa de transporte, cada intervalo de imagen, I, recibe una imagen para enviar al receptor. Estas imágenes se envían secuencialmente, de manera que una imagen no se envía hasta que la transmisión de la anterior se completa. En la Figura 1 vemos que la Imagen 1 tarda más de I segundos. Esto implica que el receptor obtendrá alguna información considerada como útil (barra blanca), ya que se recibe durante el intervalo de tiempo reservado para la recepción de esa imagen, $t \in [0, I]$. Sin embargo, la información recibida para la imagen 1 después del instante $t = I$ es inútil, ya que la imagen debería de haber sido presentada en el receptor en el instante $t = I$. Esta información inútil que no contribuye al flujo de vídeo, provoca al mismo tiempo que las imágenes sucesivas se retrasen, incrementando así la probabilidad de que lleguen también demasiado tarde. Una vez que la imagen 1 se ha enviado completamente, la imagen 2 comienza a enviarse. El retardo introducido por la parte inútil de la imagen 1 hace que la imagen 2 llegue después del instante en que debería presentarse en el receptor, $t = 2 \cdot I$, convirtiéndose también en una imagen inútil. Para la imagen 3 sucede exactamente lo mismo. En resumen, usando S-DTSN ninguna de las 3 imágenes transmitidas en nuestro ejemplo se presentan finalmente en el receptor, debido a que llegan con un retardo más alto del permitido por el receptor.

El comportamiento de DTSN es parecido al de S-DTSN, pero varía ligeramente. En base a la tasa de imagen requerida por el receptor, el transmisor es capaz de saber la imagen que este último espera, y por tanto, también de descartar las imágenes que se encuentren esperando ser transmitidas y ya no tiene sentido enviarlas. Vamos a clarificar este punto observando el diagrama de la Figura 1 para DTSN. El receptor experimenta la misma evolución que en S-DTSN para la imagen 1. Sin embargo, cuando el transmisor tiene que enviar la imagen 2, se da cuenta de que el instante para presentar esa imagen en el receptor ya pasó, y por tanto decide enviar la imagen 3. Esta imagen ahora llega a tiempo al receptor para ser presentada en $t = 3 \cdot I$. Este comportamiento modificado con respecto a S-DTSN presenta dos beneficios: primero, la transmisión de la imagen 2 no se hace, por lo que se ahorran recursos y, segundo, el receptor es capaz de presentar al menos una de las imágenes.

M-DTSN es nuestra propuesta para mejorar la eficiencia de la transmisión. En este caso, el transmisor asume que no debería de tardar más de I segundos en enviar una imagen, ya que considera que el receptor no sería capaz de recibir la trama completa a tiempo si se tardara más de I segundos en transmitirla. Consecuentemente, el transmisor detiene la transmisión de una imagen cuando pasan I segundos desde el inicio de la transmisión. Fijándonos en la Figura 1, vemos que la transmisión de la imagen 1 se detiene en $t = I$. Entonces, la transmisión de la imagen 2 empieza. Debido a un cambio en las condiciones de la red, esta segunda imagen llega a tiempo. Finalmente, la imagen 3 también llega exitosamente y se podrá reproducir por parte del receptor. Vemos en este ejemplo que, con esta estrategia, dos de las imágenes se reciben completamente, mientras que la recepción de la primera imagen sólo se realiza parcialmente, y por tanto, esta imagen sería inútil para el receptor.

En resumen, nuestra propuesta para mejorar la transmisión de información multimedia en redes inalámbricas de sensores consiste en adaptar la capa de transporte, de modo que sea capaz de recibir una petición de la capa de aplicación solicitando no solamente el envío de una imagen, sino también requiriendo dicho envío en un umbral de tiempo específico.

Aunque los beneficios de M-DTSN sobre las otras aproximaciones son claros en este escenario, algunos detalles deben aclararse. Primero, muchos receptores son capaces de recuperar la información completa de una imagen a partir

de información parcial. Por ejemplo, en [4] se propone un codificador capaz de recuperar la imagen completa a partir de 5/7 (72 %) de la misma. En este escenario no estaría claro si los beneficios de M-DTSN se mantienen, ya que la transmisión se detiene cuando pasan I segundos. Segundo, los receptores normalmente implementan memorias intermedias para solventar el efecto del jitter. Esto significa que los receptores serán capaces de recibir información incluso después de que el plazo máximo para la transmisión se alcance. Por estas razones, se evalúa a continuación (Sección IV) el comportamiento de M-DTSN, comparándolo con el de S-DTSN y DTSN.

IV. Evaluación Experimental

En esta sección se evalúa M-DTSN en un entorno experimental. Nuestra intención es comprobar si M-DTSN sobrepasa a DTSN y S-DTSN en rendimiento, tal como se espera, y analizar si los resultados son válidos para un amplio rango de configuraciones. Para este propósito, se ha implementado M-DTSN en el simulador TOSSIM usando TinyOS 2.1.0, y se ha utilizado una versión ya implementada de DTSN, cuyos detalles se encuentran en [3].

Se ha realizado un amplio conjunto de experimentos en los cuales se varían los valores de los siguientes parámetros: tamaño de imagen, S, atenuación de todos los enlaces en la red, A, número de saltos intermedios entre el receptor y el transmisor, H, e intervalo entre imágenes para la transmisión multimedia, I. En cada simulación se fija el valor de todos los parámetros y se va variando uno de ellos para observar el comportamiento según dicho parámetro. Se repiten simulaciones cambiando el parámetro a variar. Los parámetros de configuración de la capa DTSN han sido correctamente ajustados para evitar efectos colaterales indeseados, tales como congestión de la ventana o excesivos retardos. Esta configuración se ha realizado teniendo como guía la descripción de DTSN presentada en [3]. Se ha configurado una red de 20 sensores donde todos los enlaces bidireccionales tienen una atenuación variable (esta es de hecho una de las variables de estudio) y un patrón de ruido. Se ha escogido el patrón de ruido usado comúnmente en el modelo de ruido de TOSSIM, y definido en `heavy-meyer.txt`. Respecto a la capa de aplicación, el receptor implementa una memoria intermedia que soporta un jitter de 100 ms.

A. Medida de la eficiencia de una transmisión multimedia

Estamos interesados en evaluar los resultados producidos por M-DTSN en términos de eficiencia de la transmisión. Esta eficiencia se entiende como la percepción que la capa de aplicación obtiene del servicio dado por la capa de transporte. Por tanto, nos interesa descubrir cuánta información útil la capa de aplicación va a obtener cuando se activa M-DTSN. Para una imagen enviada durante la transmisión multimedia, definimos el *porcentaje de imagen recibida, PIR,* como el porcentaje de bytes de la imagen que llegan al receptor antes del instante en el que el receptor debería presentar la imagen. También definimos, para una transmisión multimedia específica, el *porcentaje promedio de imagen recibida, PPIR,* como el valor medio del PIR para todas las imágenes que deberían ser enviadas durante dicha transmisión multimedia.

Tabla I: Valores por defecto para las simulaciones.

Parámetro	***Valor***
Capa de aplicación	
Intervalo de imagen	5 s
Jitter permitido en el receptor	100 ms
Parámetros de la red	
Ruido del canal	definido en heavy-meyer.txt
Número de saltos	1
Parámetros de DTSN	
Tamaño de la ventana de DTSN	50 paquetes
Ventana de confirmación de DTSN	12 paquetes
Máximo número de intentos de EAR	10
Timeout DTSN de actividad (transmisor)	30*250ms
Timeout DTSN de actividad (receptor)	40*250ms

En una primera aproximación, los receptores solamente son capaces de reproducir aquellas imágenes que han llegado completamente al receptor cuando se alcanza el instante en el que han de presentarse, es decir, las imágenes cuyo PIR es 100 %. Sin embargo, como se mencionó previamente, muchos codificadores propuestos recientemente son capaces de recuperar la información de la imagen completa cuando se recibe sólo una porción de la imagen. Por ejemplo, la codificación propuesta en [4] usando códigos FEC sobre canales con pérdidas es capaz de recuperar una imagen completa si más del 72 % de su contenido se ha recibido. Por esta razón, no estamos interesados únicamente en explorar la cantidad de imágenes que se reciben completamente y a tiempo, sino en el porcentaje de la imagen que ha llegado a su destino en el instante en que debería ser reproducida. Esto último se mide, precisamente con el indicador ya definido: *PIR*.

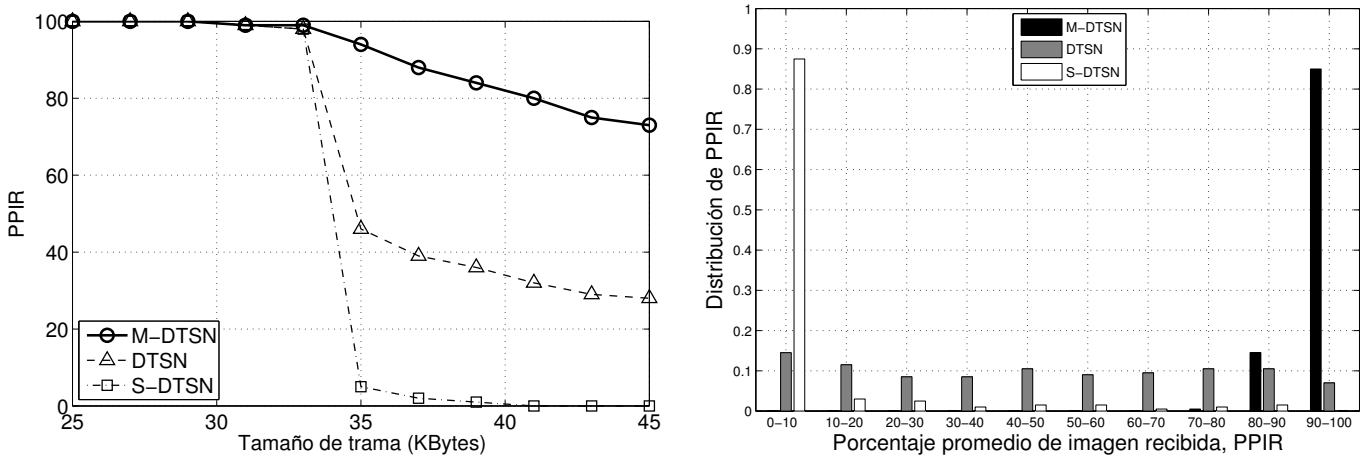
B. Resultados de las simulaciones

A continuación mostramos los resultados más significativos obtenidos a partir de los experimentos. En concreto, para cada una de las cuatro variables estudiadas, S, A, H, I, se presentan los detalles y resultados para un escenario, que es diferente según la variable estudiada y que está seleccionado para poder observar valores significativos de la evolución del rendimiento de M-DTSN. En cada uno de ellos, se muestra el porcentaje promedio de trama obtenido para las tres estrategias expuestas en la Sección III, M-DTSN, DTSN y S-DTSN. Además, para una mejor visibilidad de los resultados, estudiamos algunos puntos interesantes de la simulación y obtenemos la distribución del PIR mediante un histograma.

En todos los resultados mostrados a continuación, los valores ajustados para las variables estudiadas se indicarán explícitamente y, cuando no es así, los valores configurados se corresponden con los mostrados en la Tabla I.

Dependencia del rendimiento con el tamaño de imagen.

La Figura 2(a) muestra resultados para el porcentaje promedio de imagen recibida, PPIR, cuando el tamaño de la imagen, S, se ha ido variando. Podemos comprobar cómo en esta figura, para tamaños de imagen mayores de S=33KB, el valor del PPIR disminuye cuando el tamaño de imagen aumenta. Este comportamiento se debe al hecho de que un tamaño de imagen



(a) A = 75dB

(b) A=75dB, S=35KB

Figura 2: Comparación del rendimiento entre M-DTSN y DTSN,S-DTSN cuando el tamaño de imagen *S* varia: (a) porcentaje promedio de imagen recibida para una atenuación de 75 dB; (b) histograma de PPIR para una atenuación de 75 dB y S=35 KB.

más grande implica un tiempo mayor para enviar las imágenes y, por tanto, una reducción de su PPIR.

También es interesante determinar la cantidad de imágenes que se presentaría correctamente en el receptor. Para este propósito necesitamos primero establecer un umbral en la cantidad de información que se necesita recibir para cada imagen que se quiere presentar. Consideraremos en este caso que nuestra transmisión multimedia utiliza el codificador propuesto en [4], y que tiene por tanto un umbral del 72 % del tamaño total de la imagen. Para hacer posible esta evaluación, obtenemos la distribución del porcentaje de trama recibido en un punto significativo y usamos el método del histograma. Esta distribución se muestra en la Figura 2(b). Aquí, vemos que todas las imágenes recibidas cuando usamos M-DTSN están por encima del 70 %. Esto implica que el codificador sería capaz de recuperar todas las imágenes, al contrario que si usamos DTSN, donde sólo el 24 % de las imágenes llegan con un PPIR mayor a 72 %, siendo este porcentaje en torno al 2 % para el caso de S-DTSN.

Queda claro a partir de estas figuras que el rendimiento de M-DTSN es considerablemente superior al de DTSN y S-DTSN. Además, como se esperaba, los resultados obtenidos para DTSN son superiores a los de S-DTSN, ya que S-DTSN utiliza menos inteligencia en la transmisión.

Dependencia del rendimiento con la calidad del enlace.

La Figura 3 muestra los resultados obtenidos cuando la atenuación del enlace varía, para un tamaño de imagen S=10KB. Hasta un umbral de 75dB, las tres estrategias se comportan igual. Sin embargo, se observa que la evolución del rendimiento en M-DTSN es mucho mejor cuando las condiciones de los enlaces empeoran. En este caso, para el punto estudiado A=80dB, el histograma obtenido muestra que prácticamente la mitad de las imágenes se reciben por encima del 72 %.

Dependencia del rendimiento con el intervalo de imagen.

Los resultados correspondientes a la variación del intervalo entre imágenes, *I*, se representan en la Figura 4(a). Claramente muestran que, tal como se esperaba, PPIR crece con el intervalo entre imágenes. Esto es debido a que se permite más tiempo para la recepción de una imagen, y por tanto se incrementa el porcentaje recibido de cada imagen.

En estos resultados confirmamos que el comportamiento de M-DTSN es mucho más adecuado que el de DTSN y S-DTSN y su rendimiento muy superior. Además podemos ver cómo M-DTSN concentra el histograma en valores más altos de distribución de PPIR -ver Figura 4(b)-, mientras que DTSN por ejemplo genera una distribución cuasi-plana. Esto implica que, cuando los valores de PPIR>70 % son aceptables para el receptor, el porcentaje de imágenes útiles será superior al 90 % para M-DTSN, mientras que estará en torno al 16 % para DTSN.

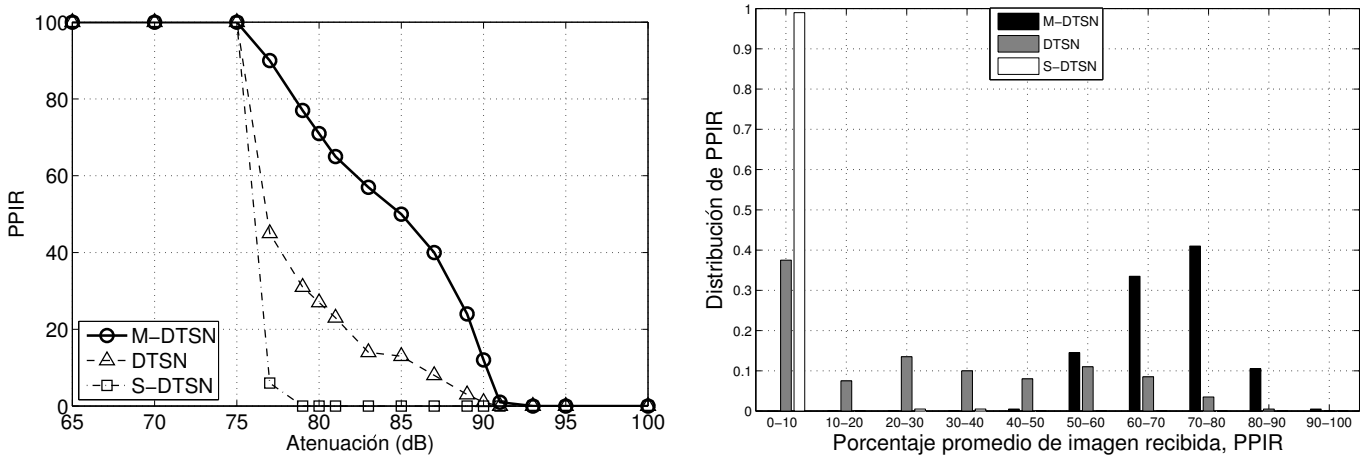
Dependencia del rendimiento con el número de saltos.

Como podemos ver en la Figura 5, M-DTSN es superior también en los casos en que el número de saltos es suficientemente bajo para permitir la llegada en tiempo de una parte considerable del tráfico multimedia. Nótese que los histogramas para las tres estrategias claramente indican que la cantidad de tramas potencialmente válidas para ser presentadas es mucho mayor para M-DTSN.

Dependencia del rendimiento con el jitter.

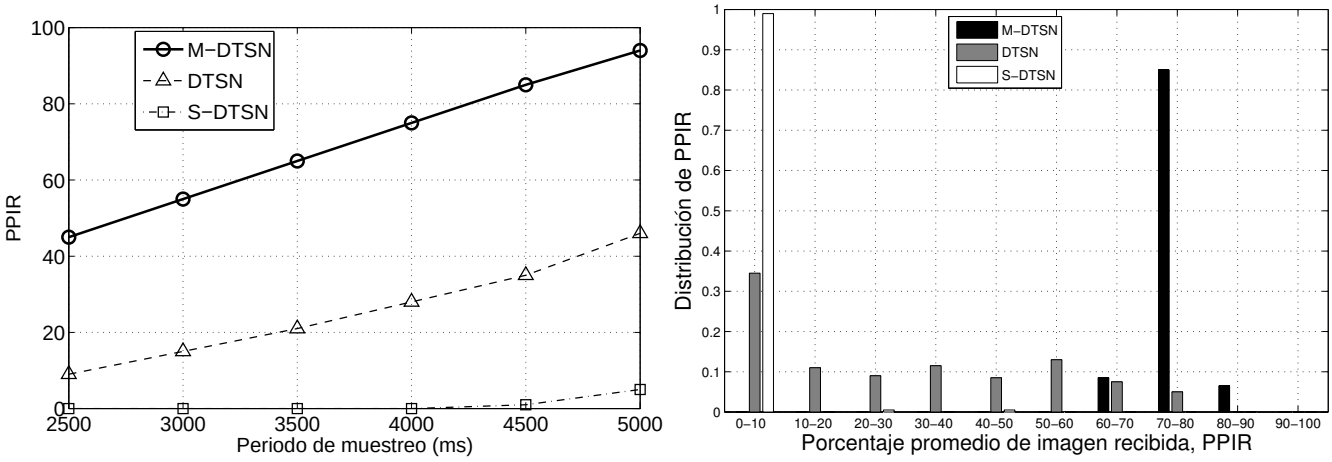
Para comprobar la influencia que el jitter tiene en los escenarios presentados, a continuación se realiza un batería de simulaciones en las que se varía el jitter permitido por el receptor.

Como se observa en la Figura 6, la influencia del jitter es practicamente irrelevante frente al resto de parámetros. Esto nos sirve para constatar que, en efecto, el hecho de haber establecido un jitter de 100 ms no conlleva pérdida alguna de generalidad en las simulaciones realizadas sino todo lo contrario, se acerca más al comportamiento de un receptor real.



(a) S=30KB (b) S=30KB, A=80dB

Figura 3: Comparación de rendimiento entre M-DTSN y DTSN, S-DTSN cuando varía la calidad del enlace (atenuación,A): (a) porcentaje promedio de imagen recibida para S=30KB; (b) histograma de PPIR para S=30KB y A=80dB.



(a) S=35KB, A=75dB (b) S=35KB, A=75 dB, I=4000ms

Figura 4: Comparación de rendimiento entre M-DTSN y DTSN, S-DTSN cuando variamos el intervalo de imagen, *I*: (a) porcentaje promedio de imagen recibida para S=35KB y A=75dB; (b) histograma de PPIR para S=35KB, A=75 dB e I=4000ms.

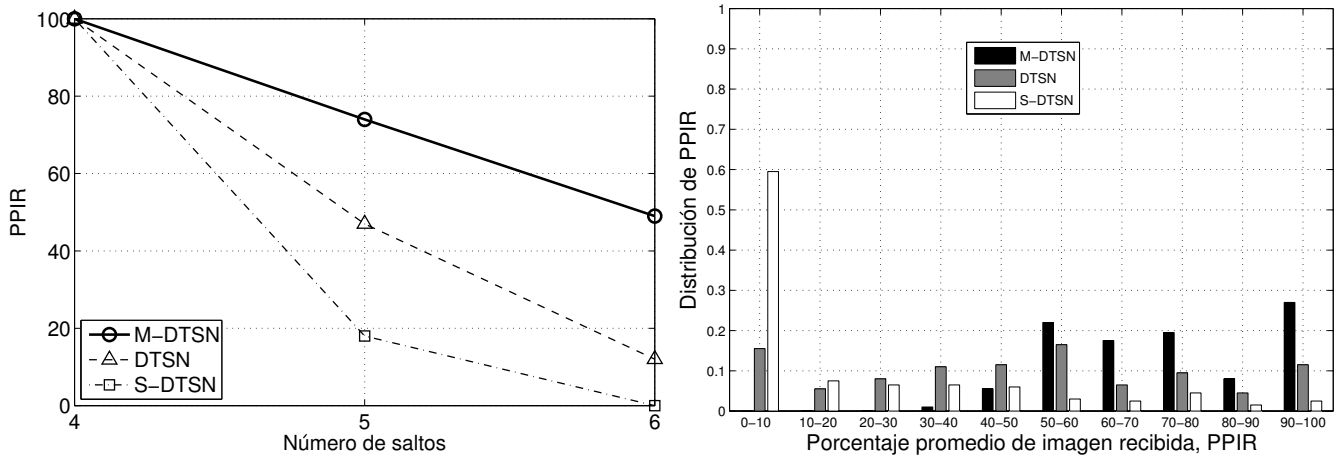
Dependencia del rendimiento con el tamaño de la ventana DTSN.

De la misma forma que se ha comprobado que la configuración para jitter en el receptor no influye de manera importante en los resultados obtenidos, se comprueba también si los tamaños de ventana que se han usado en las simulaciones están congestionando la transmisión y, por tanto, evitan obtener el máximo rendimiento posible en las transmisiones.

Para ello se han realizado experimentos variando el tamaño de la ventana de DTSN. En la Figura 7 se muestran algunos resultados, en los que la ventana de confirmación se ha configurado a 1/4 de la ventana DTSN. Se observa que para valores pequeños de la ventana (10 - 20 paquetes) se produce congestión y esto impide las transmisiones alcancen su máximo rendimiento. Al aumentar la ventana (30 - 60 paquetes) la curva de rendimiento obtenida converge a una asíntota. Esto se debe al hecho de que en este rango el tamaño de ventana es suficientemente grande para que no se produzca congestión. A partir de este punto, un aumento en el tamaño de la ventana no se traduce en un incremento de PPIR, ya que éste se encuentra limitado ahora por el resto de parámetros que configuran el escenario.

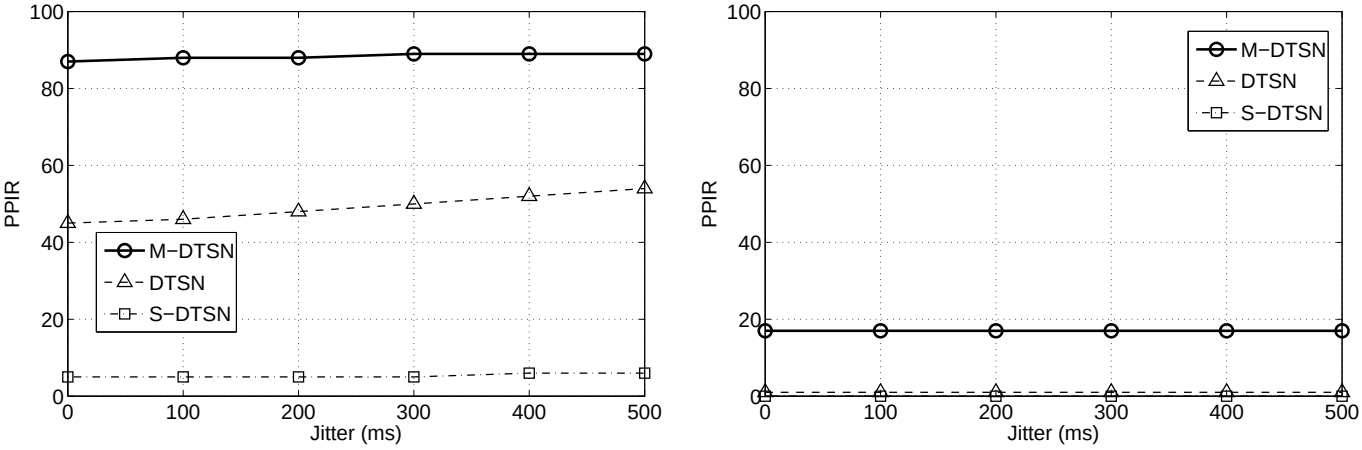
V. Trabajo relacionado

Tradicionalmente, la principal función de la capa de transporte ha sido proporcionar control de congestión y garantizar la comunicación. Además, proporciona una abstracción de la red y calidad de servicio (QoS) a la capa de aplicación. Esta última especifica los parámetros de QoS y configura el servicio para alcanzar las garantías requeridas a través de la capa de transporte. Asimismo, es deseable para la capa de transporte reducir la latencia y maximizar el throughput. La transmisión de flujos de datos multimedia es un campo relativamente nuevo identificado en el exhaustivo estudio [17]. Los protocolos de



(a) S=10KB, A=0dB (b) S=10KB, A=0dB, 5 saltos

Figura 5: Comparación del rendimiento entre M-DTSN y DTSN,S-DTSN cuando varía el número de saltos: (a) porcentaje promedio de imagen recibida para S=10KB y A=0dB; (b) histograma de PPIR para S=10KB, A=0dB y 5 saltos.



(a) S=35KB, A=75dB (b) S=30KB, A=90dB

Figura 6: Comparación del rendimiento entre M-DTSN y DTSN,S-DTSN cuando se varia el jitter del receptor: (a) porcentaje promedio de trama recibido para S=35KB y A=75dB y (b) porcentaje promedio de trama recibido para S=30KB y A=90dB.

transporte usados para la transmisión multimedia a través de internet, tales como RTP/RTCP (en su versión sobre TCP) [5] y DCCP [6] no pueden aplicarse directamente a las WSN porque fueron diseñados principalmente para trabajar en redes cableadas. Sin embargo RTP sobre UDP sí ofrece características más convenientes para funcionar sobre redes inalámbricas. Por tanto, las suposiciones subyacentes no funcionan en redes inalámbricas de sensores. En particular, las redes cableadas no tienen problemas de interferencias, y las pérdidas de paquetes surgen principalmente por la congestión. Por otro lado, las redes inalámbricas sufren los impedimentos de la capa física, lo que conlleva tasas de error de bit mucho más altas. Como resultado, el uso de protocolos de transporte de internet y/o redes cableadas implica una degradación del rendimiento y enormes ineficiencias energéticas [7].

La mayoría de los protocolos de transporte más famosos desarrollados para redes inalámbricas de sensores como ESRT [8], CODA [9], SenTCP [10], y RMST [11] proporcionan una calidad de comunicación muy pobre, porque estos protocolos no consideran los retardos extremo a extremo y, por tanto, el retardo de las tramas puede ser muy alto [12]. Por otro lado, otros trabajos recientes como DTSN [13], CTCP [14] y RCRT [15] se centran en la entrega fiable de información sin altos retardos.

A pesar de los esfuerzos realizados, se han desarrollado pocos protocolos dirigidos a los requisitos específicos del tráfico multimedia. Por ejemplo, aunque no diseñado específicamente para aplicaciones multimedia, el protocolo DART [16] concilia las restricciones de los retardos en tiempo real con la fiabilidad. Otra aproximación es el uso de protocolos de encaminamiento multitrayecto, que pueden mejorar la entrega de los datos multimedia enviando el tráfico a través de diferentes caminos. MPMPS [2] soporta múltiples prioridades de tráfico para diferenciar los flujos multimedia de otro tráfico

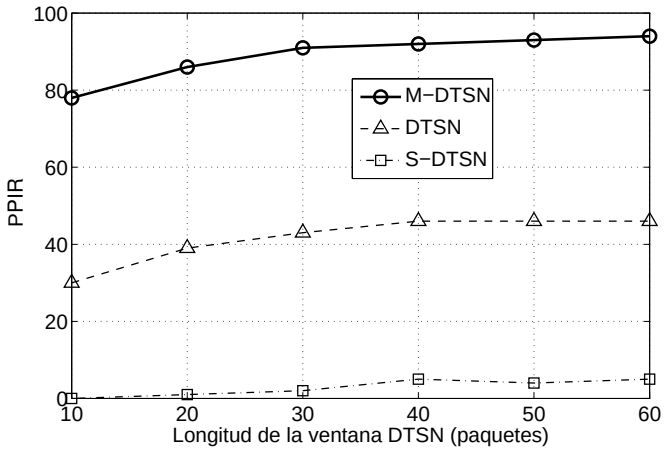


Figura 7: Comparación del rendimiento entre M-DTSN, DTSN y S-DTSN cuando varía el tamaño de la ventana DTSN: porcentaje promedio de imagen recibida para S=35KB y A=75dB.

y elige el máximo número de caminos entre todos los posibles para maximizar el rendimiento de la transmisión multimedia.

Por último, la codificación de red ha surgido como una alternativa al enrutamiento tradicional de paquetes y ha abierto una nueva área de investigación en la que pueden desarrollarse nuevos métodos y protocolos. Un trabajo reciente [17] proporciona una visión general de los principios de la codificación de red aplicada a las transmisión multimedia en los entornos aquí estudiados. También existen técnicas centradas en la planificación de políticas de transmisión con óptima tasa-distorsión dadas las condiciones de la red. Dichos esquemas tienen la ventaja de decidir qué paquete enviar a continuación, cuándo enviarlo, o no enviarlo (si se estima que va a llegar tarde o perderse), conociendo las características del flujo codificado (importancia relativa de los paquetes) y las condiciones de la red, de forma que se minimiza la distorsión observada en el receptor [18].

VI. Conclusiones y trabajo futuro

En este artículo se ha estudiado si es posible desarrollar protocolos de transporte dirigidos a optimizar el compromiso entre los requerimientos de tiempo real y la fiabilidad de la información multimedia, parcialmente tolerante a pérdidas y sensible a retardos, en WMSN. Se ha propuesto un mecanismo para el transmisor que es capaz de aumentar considerablemente la eficiencia de las transmisiones multimedia. Este mecanismo ha sido evaluado adaptando el protocolo de transporte fiable DTSN. La versión adaptada, M-DTSN ha demostrado ser mucho más efectiva en la transmisión de información multimedia. Además, se ha evaluado si esta aproximación funciona cuando se aplican técnicas de codificación de red conjuntamente con protocolos de transporte fiables en la capa inferior a la de nuestra solución, obteniendo la conclusión de que nuestra aproximación es sumamente beneficiosa en estos entornos.

Como trabajo futuro planeamos optimizar este mecanismo desarrollando algoritmos adaptativos capaces de seleccionar los valores de configuración apropiados de nuestra aproximación como una función de la evolución de la red y el receptor a lo largo del tiempo.

Agradecimientos

Este proyecto ha sido parcialmente financiado por el MICINN Español bajo el proyecto TEC2008-06663-C03-02 (70% fondos FEDER), the European Community Seventh Framework Programme bajo el acuerdo de concesión no. 225186, proyecto WSAN4CIP, y el Departamento de Ciencia y Tecnología de la Universidad de Filipinas a través de la concesión ERDT.

Referencias

[1] Shiwen Mao, D. Bushmitch, S. Narayanan, and S. Panwar, "MRTP: a multiflow real-time transport protocol for ad hoc networks," IEEE Transactions on Multimedia, vol. 8, 2006, pp. 356-369.

[2] L. Zhang, M. Hauswirth, L. Shu, Z. Zhou, V. Reynolds, and G. Han, "Multi-priority Multi-path Selection for Video Streaming in Wireless Multimedia Sensor Networks," Ubiquitous Intelligence and Computing, 2009, pp. 439-452

[3] F. Rocha, A. Grilo, P. Pereira, "Performance Evaluation of DTSN in Wireless Sensor Networks", Proceedings of the 4th EuroNGI Workshop on Wireless and Mobility, Barcelona, Spain, January 2008. In Springer-Verlag Lecture Notes in Computer Science, vol. 5122, 2008.

[4] X. Zhang, and X.-H. Peng, "A tested of erasure coding on video streaming system over lossy networks," in Proc. IEEE 7th International Symposium on Communications and Information Technologies (ISCIT), Oct. 2007

[5] "RTP: A Transport Protocol for Real-Time Applications," http://tools.ietf.org/rfc/rfc3550.txt.

[6] "Datagram Congestion Control Protocol (DCCP)," http://tools.ietf.org/rfc/rfc4340.txt.

[7] T. Braun, T. Voigt, and A. Dunkels, "TCP support for sensor networks," 2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services, Obergurgl, Tyrol, Austria: 2007, pp. 162-169.

[8] O. Akan and I. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 13, 2005, pp. 1003-1016.

[9] C. Wan, S.B. Eisenman, and A.T. Campbell, "CODA," Proceedings of the first international conference on Embedded networked sensor systems - SenSys '03, Los Angeles, California, USA: 2003, p. 266.

[10] C. Wang, K. Sohraby, and B. Li, "SenTCP: a hop-by-hop congestion control protocol for wireless sensor networks," Proc. IEEE INFOCOM 2005, March 2005.

[11] F. Stann and J. Heidemann, "RMST: reliable data transport in sensor networks," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003., Anchorage, AK, USA: , pp. 102-112.

[12] O. Akan, "Performance of Transport Protocols for Multimedia Communications in Wireless Sensor Networks," IEEE Communications Letters, vol. 11, 2007, pp. 826-828.

[13] B. Marchi, A. Grilo, and M. Nunes, "DTSN: Distributed Transport for Sensor Networks," 2007 IEEE Symposium on Computers and Communications, Santiago, Portugal: 2007, pp. 165-172.

[14] E. Giancoli, F. Jabour, and A. Pedroza, "CTCP: Reliable Transport Control Protocol for sensor networks," 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing. 2008, pp. 493-498.

[15] M.H. Yaghmaee and D. Adjeroh, "A reliable transport protocol for Wireless Sensor Networks," 2008 International Symposium on Telecommunications, Tehran: 2008, pp. 440-445.

[16] V.C. Gungor and Ö.B. Akan, "Delay aware reliable transport in wireless sensor networks," International Journal of Communication Systems, vol. 20, 2007, pp. 1155-1177.

[17] E. Magli and P. Frossard, "An overview of network coding for multimedia streaming," 2009 IEEE International Conference on Multimedia and Expo. 2009, pp. 1488-1491.

[18] Rate-distortion optimized scheduling for redundant video representation. IEEE Transactions on Image Processing archive V-18. H. Wang. A. Ortega.

ESTUDIO DEL RENDIMIENTO DE LA EMULACIÓN DE REDES EN ENTORNOS REALES

David Cortés-Polo, Alfonso Gazo-Cervero, José Luis González-Sánchez, Javier Carmona-Murillo.
Departamento de Ingeniería de Sistemas Informáticos y Telemáticos,
Universidad de Extremadura
Laboratorio GÍTACA, Escuela Politécnica de Cáceres.
Av. Universidad s/n. 10.003, Cáceres.
dcorpol@unex.es, agazo@unex.es, jlgs@unex.es.

***Resumen*- La emulación de redes se está convirtiendo desde hace varios años en una de las herramientas más potentes para el estudio y desarrollo de nuevos protocolos y aplicaciones de red. Debido a la capacidad de configuración y a la posibilidad de usar tráfico capturado en tiempo real, la emulación abre el abanico de posibilidades tanto a los investigadores y a la industria. Es por esto necesario estudiar el impacto de la emulación sobre los experimentos realizados y ver cómo influyen los parámetros de configuración en el resultado final de la emulación. En este artículo se presenta un estudio de las posibilidades de la emulación frente a los escenarios reales y cómo la emulación de red influye en el resultado final de los experimentos.**

***Palabras Clave*- Emulación de redes, ingeniería de protocolos, virtualización de redes, CBR, software libre, UDP.**

I. INTRODUCCIÓN

La emulación se puede definir como el proceso por el que un dispositivo es capaz de comportarse como otro. De manera genérica, un emulador copia (provee una emulación de) las funcionalidades de otro sistema completamente distinto a las que originariamente posee el emulador, de manera que el primer sistema "parece" que se comporta como el segundo.

La simulación y la emulación de redes son dos de las herramientas más usadas para el diseño y la validación de protocolos y aplicaciones de red.

La mayor diferencia entre estas técnicas es que la primera es un software que simula el comportamiento de la red, mientras que la segunda es capaz de comportarse como el original. Por lo tanto es muy importante validar cómo se comporta la emulación de redes comparado los dispositivos originales.

Este trabajo por lo tanto, analiza las ventajas y desventajas de usar la emulación de redes comparando con el comportamiento de un conjunto de redes reales y su "copia" emulada.

Para ello se usan varias métricas que permiten medir el rendimiento de IP en una comunicación. Estas métricas son el delay extremo a extremo (One-Way-Delay, OWD) [1], el jitter (Inter-Packet Delay Variation, IPDV) [2] y el ratio de périda de paquetes (Packet Loss Ratio, PLR) [3]. Estas métricas son consideradas como los estándares para medir el rendimiento de los servicios de transporte de datos en Internet.

El resto del artículo se estructura de la siguiente manera: en el segundo punto se explica las bases de la emulación de escenarios de red; el tercer punto recoge el caso de estudio que se ha utilizado de base, así como las aplicaciones usadas para ello; seguidamente en el punto cuatro se muestra la evaluación y los resultados obtenidos al realizar diferentes experimentos sobre el caso de estudio propuesto; en el punto cinco se exponen las conclusiones obtenidas y el trabajo futuro de esta investigación.

II. EMULACIÓN DE REDES

La emulación de red, como se ha dicho anteriormente, permite interactuar con el mundo real. Es decir, permite tratar tráfico generado en sistemas que no pertenecen al plano emulado (mundo real) y aplicarle parámetros de QoS (Quality of Service) modelados como el delay y tasa de pérdida en un flujo de datos.

Del párrafo anterior se puede obtener una primera clasificación de los distintos tipos de emuladores de red. Dependiendo de si el emulador está implementado usando un dispositivo hardware o por el contrario es un software que simule el comportamiento de la red, se puede clasificar a los emuladores como *emulador hardware* o *emulador software*.

Los *emuladores hardware* pueden ser implementados usando una única máquina o un clúster de máquinas. Estas máquinas pueden ser máquinas físicas o emuladas dentro de un *host* (o máquina anfitriona).

Los *emuladores software* son emuladores basados en simuladores, de manera que no usan máquinas reales sino software preparado para la simulación de redes. Normalmente son simuladores paralelos que pueden ejecutarse en un único nodo, un clúster de estaciones de trabajo o en máquinas de memoria compartida para simular una red virtual y la interfaz con el tráfico que proviene del entorno no emulado.

III. CASO DE ESTUDIO

En el segundo punto se ha desarrollado el concepto de emulación de red. La emulación se basa por tanto, en el tratamiento de flujos de datos obtenidos fuera del plano de emulación, y una vez tratado esos flujos, devolverlos fuera del mismo.

En este trabajo se presentan las ventajas y desventajas de usar la emulación frente a las mediciones obtenidas de las redes reales. Para ello, en el siguiente subapartado se detalla el test-bed usado, así como la metodología con la que se han obtenido los datos que serán procesados y los cuales serán los que se comparen en el artículo.

A. *Test-Bed*

La Figura 1 muestra los escenarios propuestos para evaluar el comportamiento de la emulación sobre las redes reales.

El primer escenario es la conexión del emisor y receptor a través de un equipo que ejecuta una distribución de Linux llamada Vyatta[4], con capacidades de routing.

El segundo escenario es la evaluación del emulador. Para la evaluación se utiliza el mismo equipo que ha sido usado en el primer escenario. Esta vez la máquina no ejecuta la distribución Vyatta de manera nativa, sino que se usa un emulador para que se ejecute la misma.

El sistema operativo que implementa la máquina host es Ubuntu 9.10 y el emulador sobre el que corre la distribución Vyatta es VirtualBox-OSE.

Tanto el emisor como el receptor se conectan a los puertos Ethernet de la máquina host. Estos puertos están comunicados con dos interfaces virtuales de la máquina emulada mediante dos bridges software que permite la obtención del flujo de datos del exterior al emulador.

En todos los experimentos, el nodo emisor como el receptor ejecutan la aplicación TCPDump[5], la cual es una aplicación basada en PCAP y que permite la captura del tráfico para su posterior análisis.

La sincronización de los relojes de los equipos se ha realizado a través de NTP [6]. NTP permite la sincronización del reloj del kernel del sistema operativo mediante el intercambio de mensajes con un servidor NTP.

Para acelerar la sincronización de los relojes tanto del emisor como del receptor con el servidor de NTP, se ha rebajado el intercambio de mensajes a 16 segundos, de manera que se consigue la sincronización con una tasa de error por debajo a 1 ms en un tiempo más rápido que al usar la tasa original (de 60 segundos) de intercambio de mensajes.

Una vez que se comienza a ejecutar el escenario, la sincronización con NTP se desactiva para evitar correcciones en el reloj que puedan influir en el timestamp de los paquetes.

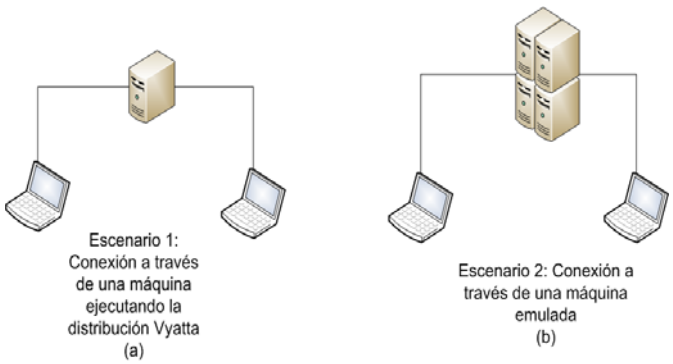


Figura 1: Escenarios de Test-Bed

B. *Metodología de medición*

El principal objetivo de las pruebas que se han realizado es la obtención de las siguientes medidas: Delay del paquete extremo a extremo (One-Way-Delay, OWD), Jitter del paquete (IP Delay Variation) y porcentaje de pérdida de paquetes (Packet Loss Ratio, PLR).

El delay del paquete extremo a extremo representa el tiempo que tarda el paquete desde que se envía por el emisor hasta que lo recibe el equipo receptor de la comunicación.

El jitter se refiere a la variación del delay del paquete con respecto al paquete anterior. En este caso todos los paquetes pertenecen al mismo flujo de datos ya que sólo se va a estar transmitiendo un único flujo en el escenario.

Por último, el porcentaje de pérdida de paquetes que es el ratio de paquetes que se pierden con respecto al total de paquetes enviados por el origen.

El tráfico se ha generado usando la herramienta Mausezahn [7]. Para ello el emisor del flujo de datos, ejecuta el generador de tráfico, mientras que el receptor ejecuta un destino de tráfico el cual también lo implementa la misma herramienta.

Al usar un generador de tráfico se puede estimar el rendimiento de la red gracias a que los parámetros del flujo creado por el generador, los cuales son definidos de antemano. Para ello se ha usado un tráfico CBR (Constant Bit Rate) usando UDP (User Datagram Protocol) como protocolo de transporte.

C. *Caracterización de la información enviada*

La información que se transmite es un flujo UDP como se ha dicho anteriormente. El tamaño de paquete es de 1372 Bytes y se envía cada uno a un intervalo de 21 µs. Estos parámetros han sido calculados para obtener una velocidad de transmisión de aproximadamente 60Mb/s. De manera que el flujo de datos transmitido fuera considerable pero no llegase a sobrepasar la capacidad del hardware de red usado que es de 100 Mb/s.

Para que el timestamp de los paquetes tanto emitidos como recibidos no se vean afectados por la deriva del reloj (ya que en el momento de la realización de los experimentos no se mantiene la sincronización NTP entre los extremos), se van a realizar pruebas lo suficientemente pequeñas para evitar ese efecto, pero que tengan un número de paquetes significativo para su estudio. Es por esto que se ha llegado a la convención de capturar 12000 paquetes para su estudio.

IV. Resultados

En este apartado se van a mostrar los resultados obtenidos en los escenarios expuestos en el apartado anterior, así como una comparativa para buscar similitudes y diferencias entre la emulación y los escenarios usando elementos reales.

A. *Escenario 0: Delay y Jitter introducido por los dispositivos hardware*

En la siguiente tabla se muestran los valores base de delay y jitter que se le introduce a un paquete cuando tiene que atravesar un dispositivo hardware (un switch Ethernet).

Los valores registrados en la Figura 2 y en Tabla 1, serán tomados como base para realizar la comparativa.

Tabla 1: Valores estadísticos de las métricas del escenario usando un dispositivo hardware (switch Ethernet)

Métrica	Max	Media	Min	Desv
Delay Paquete	0, 019611	0, 01332290	0, 018367	0, 003197
Jitter Paquete	0, 011456	0, 00271955	0	0, 001681

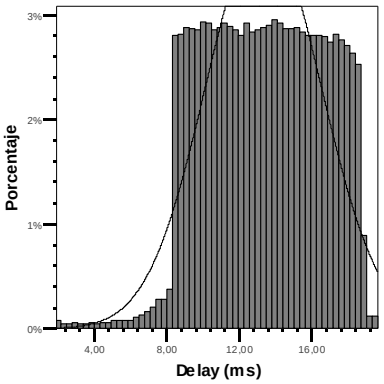


Figura 2: Gráfico de distribución del delay en el escenario base

B. Escenario 1: Interconexión a través de un router hardware

En este escenario se muestra el delay y el jitter que se le introduce a los paquetes al atravesar un router hardware. Para la configuración del router se ha usado una distribución Vyatta sobre un equipo que interconecta al emisor y al receptor a través de dos puertos Ethernet.

La siguiente tabla muestra los valores estadísticos de las métricas del rendimiento en el escenario propuesto. El porcentaje de pérdidas se mantiene a 0% en esta prueba al igual que en la tabla anterior. Esto se ha podido estudiar gracias al campo identificación de los paquetes IP y de esta manera se puede calcular el número de paquetes que no llegan a su destino o llegan duplicados.

Tabla 2: Valores estadísticos de las métricas del escenario usando un router ejecutado sobre la máquina.

Métrica	Max	Media	Min	Desv
Delay Paquete	0,020456	0,01386815	0,001057	0,00318375
Jitter Paquete	0,012811	0,00269717	0	0,00169143

Al comparar las métricas de este escenario con los valores estadísticos de la aproximación base, se puede observar que el valor del delay medio se ha incrementado en 0, 54 ms. De igual forma el jitter de los paquetes se ha decrementado en 0,02 ms.

La Figura 3 muestra la dispersión del retardo, la mayor parte de los paquetes experimentan un retardo entorno al 15 ms.

Como conclusión del análisis de los valores estadísticos de las métricas se puede advertir un aumento en el delay experimentado (se observa en los valores máximos y mínimos del delay de los paquetes) debido a tener que atravesar un equipo que implementa la pila TCP/IP con lo que el paquete al ser almacenado en el buffer de la máquina que interconecta el recptor y el emisor, introduce un retardo a la comunicación.

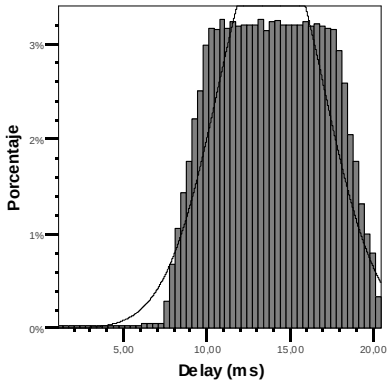


Figura 3: Gráfico de distribución del delay en el escenario 1

C. Escenario 2: Interconexión a través de un router emulado

En este escenario se realiza la medición del jitter y el delay de los paquetes al atravesar un router emulado sobre una máquina virtual.

Para ello se conecta a los puertos Ethernet de la máquina host los equipos emisor y receptor de la comunicación. Estos dos puertos estarán interconectados a la máquina virtual de manera que pueda obtener los paquetes de la red real y procesarlos.

Con esta aproximación se pueden tomar medidas con TCPDump tanto en los extremos de la comunicación como en los dos puertos físicos de la máquina host. Esto es lo que se muestra en Tabla 3. El delay y el jitter del paquete corresponde a los extremos del a comunicación, mientras que el delay y el jitter en emulador corresponde a las interfaces de la máquina host.

Tabla 3: Valores estadísticos de las métricas del escenario usando la máquina emulada.

Métrica	Max	Media	Min	Desv
Delay Paquete	0, 036076	0, 02233877	0, 001469	0, 0059751
Jitter Paquete	0, 020870	0, 00495575	0, 000003	0, 0033377
Delay en emulador	0,017571	0,00170350	0,000034	0,00272419
Jitter en emulador	0,015885	0,00163372	0,000002	0,00217997

En esta prueba al igual que en las anteriores, no se ha perdido ningún paquete, ya que es el único flujo de datos que la red gestiona y no sobrepasa los límites físicos de los dispositivos.

En la Tabla 3 al poder realizar las capturas del tráfico en varios puntos del escenario, se puede calcular las métricas no sólo extremo a extremo sino las introducidas por el emulador.

Como se puede observar la comunicación usando una máquina emulada aumenta el delay de la comunicación 10 ms. Es decir aumenta más de un 150% el delay de los paquetes. Esto mismo se puede observar al comparar el jitter

obtenido de las métricas en el escenario 2 con respecto al escenario 0.

Esto se ve reflejado en la Figura 4 y Figura 5 que muestra el delay que experimentan los paquetes tanto en extremo a extremo como en las interfaces del emulador.

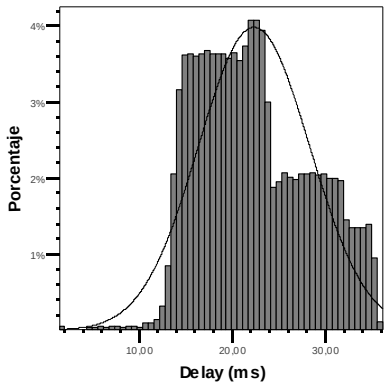


Figura 4: Gráfico de distribución del delay en el escenario 2

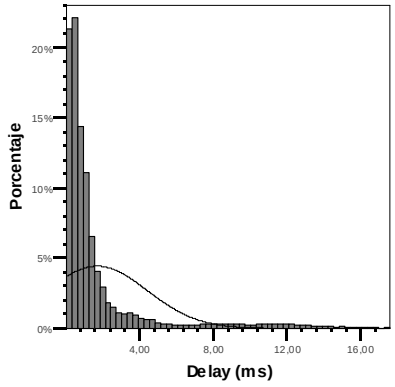


Figura 5: Gráfica de distribución del delay escenario 2 (interfaz host)

La gráfica anterior muestra la distribución del delay de la prueba. Si se compara ésta gráfica con respecto a la de prueba anterior, se puede observar que hay un conjunto de paquetes que se ven afectados por un delay más alto. Esto es debido a que el emulador se ha visto saturado por la cantidad de paquetes que se han transmitido en la prueba.

Las siguientes figuras muestran las estadísticas en las interfaces Ethernet de la máquina host.

La Figura 5 muestra la información del delay en la máquina host del emulador. La gráfica coincide con las anomalías mostradas en la Figura 4 y lo observado en la Tabla 3.

La mayor parte de los paquetes experimentan un delay en torno a 1 ó 2 ms. Estos paquetes son los que coinciden con el delay general de 20ms extremo a extremo de media.

La anomalía se produce en el conjunto de paquetes (aproximadadamente 30% de los paquetes) que sufre un delay mayor a 4 ms de forma que estos paquetes son los que se ven perjudicados en las esperas en el emulador y lo que produce un delay de más de 30 ms extremo a extremo en la comunicación.

Por último, la Figura 6 muestra la comparativa de las tres pruebas de manera que se puede observar que el delay experimentado al atravesar un router o un switch es muy similar, mientras que al atravesar un router emulado, los paquetes se ven penalizados con un delay mucho mayor.

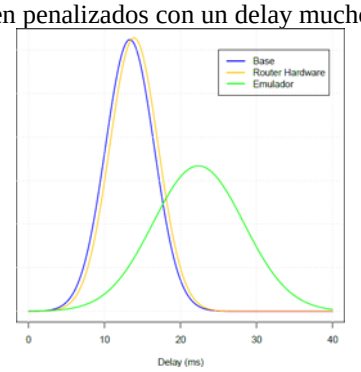


Figura 6: Comparación de la distribución de las tres pruebas

V. Conclusiones y trabajo futuro

En este artículo se han presentado un conjunto de escenarios con los que evaluar el comportamiento de los emuladores de red. Para ello se han usado diversas medidas que han ayudado a caracterizar el comportamiento del tráfico.

Se ha podido observar el incremento del delay de un router hardware a un dispositivo dedicado (switch Ethernet) es de un 4.7%, como se puede observar en la Figura 6. Este incremento es mínimo si se compara con el incremento que se observa en la máquina emulada que está en torno al 41%.

Este resultado es debido a la gestión de los paquetes en la máquina virtual que produce un delay extremo a extremo.

El trabajo futuro a esta investigación es la necesidad de métricas que permitan relacionar la efectividad de la emulación en relación con los recursos asignados a cada máquina emulada.

Agradecimientos

Este trabajo ha sido financiado en parte por la Consejería de Economía, Comercio e Innovación de la Junta de Extremadura y el Fondo Europeo de Desarrollo Regional (FEDER) mediante el proyecto Com.Info.Com, PDT09A047.

Referencias

[1] G. Almes, S. Kalidindi and M. Zekauskas, A One-way Delay Metric for IPPM, Request for Comments 2679, September 1999

[2] C. Demichelis and P. Chimento, IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), Request for Comments 3393, November 2002.

[3] G. Almes, S. Kalidindi and M. Zekauskas, A One-way Packet Loss Metric for IPPM, Request for Comments 2680, September 1999

[4] Vyatta open source routers, http://www.vyatta.com/

[5] LibPCAP, http://www.tcpdump.org/

[6] Carsten Rieck, An Approach to Primary NTP by Using the LINUX Kernel, Frequency Control Symposium, 2007

[7] Mausezahn, http://www.perihel.at/sec/mz/

[8] Patrik Arlos and Markus Fiedler, A Method to Estimate the Timestamp Accuracy of Measurement Hardware and Software Tools, PAM 2007, LNCS 4427, pp. 197–206, Springer-Verlag Berlin Heidelberg 2007

La plataforma de metadatos CAM y su aplicación al streaming de vídeo adaptativo

Pedro A. Tudela Solano, Eduardo Martínez Graciá, Antonio F. Gómez Skarmeta.
Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia
Facultad de Informática. Campus de Espinardo. 30071 Murcia.
pedroantonio@um.es, edumart@um.es, skarmeta@um.es

***Resumen*- Este artículo describe un nuevo modelo de metadatos (meta-modelo) para la descripción genérica de contenidos multimedia, llamado CAM (Content Aggregated Multimedia), y su aplicación a la adaptación de streaming de vídeo en tiempo real. El meta-modelo no sólo maneja información sobre el contenido multimedia, sino que también puede describir servicios auxiliares para su manipulación, así como el contexto en el que se realiza la entrega de la información (dispositivo del usuario y red). El meta-modelo ha sido diseñado para poder ser fácilmente extendido con nueva información o estándares suplementarios. El artículo muestra la aplicación del meta-modelo en la adaptación de flujos de vídeo transmitidos por streaming. Este meta-modelo ha sido desarrollado dentro del proyecto CAM4HOME, Collaborative Aggregated Multimedia for Digial Home (TSI-020400-2008-80), subvencionado por el Ministerio de Industria, Turismo y Comercio.**

***Palabras Clave*-metadatos, multimedia, streaming, adaptación.**

I. INTRODUCCIÓN

El rápido desarrollo de las infraestructuras de red, y de la capacidad de almacenamiento y de procesamiento de los equipos informáticos, está incrementando el uso de los servicios multimedia a través de redes de datos, abarcando áreas como la vídeo conferencia, los servicios de vídeo bajo demanda, o la difusión de televisión en alta definición.

Este nuevo tipo de sistemas multimedia ubicuos requieren un ajuste de los contenidos a las distintas restricciones de los terminales y redes, así como a las preferencias del usuario, manteniendo la mejor calidad posible en el dispositivo receptor. Para realizar esta función, los servicios de transmisión necesitan acceder a la información que describe el contenido y el contexto de la transmisión. Esta información debe estar en un formato aceptado por los dispositivos y servicios participantes en el proceso de transmisión.

Existen varios estándares dedicados a la descripción del contenido multimedia, su estructura o su ciclo de vida, pero no existe un estándar de metadatos único que contemple por completo cada uno de estos campos. Varios autores [1][2] consideran que es necesaria una armonización de los estándares existentes, y que esta armonización necesita basarse en un desarrollo modular que permita una extensión específica de cada aplicación. Las tecnologías de la web semántica son idóneas para abordar este objetivo, ya que fueron diseñadas con criterios de extensibilidad y flexibilidad. Por ello, el modelo de metadatos CAM, desarrollado en el proyecto ITEA2 CAM4HOME [3], se basa en las tecnologías desarrolladas para la web semántica, y pretende producir un marco de desarrollo de aplicaciones multimedia que tengan requisitos de manipulación de metadatos en alguno de los ámbitos indicados.

La transmisión de vídeo mediante técnicas de streaming es un ejemplo de aplicación multimedia en la que es interesante aplicar técnicas de adaptación basadas en los metadatos CAM. El concepto de MANE (Media Aware Network Element) se refiere a un tipo de nodo, situado en un punto intermedio entre el transmisor y el receptor, que es capaz de realizar alguna manipulación sobre los datos transmitidos. En el caso del servicio de streaming, se puede implementar un MANE mediante un proxy RTSP [4], capaz de transcodificar el flujo de vídeo de acuerdo con las condiciones del contexto en el que se produce la transmisión.

El resto del artículo está estructurado de la siguiente forma: en la sección II se describen el modelo de metadatos CAM; en la sección III se presenta la plataforma de servicios implementada para manipular e interpretar estos metadatos; la sección IV describe el servicio de streaming adaptativo; finalmente, la sección V presenta las conclusiones obtenidas.

II. MODELO DE METADATOS CAM

El objetivo del proyecto CAM4HOME es la creación de un marco para la distribución de contenidos multimedia que se apoye en la disponibilidad de metadatos, permitiendo así tanto a los usuarios finales como a los proveedores de contenidos comerciales la creación y el suministro de productos multimedia de valor añadido. Estos productos se basan en el concepto de paquete de contenidos multimedia colaborativo. Precisamente, el término CAM (Collaborative Aggregated Multimedia) hace referencia a esta agrupación como un conjunto de contenidos y servicios relacionados, coherentes a nivel semántico.

El meta-modelo CAM está constituido por una serie de conceptos y reglas semánticas que garantizan la coherencia en el uso de dichos conceptos. Está diseñado para ser extensible y para permitir una encapsulación sencilla de otros formatos de metadatos externos. La extensibilidad se basa en la construcción del meta-modelo de forma jerárquica.

Todo el meta-modelo se apoya en una descripción de alto nivel, denominada CAM Abstract Metamodel, que define las construcciones y asociaciones básicas en un nivel abstracto. Este nivel actúa como conector de las restantes categorías del meta-modelo, facilitando su extensión. El

diseño de bajo nivel del meta-modelo se encuentran en tres categorías: CAM Core Metamodel, CAM Supplementary Metamodel y CAM External Metamodel.

La mayor parte del meta-modelo está contenida en el bloque CAM Core Metadata, dedicado a la descripción de las entidades fundamentales manejadas en el proyecto. El meta-modelo define los metadatos que se pueden asociar a estas entidades, las operaciones implicadas en el ciclo de vida de éstos, y las reglas de integridad de dichas operaciones.

El bloque denominado CAM Supplementary Metadata incluye la definición de perfiles de metadatos de dispositivos, redes de transmisión y usuarios, es decir, especifica los metadatos requeridos para permitir la interoperabilidad entre las aplicaciones que consumen los contenidos y la plataforma CAM. El meta-modelo se completa con la definición del bloque CAM External Metadata, que actúa como un interfaz con los metadatos externos, como MPEG-7 [5] o SMIL [6].

A. **Conceptos básicos definidos en el meta-modelo**

La Fig. 1 representa la relación entre los conceptos más importantes definidos en el meta-modelo.

Un elemento CAM (CAMElement) se define como una unidad atómica de agregación. Representa a un ítem de tipo vídeo, audio, imagen, documento, o aplicación descargable, o bien a un servicio accesible por red. Un elemento CAM dispone de una referencia (EssenceFileIdentifier) en formato URI, que apunta al fichero físico descargable que lo contiene, a un servicio de streaming que lo transmite bajo demanda, etc.

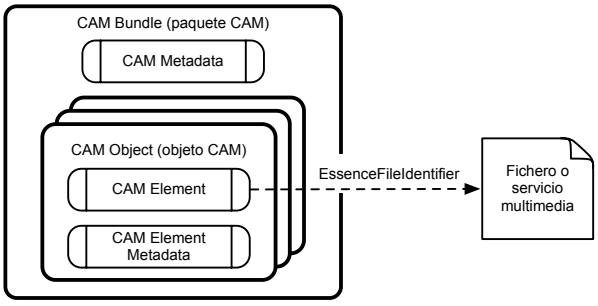


Fig. 1. Visión conceptual de la agregación de objetos en paquetes.

Por otra parte, los elementos CAM tienen asociados una serie de metadatos (CAMElementMetadata) que los describen. Cada instancia de metadato se identifica a través de un identificador (CAMElementMetadataID), y un número de versión (VersionNumber) que se actualiza al modificar el metadato. Denominamos objeto CAM (CAMObject) a la unión de un elemento CAM y los metadatos que lo describen.

Un paquete CAM (CAMBundle) define una agregación de objetos CAM, vinculados entre sí empleando alguno de los tipos de relación definidos en el meta-modelo. Se permite que un mismo objeto sea referenciado desde múltiples paquetes, fomentando así la reutilización de contenidos. Los paquetes CAM pueden ser descritos con metadatos que permiten caracterizar, en su conjunto, los objetos que contienen.

B. **Implementación del meta-modelo**

Para la realización técnica del modelo de metadatos, se ha escogido la representación basada en RDF Schema (RDFS) [7]. Las entidades presentes en el meta-modelo se han traducido en instancias de rdf:Class, y las relaciones se han implementado mediante rdf:Property. Las descripciones de los recursos se han realizado mediante sentencias RDF.

En la raíz del meta-modelo se define la clase de CAM abstract llamada ContentFeatureMetadataContainter. De esta clase abstracta hereda cualquier clase que contenga propiedades (features). Las propiedades pueden ser de dos tipos: las propiedades simples (simpleFeatureMetadata) representables con alguno de los tipos básicos de XML; las propiedades complejas (ContentFeatureMetadata) se definen con clases RDFS.

La clase CAMElementMetadata se define como una clase de CAM Core que representa los metadatos de cualquier elemento atómico definido en el entorno de CAM4HOME. Una propiedad simple de esta clase es el título (title), representado con un string. Por otra parte, una propiedad compleja se define con hasAppearingConcept, que puede ser un objeto identificable, como una persona, o algo más abstracto, como la naturaleza o los deportes.

La Fig. 2a muestra un ejemplo de instanciación de las clases y propiedades del meta-modelo en un documento RDF. Un objeto de tipo vídeo dispone de una referencia al fichero que lo contiene a través de la propiedad isMetadataOf.

En la Fig. 2b también se muestra un paquete CAM que contiene a este objeto de vídeo, enlazado a través de la propiedad containsCAMObjectReference, cuyo valor coincide con el identificador de la instancia del objeto.

a) Definición de un vídeo

```
<rdf:RDF ...>
 <core:VideoElementMetadata rdf:about="&inst;O;Ob2;1">
  <core:title>A sunny weekend</core:title>
  <core:creatorReference>c4h:John</core:creatorReference>
  <core:legalNotice>free</core:legalNotice>
  <core:hasAppearingConcept rdf:nodeID="AP"/>
  <core:isMetadataOf rdf:nodeID="VE1">   ...
 </core:VideoElementMetadata>
 <core:AppearingConcept rdf:nodeID="AP">
   <core:name>fish</core:name>  ...
 </core:AppearingConcept>
 <core:VideoElement rdf:nodeID="AP1">
  <core:essenceFileIdentifier>
    http://homedomain.net/fishing-video </...>
 </core:VideoElement>
</rdf:RDF>
```

b) Definición de paquete con dos objetos

```
<rdf:RDF ...>
 <core:CAMBundleMetadata rdf:about="&inst;B;Bdl1;1">
  <core:containsCAMObjectReference>O;Ob1;1</...>
  <core:containsCAMObjectReference>O;Ob2;1</...>
  <core:hasSharedSocialTags rdf:nodeID="CCMetadata1"/>
 </core:CAMBundleMetadata>
 <core:SharedSocialTags rdf:nodeID="CCMetadata1">
  <core:serverURI>http://c4h.org/tags</core:serverURI>
  <core:hasSocialTag rdf:resource="#catching"/>
  <core:hasSocialTag rdf:resource="#fishing"/>
 </core:SharedSocialTags>
</rdf:RDF>
```

Fig. 2. Instanciación de objetos y paquetes CAM

Para implementar la persistencia de las descripciones RDF, el proyecto optó por emplear Jena [8]. Se trata de un marco de desarrollo para construir aplicaciones basadas en las tecnologías de la web semántica. Incluye un interfaz de

programación Java para el almacenamiento y recuperación de los datos en formato RDF/XML, así como un motor SPARQL [9] que permite la realización de potentes operaciones de búsqueda. Para facilitar el desarrollo de aplicaciones que manejen el modelo de metadatos propuesto, se han implementado una serie de servicios web que permiten aislar las operaciones de manejo de la plataforma Jena.

III. ARQUITECTURA DE SERVICIOS

La arquitectura del proyecto CAM4HOME presenta un entorno coherente e integrado del sistema a partir de una visión de computación orientada a servicios.

Se definen dos categorías principales de servicios: de usuario y de software. Los servicios de usuario incluyen servicios proporcionados a los usuarios humanos de la plataforma a través de interfaces o clientes software, como puede ser un navegador web o un cliente software específico. La categoría de servicios software está integrada por servicios que se proporcionan a las entidades de cómputo de la plataforma, por ejemplo, software ejecutable dentro del sistema distribuido CAM4HOME, o servicios auxiliares que permiten la implementación y ejecución de servicios de usuario. Entre las categorías más relevantes de los servicios software podemos destacar las siguientes:

- *Metadata Services*. Son servicios para el tratamiento y procesamiento de los metadados definidos en el meta-modelo. También se incluyen en esta categoría los servicios dedicados al registro y búsqueda de metadatos dentro de la base de datos de CAM4Home.
- *Content and Network Services*. Utilizados para la entrega y manipulación de contenido multimedia, así como para la gestión de la red y la calidad de servicio. Dentro de esta categoría de servicios se encuentra el servicio Cross-Delivery Streaming, cuya función es coordinar la entrega de objetos CAM mediante streaming.

IV. STREAMING ADAPTATIVO

Una de las principales novedades que aporta el proyecto CAM4HOME es el proceso de streaming adaptativo, que puede ser utilizado por los usuarios para extender su experiencia a distintos tipos de dispositivos. El objetivo es modelar el flujo de streaming para utilizar, de manera eficiente, los recursos de los que dispone el usuario para la reproducción de vídeo.

La arquitectura general del sistema utilizada para realizar el streaming adaptativo se puede observar en la Fig. 3. Cuando el usuario desea hacer uso del servicio de streaming, accede a una interfaz web que integra un plugin de QuickTime [10] para la reproducción de streaming vía RTSP, junto con una aplicación Flash que permite navegar en el directorio de CAM4home en busca de contenidos multimedia utilizando los servicios CAM Object/Bundle Search, y una vez obtenidos estos contenidos, modificar sus atributos de visualización para adaptarlos a las preferencias del usuario. Además, es la encargada de llevar a cabo el proceso de comunicación con el servicio Cross Delivery Streaming para la gestión de sesiones, y de controlar el reproductor QuickTime mediante JavaScript: este plugin proporciona una API para reproducir el vídeo, pausar, reiniciar, etc.

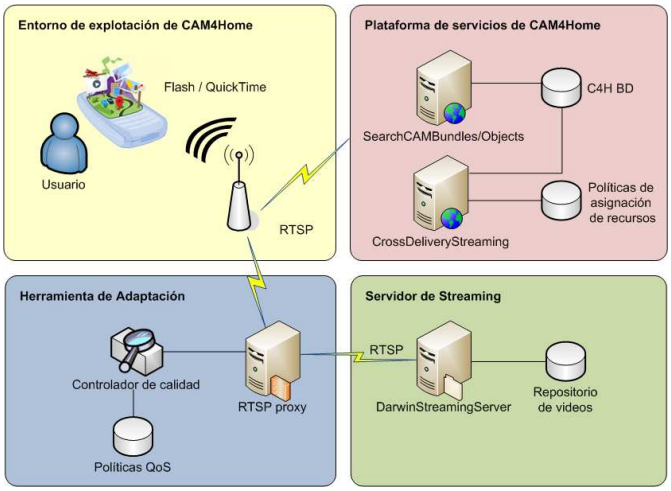


Fig. 3. Arquitectura general del proceso de straming adaptativo

A. Servicio Cross-Delivery Streaming

Este servicio proporciona los mecanismos necesarios para establecer un flujo de streaming de vídeo entre dos nodos, independientemente de las redes en que residen, proporcionando una capa de abstracción de los dominios de red en el ecosistema CAM4HOME. El primero de estos nodos es el cliente del servicio, cuya conexión se establece directamente con el servidor de streaming, si no es necesaria ninguna adaptación, o con un proxy RTSP en caso contrario. De cualquier modo, la designación o no de un elemento intermedio se realiza siempre de manera transparente al usuario, y la decisión de introducirlo se evalúa en el servicio de acuerdo con los metadatos del vídeo solicitado, junto con la descripción del perfil del dispositivo receptor.

El sistema CAM4Home puede estar compuesto por varios proxys RTSP. El servicio Cross-Delivery Streaming establece un conjunto de reglas que definen la política de asignación del proxy que será asociado a cada sesión. Esta decisión se toma en base a ciertos parámetros del proxy: la capacidad de cómputo, sesiones activas, el consumo actual de recursos, etc.

B. Proxy RTSP

Para que la adaptación de vídeo se realice de forma transparente, y para mantener desacoplada la gestión de sesiones del proceso de adaptación en sí, se ha optado por introducir un MANE en forma de proxy RTSP, encargado de la manipulación del flujo de streaming de vídeo entre servidor y cliente. El proxy RTSP permite la adaptación de vídeo H.264/AVC [11], mediante la transcodificación del flujo de vídeo original, a un nuevo flujo cuyas características se adapten al dispositivo receptor y a las condiciones de red.

La adaptación de vídeo se realiza sobre la base de ciertos parámetros del meta-modelo CAM (C4HDeviceProfile), que son comunicados al proxy junto con el identificador de sesión establecido por el servicio de streaming: el *BitRate*, que establece la tasa de bits por unidad de tiempo, el *DisplaySize*, que define la resolución del vídeo, y el *RefreshRate* que define la frecuencia de reproducción de las imágenes.

Durante la comunicación RTSP, el servidor envía al cliente las características del vídeo empleando el formato

SDP (Session Description Protocol) [12]. En esta descripción también se encuentran los parámetros de decodificación del vídeo original. Estos parámetros se denominan *SPS* (Sequence Parameter Set) y *PPS* (Picture Parameter Set). La modificación del vídeo supone la necesidad de sustituir los parámetros del SDP original por unos nuevos, correspondientes a la configuración del codec en el proxy.

La adaptación del streaming de vídeo inicia un proceso de transcodificación *on-line*, pues la adaptación se realiza conforme se recibe el flujo de datos. Este proceso se puede dividir en cinco etapas: en la primera fase se lleva acabo la *depaquetización* de los paquetes RTP [13] que contienen las unidades NAL [11] que componen cada uno de los frames del vídeo. Posteriormente, se *decodifica* cada uno de estos frames, y son *reescalados* a la nueva resolución especificada en el perfil de usuario. El siguiente paso es la *codificación* de los frames utilizando los nuevos valores bitRate y refreshRate para, por último, *paquetizar* las unidades NAL obtenidas siguiendo las especificaciones definidas en [14].

Durante el proceso de adaptación, se pueden producir cambios en el contexto en el que se desarrolla la sesión de streaming, véase congestión en la red, cambio de interfaz de red del usuario, etc. Estas situaciones pueden provocar una disminución sustancial de calidad de recepción del vídeo. Para paliar este tipo de problemas, el proxy incorpora un sistema de ajuste de parámetros dinámico que es capaz de modificar ciertos atributos de codificación de manera eficaz.

En la Fig. 4 se ilustra como evoluciona el bitRate y la calidad de vídeo obtenida a la salida del proxy para un vídeo H.264/AVC, con resolución original 720x576, 25 frames por segundo y 4 Mbps, en el transcurso de una sesión de streaming utilizando una red EDGE y un dispositivo IPhone.

La calidad del vídeo se estima utilizando la medida PSNR (Peak Signal-to-Noise Ratio), que establece la calidad de la reconstrucción en el ámbito de la compresión de imágenes. La variación del flujo de streaming se lleva a cabo variando el bitRate y el refreshRate, garantizando que el PSNR se mantenga por encima del umbral de calidad. El proceso de adaptación mostrado en la Fig. 4 se divide en cuatro fases:

1. El bitRate es muy elevado para la tecnología de red utilizada, y se producen pérdidas y retrasos en la entrega de paquetes. Esta información se obtiene a través de los informes RTCP [13], y se decide decrementar el bitRate medio especificado en la codificación en 1/3.
2. Los valores de salida de bitRate siguen siendo mayores de los soportados por la red. El controlador opta por disminuir otra vez el bitRate, ya que la calidad de señal sigue siendo buena, por encima de 35 dB.
3. Durante esta etapa se produce una disminución en la calidad de imagen, bajando hasta los 25 dB. El controlador toma medidas, y disminuye el ratio de refresco del vídeo a la mitad para mantener la calidad.
4. En la última etapa, ambos valores permanecen estables y dentro de los valores establecidos.

V. CONCLUSIONES

El meta-modelo CAM, descrito en este artículo, facilita el despliegue homogéneo de contenidos y servicios agregados en paquetes. El modelo de metadatos provee información suficiente para abordar los retos de la distribución de contenidos multimedia en una plataforma distribuída. No sólo proporciona un nuevo modo de plantear la creación y distribución de contenidos multimedia, sino que permite afrontar el desarrollo de servicios de distribución que garanticen la calidad de la recepción en diversos terminales y redes en las que se producen fluctuaciones dinámicas de sus parámetros de rendimiento. Se ha desarrollado un sistema prototipo que permite dar un valor añadido al servicio básico de streaming basado en el protocolo RTSP. Entre los objetivos futuros del proyecto se encuentra la apertura de la plataforma de metadatos a la comunidad de programadores, a través del portal CAM4Home Open Platform.

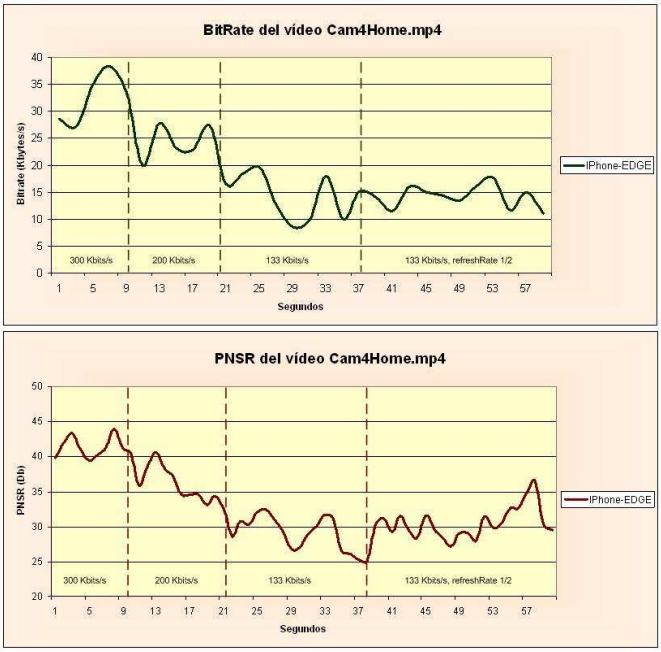


Fig. 4. BitRate y calidad de vídeo de salida durante el proceso de adaptación

REFERENCIAS

[1] Smith, J. R. and Schirling, P. 2006. Metadata Standards Roundup. *IEEE MultiMedia* 13, 2 (Apr. 2006), 84-88.

[2] Pereira, F. Vetro, A. Sikora, T. Multimedia Retrieval and Delivery: Essential Metadata Challenges and Standards. *Proceedings of the IEEE*, vol. 96, issue 4, April 2008.

[3] CAM4Home Open Platform. Collaborative Aggregated Multimedia for Digital Home. [Online]: http://openplatform.cam4home.fi

[4] IETF RFC 2326. Real Time Streaming Protocol (RTSP). [Online]: http://www.ietf.org/rfc/rfc2326.txt

[5] ISO/IEC 15938-1:2002, Information technology - Multimedia content description interface Part 1: Systems. Geneva, Switzerland: ISO/IEC.

[6] Synchronized Multimedia Integration Language (SMIL 3.0), W3C Rec. 01 December 2008. [Online]: http://www.w3.org/TR/SMIL3/

[7] RDF Vocabulary Description Language 1.0: RDF Schema. W3C Rec. 10 February 2004. [Online]: http://www.w3.org/TR/rdf-schema/

[8] Jena Semantic Web Framework. [Online]: http://jena.sourceforge.net/

[9] SPARQL Query Language for RDF. W3C Rec. 15 January 2008. [Online]: http://www.w3.org/TR/rdf-sparql-query/

[10] Sitio web de Apple QuickTime para desarrolladores. [Online]: http://developer.apple.com/quicktime

[11] ITU-T Rec. H.264 (03/2005), Advanced vídeo coding for generic audiovisual services, Geneva Switzerland: ITU-T, 2005.

[12] IETF RFC 2327. SDP Session Description Protocol. [Online] Available: http://www.ietf.org/rfc/rfc2327.txt

[13] IETF RFC 3550. A Transport Protocol for Real-Time Applications. [Online] Available: http:// www.ietf.org/rfc/rfc3550.txt

[14] IETF RFC 3984. RTP Payload Format for H.264 Vídeo. [Online]: http://www.rfc-editor.org/rfc/rfc3984.txt

Desarrollo de una Arquitectura de Comunicaciones para Transmisión de Señales Médicas en Entorno Hospitalario

David Alonso Abarca, Tomás Robles, Augusto Morales Domínguez, Ramón Alcarria.
Departamento de Ingeniería Telemática
Universidad Politécnica de Madrid
Ciudad Universitaria s/n 28040 Madrid
david.alonso.abarca@alumnos.upm.es, {trobles, amorales, ralcarria}@dit.upm.es

***Resumen*- Este artículo presenta una arquitectura de comunicaciones propuesta en el proyecto Cardinea para la transmisión de información médica en entornos hospitalarios. La información se obtiene de sensores médicos o de tarjetas RFID para el control de medicamentos, personal o pacientes. El intercambio de la información se realiza mediante el protocolo SIP sobre un entorno de desarrollo OSGi. Los datos médicos son tratados en formato HL7 y controlados mediante el software médico MIRTH.**

***Palabras Clave*-Arquitectura de servicios, SIP, OSGi, RFID, HL7, MIRTH.**

I. INTRODUCCIÓN

Los hospitales y centros sanitarios son entornos que están en constante cambio y tienen un grado importante de impredicción. Esto es debido al cambio constante de pacientes, urgencias y situaciones que se podrían mejorar si se añade un buen sistema de comunicaciones para el registro e interpretación de toda la información generada. Por todo esto forman una parte muy importante en el desarrollo de Internet del Futuro, ya que integra equipos**,** servicios avanzados, todo ello en el contexto de grupos sociales en el marco específico de la salud. CARDINEA [1] como continuación de CARDEA [2] pretende investigar cómo realizar el paradigma de *Internet de las cosas* en el entorno de Servicios hospitalarios creando servicios avanzados y descubriendo patrones de comportamiento en diferentes niveles. Las comunicaciones se llevan a cabo mediante el establecimiento de una red de sensores intrahospitalaria, que envían datos entre sí. El proyecto CARDINEA trata de desarrollar e investigar el conocimiento, gestión y coordinación de los diferentes elementos dinámicos de un hospital, empleando tecnologías semánticas que permiten determinar flujos de personas y elementos como medicamentos, camas...

La necesidad de mejorar la atención en los hospitales, su estructura y protocolos de seguridad hacen más complicado el problema de las comunicaciones. Los hospitales deben tener un mínimo de seguridad para pacientes, así como la información debe estar protegida, asegurando el tránsito de información crítica entre los distintos elementos, lo cual Health Level 7 [3] (HL7) no asegura. La solución sería añadir funciones de disponibilidad, integración y confidencialidad a los datos intercambiados. También se ofrece protección frente a agentes perjudiciales.

Los protocolos y tecnologías a utilizar tienen que cumplir los requisitos del hospital. Por ello los flujos de datos, que en este caso se tratan como sesiones, se tienen que adaptar a los formatos de mensaje HL7 o a software hospitalarios como MIRTH [4]. La adaptación de las comunicaciones en esta propuesta, se centra en añadir funciones de localización, movilidad y control de presencia a las estructuras ya desplegadas. Estas funciones las aporta el Session Initiation Protocol [5] (SIP) que permite la comunicación entre la parte del sistema que obtiene la información y el software necesario para validar o gestionar los datos detectados.

El resto del artículo se estructura de la siguiente manera. La sección II presenta el diseño de la arquitectura de comunicaciones a alto nivel para enfocar de manera generalizada qué elementos se encontrarían en el sistema. A continuación, la sección III detalla las funcionalidades de los diferentes elementos de la arquitectura. La sección IV presenta los tipos de datos que se gestionan en el hospital. En la sección V se detalla la arquitectura de la sección II. Finalmente en la sección VI las conclusiones

II. ARQUITECTURA DE ALTO NIVEL

Algunos problemas que se pueden considerar en entornos hospitalarios son el control de medicamentos expedidos, la gestión de medicamentos peligrosos y el control de sustancias u objetos que pueden ser tanto bolsas de sangre como sustancias nocivas. También se plantea mejorar la atención de los pacientes con un control informatizado de sus constantes y condiciones generando un historial médico electrónico.

La solución que se plantea es establecer una arquitectura de comunicaciones para que diferentes sensores comuniquen los datos obtenidos y poder de esta forma gestionar todas sus sesiones. En cuanto a los sensores se utilizan tanto sensores RFID [6] como sensores para la monitorización de constantes. La arquitectura global del sistema depende de las características del hospital. En la figura 1 se propone una arquitectura genérica con un servidor central para el control global del sistema y un servidor intermedio para controlar cada uno de los dispositivos por planta. En cada dormitorio hay un cabecero iBed que se encarga de tomar las medidas del paciente y una antena RFID para detectar que el paciente está en la habitación correcta.

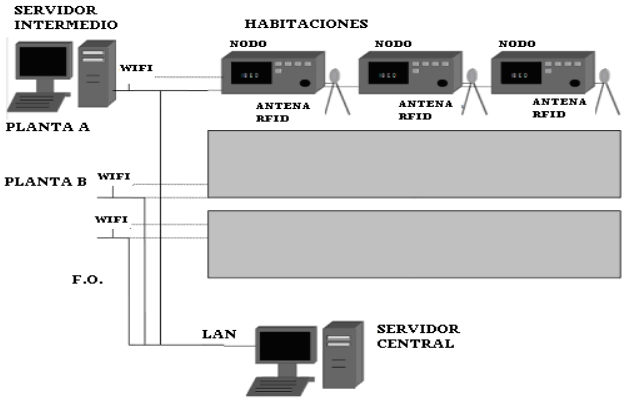


Fig. 1. Arquitectura global

Los cabeceros iBed son sistemas dotados de Windows XP empotrado en los que, a través de un software médico (MIRTH), se generan los mensajes con los datos médicos de las constantes en formato HL7. El cabecero tiene conexiones para poder conectar los distintos sensores biomédicos (espirómetro, glucómetro). A los cabeceros también se conecta una antena RFID la cual interviene en los casos de uso identificando a pacientes, personal o medicamentos. El iBed es el encargado de distribuir la información obtenida y mostrar las alarmas necesarias dependiendo del escenario. El cabecero hace la función de nodo que se comunica con el servidor intermedio mediante SIP. El servidor y todos los nodos están conectados mediante la red Ethernet primaria del hospital, pero se les ha provisto de otra red Wi-Fi como respaldo y protección ante eventos no previstos. La utilización de servidores intermedios es debida a que un hospital puede tener muchas habitaciones por lo que sería necesario dividir la carga de trabajo. Esta característica también aporta la seguridad de que si uno de ellos deja de funcionar el servidor central tomará el control.

Una arquitectura general para un nodo genérico involucrado en el sistema se define en la fig. 2. En este caso se van a incluir todos los bundles (diferentes módulos que se integran sobre OSGi) que intervienen en la arquitectura para tener una visión general y luego definir qué bundles son necesarios en cada nodo. La presencia de bundles depende, por lo tanto, de la función específica del nodo y su funcionalidad dentro del sistema. Toda la arquitectura está sobre una máquina virtual Java ya que el núcleo principal de la arquitectura de comunicaciones es el framework OSGi [7] y así lo requiere. El framework define un modelo de ciclo para los bundles y un registro de servicios para obtener una integración más fácil y mejor descubrimiento entre aplicaciones. Entre múltiples frameworks se ha elegido el framework Knopflerfish [8] porque proporciona la funcionalidad requerida. Entre otras cosas cabe destacar la consola de administración que permite un control remoto de las aplicaciones a desplegar.

La localización de pacientes y medicamentos se consigue mediante la colocación de antenas en las habitaciones para saber si el paciente está en la cama correcta. Estas antenas envían la actividad por medio de la red. El bundle RFID permite manejar e interpretar la información enviada.

El bundle OCP (Open Context Platform) se encarga de capturar, almacenar y proveer información de contexto. Contexto hace referencia a los factores que proporcionan información relevante para los elementos involucrados en el sistema.

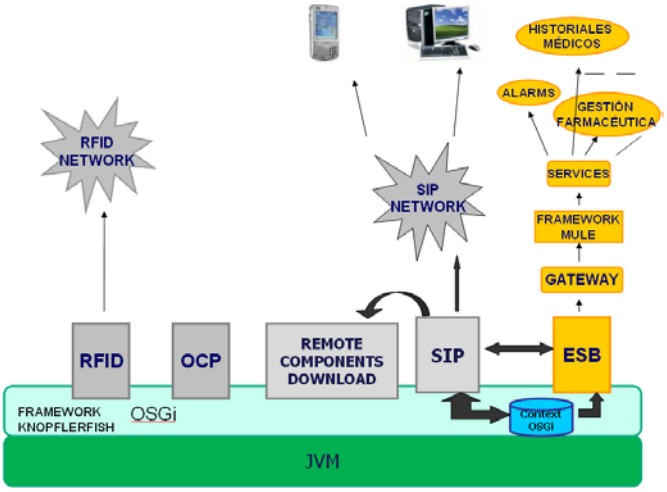


Fig. 2. Arquitectura general de nodo

La arquitectura de Cardinea debe permitir la comunicación con dispositivos y sistemas ajenos a la plataforma. Cardinea proporciona un servicio que permite el establecimiento de sesiones SIP. El bundle SIP permite que las aplicaciones desplegadas envíen mensajes de alarmas hacia los agentes SIP integrados en los diferentes dispositivos, proporcionando así un acceso multidispositivo a la plataforma debido a que SIP proporciona control de presencia y movilidad.

III. Descripción Funcional del Sistema

A. Funcionalidad nodos en los cabeceros iBed

Principalmente los nodos en los cabeceros iBed deben comunicarse con los servidores de su planta para mandarles la información del paciente. Esta información será enviada en formato HL7 por lo que los nodos deben obtener la información de los sensores y convertirla a HL7 para asegurar la interoperabilidad. También identificará al paciente y detectará que el paciente está en su habitación. De esta manera se podrá conocer si los medicamentos que está recibiendo el paciente son los adecuados.

El cabecero también mostrará en pantalla situaciones de alarma de las cuales tiene que ser informado por parte de los servidores. El cabecero diferencia que tipo de datos o mensajes son más importantes y más urgentes para su procesamiento y envío. Uno de los requerimientos de diseño tomados en cuenta es la adición de nuevos servicios y sensores en su plataforma ya sea por requerimientos del paciente o por avances tecnológicos.

Dentro de las funcionalidades está el soporte de movilidad en los nodos para proporcionar mayor flexibilidad.

B. Funcionalidad servidores intermedios

La funcionalidad tanto de los servidores intermedios como del servidor central es prácticamente la misma. Los servidores intermedios se comunican con los servidores centrales y con los nodos de su planta específica. Estos son capaces de recibir y de reenviar los datos en formato médico HL7. Estos datos serán almacenados para tener un mayor control del contexto de cada paciente.

En los servidores se detectan y visualizan las alarmas, y se distribuyen donde fuera necesario para que los avisos sean

útiles y rápidamente interpretables. También diferencia la importancia de cada dato para tomar las medidas oportunas. En los servidores se controla el stock de los medicamentos almacenado en el contexto de planta como el control del personal a exposiciones peligrosas. También se permite la adición de servicios, sensores o funcionalidades dependiendo de las necesidades del entorno hospitalario. Adicionalmente, se controla el estado de los nodos de los cabeceros. Los servidores se encargan también de la distribución de datos como historiales. Esta distribución tiene autenticación para preservar la seguridad.

C. Funcionalidad servidor central

El servidor central a parte de las funcionalidades descritas anteriormente controla la actividad de todos los servidores intermedios y decide si un servidor puede seguir con su labor o seguir él mismo con las rutinas de trabajo del servidor intermedio en cuestión. Esta funcionalidad del servidor central permite tener mayor seguridad en el caso de caída de un servidor.

IV. TIPOS DE DATOS A GESTIONAR

A través de los cabeceros iBED obtenemos datos relativos a las constantes de los pacientes. Para cada paciente hospitalizado, se registran todas las variables en el tiempo, por lo que se puede conocer cuándo se ha realizado la medición y cuándo el profesional la ha validado y por tanto ha sido enviada al HIS para que se integre en la historia Clínica del Paciente. La información recogida se envía utilizando el protocolo de inicio de sesión SIP y protocolos de transporte como Real-time Transport Protocol (RTP).

La información de los pacientes captada por los cabeceros proviene de varios sensores que se acoplan a él en el momento de medición. En la actualidad se utiliza: glucómetro, monitor de constantes, espirómetro y otras medidas que se obtienen mediante la entrada manual de datos. Mediante esta monitorización se generan avisos automáticos cuando determinadas constantes vitales, para pacientes concretos, tengan unos valores que sobrepasen ciertos umbrales. Si se produce una alarma porque las constantes no son aceptables, el ESB generará una alarma que mediante SIP y el sistema de alarmas se envía al profesional correspondiente. También se gestiona la trazabilidad de pacientes y de medicamentos.

A. Clasificación de los datos según calidad de servicio

Según el tipo de dato se necesita una calidad de servicio QoS determinada y ésta exige unas características de retardo de transmisión, jitter, fiabilidad, y ancho de banda mínimo. Los datos en tiempo real forman parte del tráfico no elástico y este tráfico tiene que cumplir: bajo jitter, baja latencia, capacidad de integrar los datos con datos que no sean en tiempo real, capacidad de adaptarse a condiciones de tráfico cambiantes, baja redundancia de bits de cabecera por paquete, baja redundancia de procesamiento por paquete dentro de la red, y una utilización de la capacidad altamente eficiente.

Principalmente se definen tres tipos de datos, por un lado los que no tienen urgencia, los datos que son importantes para el seguimiento de cada paciente y los que exigen un trato urgente. En la tabla 1 se muestra una clasificación de las constantes medidas por los cabeceros iBed según la calidad de servicio que necesitan.

Tipo de dato	QoS			
	Retardo	**Jitter**	**Ancho de banda**	**Fiabilidad**
Tiempo real de prioridad alta (Tráfico no elástico)	Muy bajo	Bajo	Alto	Media
Tiempo real Streaming (Tráfico no elástico)	Bajo	Bajo	Alto	Media
Tiempo no real clase interactiva (Tráfico elástico)	Medio	Alto	Medio	Alta
Tiempo no real best effort (Tráfico elástico)	Alto	Alto	Bajo	Alta

Tabla 1. Clasificación datos según QoS

Una primera clasificación por defecto es:

- Datos en tiempo real de prioridad alta: Datos procedentes de un paciente en estado crítico y alarmas urgentes.
- Datos en tiempo real Streaming: Datos de entrada manual, y alarmas que controlan la exposición del personal a sustancias nocivas.
- Datos en tiempo no real de clase interactiva: Espirómetro, la glucosa en sangre total y datos procedentes del monitor de constantes.
- Datos en tiempo no real best effort: Este grupo engloba transmisión de ficheros o historiales.

B. Modelo de transmisión de los datos

Para hacer una distinción en los datos según tipo en las comunicaciones del sistema se utilizan distintos valores en las cabeceras IP de los mensajes, excepto para el tipo de datos best effort que en este caso el valor corresponden a no hacer distinción y utilizar TCP [11]. En este caso proporciona fiabilidad en la entrega de los datos pero no garantiza un retardo bajo. El modelo es el siguiente:

- Datos en tiempo real de prioridad alta: Mediante *DiffServ* [12], con valor del octeto de tipo de servicio 101110 que permite una tasa mínima de salida.
- Datos en tiempo real Streaming: Mediante DiffServ con valores del octeto de tipo de servicio 111000.
- Datos en tiempo no real de clase interactiva: Mediante DiffServ con valores del octeto de tipo de servicio 001000.
- Datos en tiempo no real best effort: Mediante TCP.

A parte de estas situaciones definidas también se pueden definir nuevas situaciones con valores del DSCP (DiffServ Code Point) libres. Debido a que los pacientes son muy variables y que dependiendo de su situación unos datos pueden ser más importantes que otros, se puede cambiar el valor del servicio para establecer nuevas características.

V. ARQUITECTURA DETALLADA

A. Arquitectura cabeceros ibeds

En los cabeceros de las habitaciones se van ha desarrollar los bundles SIP y RFID únicamente. El bundle SIP es el encargado de comunicarse con los servidores, en los cuales se usa la información obtenida para controlar las alarmas o los datos de contexto. El bundle RFID es el encargado de gestionar los sensores de la habitación. La arquitectura de los nodos de los cabeceros iBeds se muestra en la figura 3.

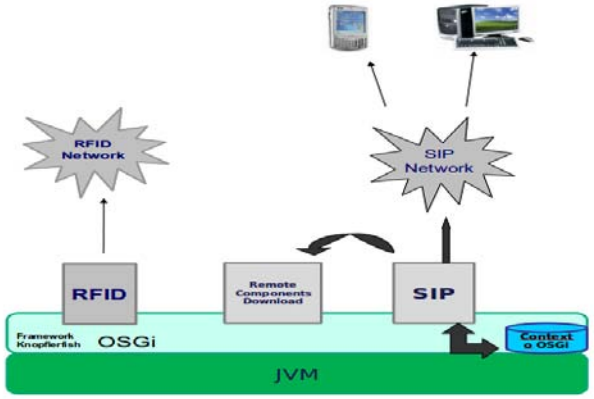


Fig. 3. Arquitectura nodos

B. Arquitectura servidores

Tanto los servidores intermedios como el servidor central están basados en la misma arquitectura, están presentes todos los bundles mencionados en la arquitectura de alto nivel. La arquitectura de ambos servidores es la mostrada en la fig. 2.

C. Arquitectura global integrada

EL bundle SIP es el encargado de la transmisión de los datos entre las diferentes partes. La integración de servicios SIP permite establecer comunicación entre el framework OSGi y elementos externos utilizados para la recepción de mensajes de alarma. El bundle SIP interactúa con un contexto OSGi donde se registran los servicios que están presentes en la arquitectura para saber que se debe hacer en cada momento, si fuera necesario iniciar la descarga de componentes. Este servicio integra tres elementos de la arquitectura SIP. Agente de usuario, servidor proxy y servidor de registro. Este último encargado de recibir las peticiones de registro SIP y su procesamiento, actualizando la información del agente de usuario (dirección, disponibilidad) situado en el servicio de localización. El servicio de localización se implementa como una tabla "Hashtable" donde se almacena la correspondencia entre la dirección URI de los usuarios y su dirección física.

La adaptación de los cabeceros y los terminales que van a captar la información para aprovechar las ventajas que aporta SIP es necesaria. Los cabeceros que toman las medidas funcionan con un software médico que facilita la creación de mensajes HL7. El software que está siendo desarrollado está basado en las librerías de código abierto MIRTH .Estas librerías proporcionan una interfaz para la creación de los mensajes.La combinación de SIP con las librerías de MIRTH es necesaria puesto que en entornos hospitalarios es conveniente utilizar formatos médicos para facilitar la obtención de información y así generar los historiales.

El bundle ESB despliega un bus que interconecta los servicios que dan soporte a las aplicaciones con las que la plataforma interacciona. Se ha establecido un servicio denominado Cardinea Gateway, el cual es el encargado de enviar al bus los datos procedentes de la plataforma hacia otras aplicaciones. Algunos de los servicios prestados mediante este bundle son alarmas, tanto por falta de stock de medicamentos como por mala administración de ellos o por sobrepasar el límite de exposición a sustancias peligrosas.

VI. CONCLUSIONES

En este artículo se ha definido la arquitectura de una plataforma basada en tecnologías OSGi, SIP y RFID, integrándolas con software y tecnologías médicas como MIRTH y HL7 para mejorar las condiciones hospitalarias. El sistema se ha basado en un framework OSGi que facilita el despliegue de los diferentes módulos utilizados y la provisión de nuevos servicios para el ámbito hospitalario. La plataforma diseñada, aunque se ha definido para entornos hospitalarios, puede reutilizarse para otros entornos, ya que, una de las aportaciones de esta arquitectura es que, gracias a la flexibilidad y la modularidad con la cual ha sido diseñada, se pueden extender nuevos servicios. El uso de esta plataforma permite una evolución de los entornos hospitalarios y de cuidados médicos hacia nuevas tecnologías. La plataforma permite que situaciones peligrosas para los pacientes se puedan detectar con mayor rapidez y eficacia, lo cual se podría aprovechar en otros sectores.

AGRADECIMIENTOS

Agradecimientos a todos los grupos colaboradores en proyectos anteriores como Cardea, y a todos los participantes en el proyecto Cardinea. También agradecer la involucración a los hospitales en proyectos de investigación.

REFERENCIAS

[1] Página web del proyecto Cardinea, disponible en http://cardinea.grupogesfor.com/home
[2] Página web del proyecto Cardea, disponible en http://cardea.germinus.com/inicio
[3] Página web de Health Level 7, disponible en http://www.hl7.org/
[4] Página web de la corporación MIRTH, disponible en http://www.mirthcorp.com/community/overview
[5] RFC 3261: "SIP: Session Initiation Protocol", J.Rosenberg, H. Schulzrinne , G. Camarillo, A. Johnston, J.Peterson, R. Sparks, M. Handley y E. Schooler, Junio 2002.
[6] Página web de tecnología RFID, disponible en rfid journal www.rfidjournal.com/
[7] Página web de la OSGi Alliance, disponible en Open Services Gateway initiative http://www.osgi.org
[8] Página web del framework knopflerfish, disponible en http://www.knopflerfish.org/
[9] A SIP-based Device Communication Service for OSGi Framework. , Denis Bushmitch, Wanrong Lin, Andrzej Bieszczad, Alan Kaplan et al. IEEE Consumer Communications and Networking Conference, 2004.
[10] RFC del protocolo de transporte TCP, disponible en http://www.faqs.org/rfcs/rfc793.html
[11] RFCs relacionadas con los servicios diferenciados, disponibles en http://tools.ietf.org/html/rfc2474, http://tools.ietf.org/html/rfc2475

Un Servidor de Aplicación Distribuido para P2P IPTV en IMS

Vanesa Tejada, Ivan Vidal, Jaime Garcia-Reinoso, Francisco Valera.
Departamento de Ingeniería Telemática
Universidad Carlos III de Madrid
Avda. Universidad 30, 28911, Leganés (Madrid).
100033944@alumnos.uc3m.es, ividal@it.uc3m.es, jgr@it.uc3m.es, fvalera@it.uc3m.es

***Resumen*—Las redes de nueva generación (NGN), ofrecerán la posibilidad de desarrollar nuevos y potentes servicios multimedia, que complacerán la actual demanda de los usuarios. Una de las líneas de investigación hoy en día, es la posibilidad de desplegar un servicio P2P IPTV sobre una NGN basada en *IP Multimedia Subsystem* (IMS), de modo que un usuario pueda disfrutar de un *streaming* de video IPTV en una red de banda ancha con calidad de servicio. Cualquier terminal cliente perteneciente al dominio IMS, y subscrito al servicio, podrá solicitar un canal IPTV estableciendo una sesión con el servidor de aplicación IPTV-AS, a través del protocolo de señalización SIP de IMS. Este artículo propone el mecanismo de señalización necesario entre los terminales clientes e IPTV-AS, para poder hacer uso del servicio P2P IPTV en IMS.**

***Palabras Clave*—NGN, IMS, P2P, IPTV, IPTV-AS, SIP.**

I. Introducción

La evolución de las redes de comunicación de los últimos años está marcada por la necesidad de los usuarios de disponer de un servicio en cualquier instante, desde cualquier lugar y a través de cualquier dispositivo.

Desde hace algunos años, los usuarios de Internet han pasado de utilizar servicios que se limitaban a la transferencia de datos, a aplicaciones multimedia que precisan alta disponibilidad, respuesta en tiempo real, y que requieren una determinada calidad de servicio (QoS). Las redes de nueva generación (NGN) proponen que los dominios de comunicación actuales, voz y datos converjan en una única arquitectura de red basada en el protocolo IP, donde los servicios tanto de los operadores de red convencionales como de terceros, compitan en un mismo mercado. La principal ventaja de las NGN y el motivo por el cual se espera un gran impacto en el mercado de las telecomunicaciones, es que están dotadas de una arquitectura capaz de ofrecer al usuario servicios de múltiples tecnologías a través de distintas infraestructuras de transporte de banda ancha con prestaciones de QoS, lo que podría denominarse *Decoupling Access and Services*.

Dada esta separación, la arquitectura NGN necesita un elemento primordial que se encargue del plano de control. *IP Multimedia Subsystem* (IMS) [1] es el subsistema principal de control desarrollado por *3rd Generation Partnership Project* (3GPP), capaz de integrar diferentes infraestructuras de transporte mediante el uso de interfaces, y de desplegar servicios multimedia de banda ancha con QoS como por ejemplo: voz sobre IP (VoIP), video bajo demanda (VoD), *streaming* de video y audio para videoconferencias en tiempo real, e *Internet Protocol Television* (IPTV) entre otros. El protocolo de señalización principal en IMS es *Session Initiation Protocol* (SIP) [2]. Todo terminal cliente que desee utilizar un servicio desplegado en IMS ha de establecer una sesión SIP con el servidor de aplicación (AS) que el usuario haya definido en su perfil de servicio del dominio IMS.

Una de las actuales líneas de investigación, es poder habilitar un servicio IPTV sobre IMS con QoS. Por ejemplo, Nozzilla [3] es una propuesta que define cómo desplegar un servicio IPTV sobre IMS, empleando las redes *Peer-to-Peer* (P2P) para distribuir su contenido. El objetivo de Nozzilla es formar una red de servidores de aplicación IPTV (IPTV-AS), que se encagarán de la señalización que interconecta a los clientes subscritos al servicio a través de IMS. Estos clientes serán capaces de beneficiarse de un servicio IPTV con QoS, y a su vez de proveérselo a otros clientes, de manera que se forme entre ellos una red de distribución de contenidos (CDN) gestionada por los IPTV-AS. Cuando un cliente solicita un canal, la petición llega al IPTV-AS que busca si existe un cliente que esté visualizando ese mismo canal, incluyendo a todos los usuarios conectados en otros IPTV-AS del proveedor de servicio Nozzilla. Si un cliente dispone del canal, será el encargado de retransmitírselo, de manera que el IPTV-AS establecerá una sesión entre ellos. Si no se encuentra ningún cliente, el *streaming* de video será difundido por el *Media Server*(MS) por defecto del IPTV-AS, al que está subscrito el terminal cliente. Este artículo, propone el mecanismo de señalización SIP necesario en IMS, para que un terminal cliente pueda establecer una sesión con el IPTV-AS que le proporciona el *streaming* de video del canal solicitado.

II. Estado del arte: IPTV

IPTV es un servicio de *video-streaming* de TV sobre las redes IP y que normalmente se difunde a los clientes a través de IP *Multicast*, lo que actualmente tiene ciertos inconvenientes. En primer lugar, la configuración que necesitan los routers es muy compleja en cuanto a la retransmisión de los datos. Por otro lado, la gestión de grupos *multicast* se dificulta cuando se mezclan diferentes dominios. Finalmente, *multicast* no funciona bien con el protocolo de transporte TCP y se utiliza UDP, lo que no grantiza la llegada de paquetes y produce retardos en el servicio [4].

3GPP y TISPAN publicaron la especificación de un servicio IPTV para IMS [5], y a partir de él se ha seguido trabajando para optimizar y mejorar el servicio de cara a un producto comercial. Respecto al inconveniente que supone la entrega de datos con IP *Multicast*, se proponen las redes P2P en IMS [6], como una posible solución, transfiriendo las tareas de replicar y difundir la información a los usuarios interconectados vía *unicast*. Las redes P2P [7] son una arquitectura distribuída

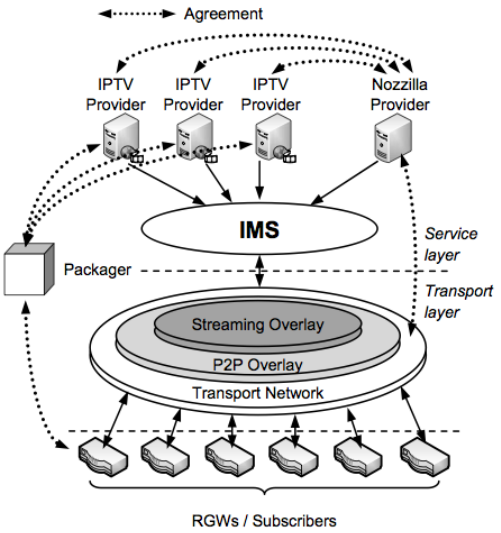


Fig. 1. Arquitectura de Nozzilla en una red NGN basada en IMS

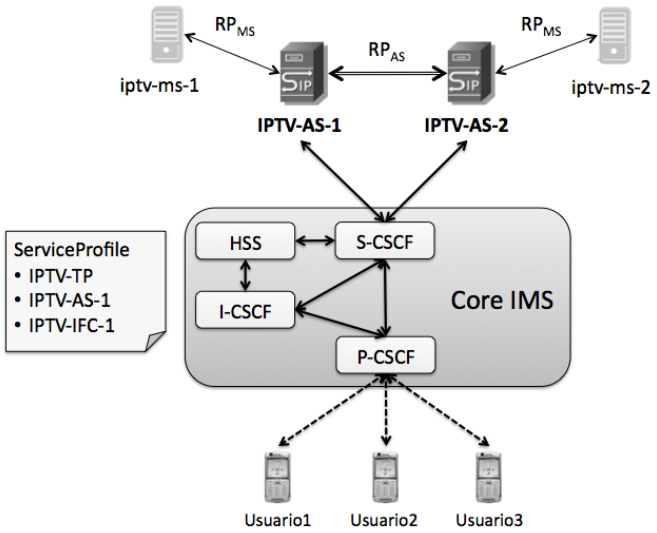


Fig. 2. Arquitectura P2P IPTV propuesta

de nodos *(peers)* interconectados entre sí, y su principal aplicación son las redes de compartición de recursos. Existen dos esquemas de conexión entre los *peers*: descentralizado y centralizado. La primera es una estructura donde no existe ninguna topología en los nodos, y la forma de acceder a los contenidos es solicitándolos a través de mecanismos de inundación de la red, su principal desventaja. El otro diseño es centralizado, con una topología conocida y un acceso a los contenidos a través de las *Distributed Hash Table* (DHT), donde se indica qué nodo tiene qué recurso. Su desventaja es que el retardo para encontrar los contenidos es variable. Aunque el diseño descentralizado es el que ofrece un mejor rendimiento en Internet, Nozzilla define un método de distribución de contenidos llamado *Application Level Multicast* (ALM), donde los datos se propagan siguiendo una arquitectura de árbol, siendo la raíz el MS y los nodos los terminales cliente, que se comportarán tanto como receptores del *streaming* de video como difusores del mismo.

La arquitectura de red que propone Nozzilla está formada por uno o varios proveedores de servicio IPTV denominados IPTV-AS, como puede verse en la Fig. 1. Al igual que en las redes P2P existen las DHT, para facilitar la búsqueda de los contenidos, cada IPTV-AS tiene una tabla compartida donde almacena qué terminal está viendo qué canal, quién es la fuente de los datos y si el cliente tiene recursos suficientes para difundir su mismo canal a otros. Con esta información, los IPTV-AS son capaces de definir un algoritmo de búsqueda de un proveedor de *streaming* con disponibilidad para ofrecer el servicio con QoS.

Todo terminal que desea un canal IPTV ha de establecer una sesión SIP con su IPTV-AS. Después el IPTV-AS busca un proveedor de *streaming* en el siguiente orden: primero entre los usuarios que él tiene en su tabla, luego busca usuarios en las tablas de sus IPTV-AS vecinos, y si no encuentra ninguno, dirige la petición al MS. De esta manera, vemos cómo es el IPTV-AS el núcleo de mantenimiento de sesiones y control del árbol de difusión de contenidos del servicio P2P IPTV.

De acuerdo con el modelo de negocio de las NGN, el proveedor de servicio Nozzilla establecerá un contrato con el proveedor de transporte respecto al tráfico de datos, y los IPTV-AS contratarán los servicios de Nozzilla para poder proveer su servicio.

III. Arquitectura del servicio P2P IPTV

La Fig. 2 representa la arquitectura propuesta para el servicio P2P IPTV, formada por los usuarios del servicio y los servidores de aplicación que lo proveen.

El servicio se compone de un conjunto de servidores de aplicación IPTV que están desplegados sobre un Core IMS. Cada uno de los IPTV-AS tiene definidos dos Puntos de Referencia (RP): uno le asocia a un *Media Server* (MS) y el otro le permite comunicarse con su IPTV-AS vecino. El funcionamiento de un IPTV-AS consiste en procesar la petición de un canal recibida por un cliente, y buscar a un miembro del servicio capaz de difundir el *streaming* de video del canal solicitado. El proveedor del canal puede ser el MS asociado o cualquier terminal usuario que esté viendo el canal solicitado, bien perteneciente al mismo IPTV-AS que está procesando la petición, o bien perteneciente al IPTV-AS vecino. Los terminales usuario pueden asumir dos roles dentro del servicio, uno como Agente de Usuario Cliente (UAC) cuando solicita un canal al IPTV-AS, y otro como Agente de Usuario Servidor (UAS) cuando retransmite un canal a otro cliente (los MS son siempre UAS). Este doble comportamiento es el que permite al servicio formar una red de difusión de contenidos ALM en forma de árbol, donde la raíz es el MS, los nodos son los usuarios, y el mantenimiento es gestionado por el IPTV-AS.

El mecanismo de comunicación entre los componentes de la arquitectura está basado en el protocolo de señalización SIP. Los terminales de usuario han de establecer una sesión SIP con el UAS que le proveerá el canal de *streaming* solicitado. El IPTV-AS es el encargado de mantener la sesión SIP entre UAC y UAS, y su comportamiento está basado en un *Back-to-Back User Agent* (B2BUA) [2] de SIP, que se caracteriza por tener un doble papel dentro de una sesión SIP, es decir, de cara al UAC se comporta como un UAS, y de cara al UAS se comporta como un UAC. De esta manera es capaz

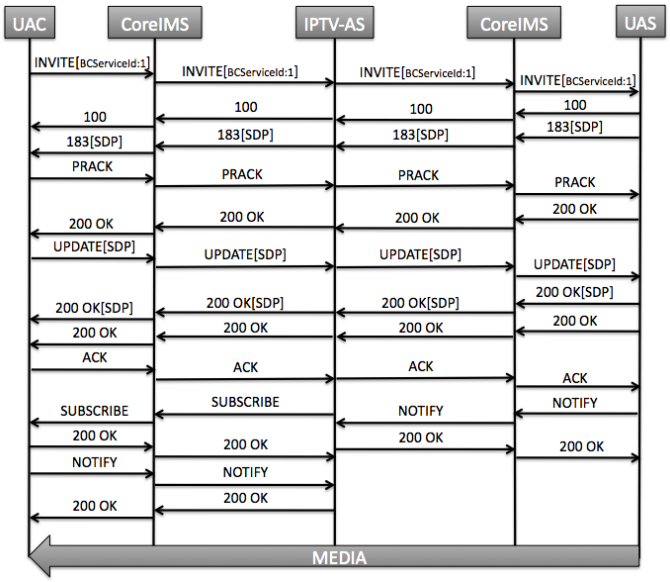


Fig. 3. Señalización SIP para P2P IPTV

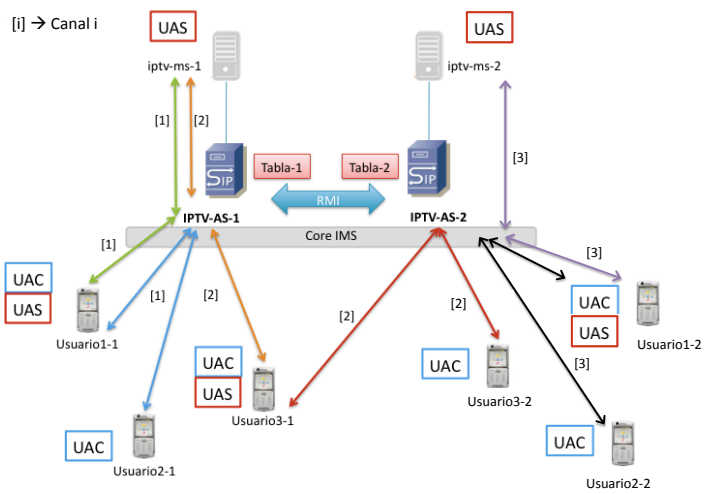


Fig. 4. Escenarios de evaluación

de controlar el estado de la sesión de forma transparente para cada extremo. La Fig. 3 muestra el intercambio de mensajes SIP necesarios para acceder a un canal IPTV. Este intercambio establece una sesión IMS entre el equipo que se conecta al canal (a través de su UAC) y el equipo que sirve el canal (a través de su UAS).

Como se observa en la Figura 3, la primera vez que el cliente solicita un canal, el IPTV-AS se suscribe a la información sobre los recursos disponibles en el cliente, mediante una solicitud SUBSCRIBE de SIP. De este modo, el cliente mantendrá siempre informado al IPTV-AS sobre sus recursos disponibles, utilizando para ello solicitudes NOTIFY de SIP. Finalmente, cuando el IPTV-AS recibe cualquier notificación de un cliente, actualiza la información sobre dicho cliente. Dado que el UAS ya habrá recibido un mensaje SUBSCRIBE desde el IPTV-AS con anterioridad, tras el establecimiento de la nueva sesión, éste notifica al IPTV-AS sus recursos disponibles.

IV. Validación de la propuesta

Para validar la propuesta presentada en el apartado anterior se ha realizado una implementación en Java del IPTV-AS, basada en la especificación JAIN SIP[1]. El IPTV-AS se configura con la dirección pública de un MS por defecto, y gestiona una tabla en memoria donde almacena la información correspondiente a los usuarios del servicio. Además, según se ha comentado anteriormente, la tabla de un IPTV-AS puede ser consultada por un IPTV-AS vecino. Por simplicidad, la comunicación entre IPTV-ASs se ha implementado mediante la tecnología *Remote Method Invocation* (RMI), definiéndose las tablas como objetos remotos. En cualquier caso, otras tecnologías podrían haber sido utilizadas para implementar el acceso a la tabla de los IPTV-AS, por ejemplo basadas en DHTs. Por otro lado, los UE y MS que se presentan en la arquitectura también se han incorporado en la validación, siendo su funcionamiento emulado mediante la herramienta SIPp[2]. La Fig. 4 presenta el escenario que se ha desplegado para la evaluación del servicio P2P IPTV.

Dicho escenario se ha implementado sobre tres máquinas distintas, tipo PC: en la primera máquina se despliega un IPTV-AS (*IPTV-AS-1*), su MS por defecto (*iptv-ms-1*) y tres terminales usuario IMS con un perfil de servicio asociado al *IPTV-AS-1* (*Usuario1-1*, *Usuario2-1* y *Usuario3-1*); en la segunda máquina se ha instalado un Core IMS[3], en el que se ejecutan los CSCFs y un HSS; y en la tercera máquina se despliega un segundo IPTV-AS (*IPTV-AS-2*), su MS por defecto (*iptv-ms-2*) y tres terminales usuario IMS con un perfil de servicio asociado al IPTV-AS-2 (*Usuario1-2*, *Usuario2-2* y *Usuario3-2*).

Sobre el escenario de evaluación mostrado en la Figura 4 se han considerado tres casos de uso:

1. Un usuario solicita un canal IPTV a través de su terminal IMS, y su IPTV-AS correspondiente configura el servicio de modo que el terminal recibe el canal seleccionado a través de su MS por defecto. Este caso de uso es iniciado por los usuarios *Usuario1-1*, *Usuario1-2* y *Usuario3-1*.
2. Un terminal IMS solicita un canal IPTV que ya se está sirviendo a otro terminal cliente. En este caso, su IPTV-AS correspondiente configura el servicio de manera que el terminal que está visualizando el canal pueda retransmitirlo al terminal que ha solicitado el mismo. Este caso de uso es ejecutado por los usuarios *Usuario2-1* y *Usuario2-2*.
3. Un terminal IMS solicita un canal IPTV que ya se está sirviendo a otro terminal cliente perteneciente a un IPTV-AS diferente. En este caso, el IPTV-AS correspondiente al terminal solicitante localiza un terminal cliente en el otro IPTV-AS y le redirige a él la petición. Este caso de uso es iniciado por el usuario *Usuario3-2*.

Para cada uno de estos tres casos de uso, se han capturado los mensajes de señalización SIP mediante la herramienta WireShark[4], verificándose que los procedimientos de control

[1] https://jain-sip.dev.java.net/

[2] http://sipp.sourceforge.net/

[3] Open IMS Core: http://www.openimscore.org/

[4] http://www.wireshark.org

ejecutados entre las distintas partes involucradas en cada caso (clientes, Core IMS e IPTV-ASs) se ajustan a los indicados en la sección III. Por otro lado, mediante el soporte de la herramienta SIPp, es posible calcular el retardo de establecimiento de las sesiones IMS correspondientes a cada caso de uso. Dicho retardo se define como el tiempo transcurrido entre que un cliente iniciador envía la solicitud INVITE hasta que recibe la respuesta OK correspondiente. Con esta definición, se ha realizado un experimento consistente en ejecutar treinta veces cada caso de uso, y se ha calculado el valor medio del retardo de establecimiento de sesión para cada cliente iniciador. Los valores resultantes de este experimento se indican en la Tabla I.

Caso de uso	Sesión multimedia	Retardo medio (ms)
1	usuario1-1 & iptv-ms-1	2265
	usuario1-2 & iptv-ms-2	2183
	usuario3-1 & iptv-ms-1	1153
2	usuario2-1 & usuario1-1	1009
	usuario2-2 & usuario1-2	1057
3	usuario3-2 & usuario3-1	1161

Tabla. I
RETARDO MEDIO DE ESTABLECIMIENTO DE SESIÓN

En el caso de uso 1, los retardos medios correspondientes a las dos primeras sesiones (usuario1-1 & iptv-ms-1 y usuario1-2 & iptv-ms-2) son sensiblemente superiores al resto de retardos. Esto es debido a que ambos retardos se corresponden con el primer establecimiento de sesión involucrando a un IPTV-AS, lo cual implica la activación del servicio y la inicialización de la pila SIP, así como generar y compartir la tabla del servidor de aplicación como objeto remoto RMI. El resto de valores de la tabla I se encuentran en el mismo orden de magnitud.

V. CONCLUSIONES

Este documento presenta cómo un servidor de aplicación es capaz de configurar un servicio P2P IPTV sobre una red IMS basándose en el protocolo de señalización SIP. El objetivo del IPTV-AS consiste en procesar las peticiones de canal IPTV de los terminales cliente IMS, y buscar una fuente de datos que le provea el canal solicitado. La fuente de datos puede ser, bien un cliente perteneciente a cualquier IPTV-AS que esté visualizando el canal, o bien un MS. La finalidad principal consiste en que los clientes sean capaces de establecer una sesión SIP entre ellos, y retransmitirse uno a otro el canal formando una arquitectura en árbol de distribución de contenidos. De esta manera un canal IPTV no se retransmite únicamente a través de un servidor de *streaming*, aumentando así la disponibilidad de los recursos del servicio P2P IPTV. Se ha conseguido desplegar un conjunto de componentes que formen un escenario de evaluación, donde se contemplan todos los casos posibles de establecimiento de sesión SIP que el IPTV-AS debe manejar. El servidor de aplicación es capaz de configurar el servicio entre un terminal cliente IMS y un MS, entre dos terminales cliente pertenecientes al mismo IPTV-AS, y entre dos terminales cliente que pertenecen a distintos IPTV-AS.

Como líneas de trabajo futuras, se podría especificar como parte del diseño, los procedimientos de señalización necesarios para desconectar el terminal de usuario del servicio y para realizar un cambio de canal. Por otro lado sería interesante diseñar, como parte de la evaluación, un experimento que permita obtener de forma precisa los valores medios para los retardos de establecimiento de sesión. Estos valores deberían incluir, además, los retardos de transmisión en la red de acceso y los retardos de procesamiento en el Core IMS.

AGRADECIMIENTOS

Este artículo está financiado parcialmente por el MEC a través del proyecto CONPARTE (TEC2007-67966-C03-03/TCM). Los autores desean agradecer a Nethalis Solutions S. L. por su colaboración en el trabajo desarrollado en este artículo.

REFERENCIAS

[1] 3GPP, IP Multimedia Subsystem (IMS), Stage 2, TS 23.228URL http://www.3gpp.org/ftp/Specs/html-info/23228.htm.
[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, SIP: Session Initiation Protocol, Tech. rep., RFC 3261, Internet Engineering Task Force (IETF) (2002).
[3] A. Bikfalvi, J. García-Reinoso, I. Vidal, F. Valera, Nozzilla: a peer-to-peer IPTV distribution service for an IMS-based NGN, in: Fifth International Conference on Networking and Services (ICNS), 2009.
[4] A. Bikfalvi, J. García-Reinoso, I. Vidal, F. Valera, A peer-to-peer IPTV service architecture for the IP multimedia subsystem, International Journal of Communication Systems.
[5] ETSI-TISPAN, IPTV architecture; IPTV function supported by the IMS subsystem, Technical Report.
[6] J. Fiedler, F. FOKUS, P2P and IMS Cooperation/Integration, Group for Next Generation Network Infrastructures, 2008, uRL http://www.ict-fireworks.eu/fileadmin/events/FIREweek/2nd-WS-Converged-Networks/04-Jens_Fiedler.pdf.
[7] E. Lua, J. Crowcroft, M. Pias, R. Sharma, S. Lim, A survey and comparison of peer-to-peer overlay network schemes, IEEE Communications Surveys & Tutorials 7 (2) (2005) 72–93.
[8] A. Roach, Session Initiation Protocol (SIP)-Specific Event Notification, Tech. rep., RFC 3265, Internet Engineering Task Force (IETF) (2002).

Hacia el *single sign-on* en la integración de herramientas externas en Entornos de Aprendizaje Virtual

Carlos Alario Hoyos, Eduardo Gómez Sánchez, Miguel L. Bote Lorenzo,
Juan I. Asensio Pérez, Adolfo Ruiz Calleja, Guillermo Vega Gorgojo
Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad de Valladolid,
Paseo de Belén 15, 47011, Valladolid, España.
{calahoy@gsic, edugom@tel, migbot@tel, juaase@tel, adolfo@gsic, guiveg@tel}.uva.es

***Resumen*—Uno de los aspectos más importantes que deben considerar las propuestas de integración de herramientas externas en Entornos de Aprendizaje Virtual (VLE), son los requisitos de seguridad que impone cada VLE y cada herramienta a la hora de permitir el acceso a su funcionalidad. El objetivo debe ser que los educadores y estudiantes puedan acceder de forma transparente a las distintas aplicaciones. Para ello, puede hacerse uso de los mecanismos de autenticación única o *single sign-on* (SSO). No obstante, las propuestas que tratan el SSO en la integración de herramientas lo hacen de forma muy específica o imponiendo una gran cantidad de requisitos. Por ello, este artículo presenta una solución que da soporte al SSO en la integración de múltiples herramientas externas en distintos VLE, basándose en los criterios de generalidad, y en la no imposición de requisitos a los proveedores de VLE y herramientas.**

I. Introducción

El uso de entornos de aprendizaje virtual (VLE - *Virtual Learning Environments*) para apoyar la realización de situaciones de aprendizaje es una tendencia en aumento a lo largo de los últimos años, gracias en parte al éxito de sistemas como Moodle[1], LAMS[2], .LRN[3] o Sakai[4]. Estos VLE suelen incluir algunas herramientas en sus distribuciones, tales como cuestionarios, *chats* o foros. Sin embargo, se ha detectado una limitación con respecto al número y tipo de herramientas que presentan, la cual dificulta el diseño y la realización de las situaciones de aprendizaje [1]. Por ello, numerosos autores se han inclinado por la integración de herramientas externas [2], [3], [4], [5]. A esto contribuye además la creciente cantidad de herramientas web para usos educativos [6]; por ejemplo, Google Apps[5], Twitter[6], o Delicious[7].

Uno de los principales problemas que se plantean en las propuestas de integración es la gestión de la seguridad. El motivo es que cada proveedor de VLE y herramienta puede definir diferentes mecanismos para permitir el acceso a los recursos. Uno de los más empleados consiste en solicitar las credenciales (normalmente en forma de usuario y contraseña) a los educadores y estudiantes, para que éstas sean validadas en los dominios del proveedor. En ocasiones, pueden utilizarse unas credenciales comunes para autenticarse en distintos VLE o herramientas, como las que se definen bajo el estándar de autenticación OpenID[8]. Otras veces, las credenciales de varios sistemas se validan contra una misma base de datos. En este sentido, es una política frecuente que distintos VLE dentro de una misma organización utilicen un servidor externo centralizado, accesible por ejemplo, mediante LDAP (Protocolo Ligero de Acceso a Directorios - *Lightweight Directory Access Protocol*) [7]. En cualquiera de estas situaciones se persiguen dos objetivos complementarios: facilitar el acceso y la autenticación de los usuarios en las diferentes herramientas integradas en los VLE, y minimizar la carga administrativa que supone la gestión adicional de la seguridad asociada a dicha integración. Ambos objetivos pueden cubrirse mediante una política de autenticación única (SSO - *single sign-on*) [8], la cual se incluye en bastantes de las propuestas de integración [9], [10], [14]. El problema es que estas soluciones son específicas para ciertas combinaciones VLE-herramienta, no pudiendo ser extendidas como una solución más general.

El objetivo de este artículo es realizar una propuesta que permita el SSO en la integración de múltiples herramientas externas en distintos VLE. Para ello, se parte de un escenario educativo en la sección II del cual se extraen los requisitos de diseño. A continuación, la sección III explora los mecanismos de autenticación que soportan los principales VLE y herramientas. En la sección IV se analizan las limitaciones de las propuestas de integración que consideran el SSO, para posteriormente proponer en la sección V una solución general. Finalmente, la sección VI recoge las conclusiones y líneas futuras.

II. Ejemplo de escenario educativo

Esta sección pretende ilustrar los problemas de seguridad asociados a la integración de herramientas externas en VLE. Para ello, se parte de una situación de aprendizaje inicial de la que se extrae un conjunto de requisitos de diseño para la propuesta de solución.

II-A. Situación de aprendizaje

Los profesores de uno de los últimos cursos de secundaria quieren que sus alumnos conozcan más detalles de la geografía española y a la vez fomenten sus capacidades de abstracción y discusión. Para ello, plantean una situación de aprendizaje utilizando las instalaciones de Moodle y MediaWiki[9] que posee su instituto. La clase se divide en varios grupos dependiendo de las ciudades a estudiar. Los usuarios de cada uno de los grupos deben consultar en primer lugar, información sobre su ciudad en Wikipedia[10]. Después deben

[1] http://moodle.org
[2] http://lamsinternational.com
[3] http://dotlrn.org
[4] http://sakaiproject.org
[5] http://google.com/apps
[6] http://twitter.com
[7] http://delicious.com
[8] http://openid.net
[9] http://mediawiki.org
[10] http://wikipedia.org

elaborar un texto con los puntos más importantes en una página de MediaWiki. Finalmente, han de hacer una breve presentación con Google Presentations[11].

II-B. Problemas de seguridad en la integración

El análisis de la seguridad parte de que los educadores y los estudiantes disponen de credenciales propias para acceder a su cuenta en Moodle. Una vez autenticados, es deseable que existan mecanismos de SSO que les permitan acceder a las herramientas mencionadas de forma transparente. En este sentido, Wikipedia no impone ningún requisito de seguridad para el acceso a la información que ofrece. Sin embargo, MediaWiki y Google Presentations requieren que los usuarios estén autorizados para acceder o modificar sus recursos. Esto genera la necesidad de disponer de credenciales adicionales, bien sean propias (una por educador/estudiante) o institucionales (compartidas por toda una clase/instituto/departamento). Disponer de credenciales propias para cada herramienta supone una sobrecarga de gestión, normalmente asumida por los propios usuarios. Disponer de credenciales institucionales puede ser una limitación importante a la hora de definir, desarrollar y evaluar actividades que incluyan grupos, ya que se dificulta la separación en el acceso a diferentes recursos dentro de una misma herramienta para cada grupo.

Las herramientas que componen esta situación de aprendizaje no aparecen actualmente en las distribuciones de los principales VLE, por lo que deben ser integradas. En esta línea, muchas de las propuestas que atacan el problema de integración lo hacen de forma específica para un VLE y una herramienta determinados [1], como por ejemplo los módulos desarrollados para Moodle [10]. El problema de este tipo de módulos es que suponen un gran esfuerzo de desarrollo para integrar múltiples herramientas en distintos VLE. Por ello, otras propuestas de integración se decantan por una arquitectura más modular en la que ciertos elementos pueden ser desarrollados y mantenidos por terceros [5]. Sin embargo, esto genera un problema de confianza [11], ya que para conseguir el SSO hay que atravesar dichos elementos.

II-C. Requisitos de diseño

A partir de la situación de aprendizaje inicial y de los problemas de seguridad detectados se establecen los siguientes requisitos de diseño.

1. **El VLE es el punto de entrada**. Los educadores y los estudiantes disponen de credenciales válidas en el VLE que les autorizan a desarrollar las situaciones de aprendizaje.
2. **Debe facilitarse el SSO a los educadores y a los estudiantes**. Las autenticaciones que se lleven a cabo para poder utilizar las herramientas han de ser transparentes, en la medida de lo posible.
3. **La solución propuesta ha de ser lo más general posible**. Se valora que se pueda conseguir el SSO en la integración de múltiples herramientas en distintos VLE, pudiendo haber sido éstas desarrolladas por distintos proveedores y con diferentes tecnologías.
4. **La solución propuesta no debe añadir requisitos a los proveedores de VLE y herramientas**. El motivo es que, en la mayoría de los casos, éstos no estarán dispuestos a modificar sus sistemas.
5. **Debe minimizarse la carga relacionada con la gestión de credenciales**. Es conveniente facilitar el trabajo de gestión de credenciales a los administradores de los distintos VLE.

[11] http://docs.google.com

III. Mecanismos básicos de seguridad

Los VLE y herramientas incluyen sus propios mecanismos para gestionar la seguridad. Esta sección analiza y discute su adecuación como parte de la propuesta de solución.

III-A. Análisis de los VLE

Los educadores y estudiantes que disponen de una cuenta válida en un VLE se autentican introduciendo sus credenciales en el sistema. Éstas pueden ser validadas contra la base de datos interna del VLE, o contra una base de datos o servidor externo. Por ejemplo, Moodle soporta, entre otros, servidores CAS (Servicio de Autenticación Centralizado - *Central Authentication Service*) o IMAP (Protocolo de Acceso a Mensajes de Internet - *Internet Message Access Protocol*). Sin embargo, LDAP es el único servidor externo soportado actualmente por las distribuciones de los principales VLE. De forma adicional, hay que mencionar que existen extensiones de Moodle, LAMS y Sakai para soportar Shibboleth[12], un mecanismo de autenticación SSO que puede utilizarse dentro de una misma federación u organización de confianza.

III-B. Análisis de las herramientas

Cada herramienta presenta sus propios mecanismos de seguridad, variando desde las que ofrecen libre acceso a su funcionalidad a aquéllas que requieren autenticación de usuarios. En este sentido, uno de los mecanismos de SSO más utilizado es OpenID, ya que permite autenticarse en una gran lista de sitios y herramientas web [12] con unas credenciales únicas proporcionadas por alguno de sus proveedores, entre ellos Google o Yahoo! De esta forma, los usuarios de Zoho[13] o Flickr[14] pueden autenticarse con las credenciales de cualquiera de estos dos proveedores. Algunas herramientas permiten también utilizar servidores o bases de datos externas. Por ejemplo, se han desarrollado extensiones para Wordpress o MediaWiki con el objetivo de soportar autenticación contra servidores CAS, IMAP y LDAP. Además, existen mecanismos de autorización delegada [9], que permiten el acceso a determinados recursos para un cierto usuario y generalmente durante un periodo de tiempo predeterminado. OAuth [13] es el protocolo estandarizado más extendido para proporcionar este tipo de autorización. Se basa en el intercambio de *tokens* o permisos entre el usuario final, el servicio que proporciona el acceso a la aplicación, y un tercero que es el que solicita y gestiona los permisos. Algunas herramientas como Google Apps, Yahoo! o Delicious implementan una interfaz OAuth. Además, existen otros mecanismos propietarios de autorización delegada, como AuthSub[15] de Google, BBAuth[16] de Yahoo! o la interfaz de autorización propia de Flickr[17].

[12] http://shibboleth.internet2.edu/
[13] http://zoho.com
[14] http://flickr.com
[15] http://code.google.com/intl/es-ES/apis/accounts/docs/AuthSub.html
[16] http://developer.yahoo.com/auth/
[17] http://www.flickr.com/services/api

III-C. Clasificación y discusión

Los mecanismos que permiten la **autenticación a través de un elemento o proveedor externo** pueden facilitar el SSO entre un VLE y una herramienta siempre y cuando ambos compartan el elemento que valida la autenticación (la base de datos, el servidor externo, OpenID). Aquí pueden surgir problemas de confianza dependientes de la arquitectura de integración, ya que utilizar elementos de terceros puede producir una suplantación de identidad de un usuario registrado en un VLE en las herramientas. Además, hay que considerar la confianza que se deposita en el elemento externo encargado de la validación. Esto se ejemplifica claramente en las herramientas que soportan OpenID, ya que la decisión de aceptar credenciales de uno u otro proveedor depende del nivel de confianza que ofrezca éste, siendo Google o Yahoo! los más aceptados.

Los mecanismos de **autorización delegada** también pueden facilitar el acceso transparente a un recurso en una herramienta integrada en un VLE durante un tiempo determinado. Para ello, este último debe conocer a quién solicitar los permisos correspondientes. En este caso, los problemas de confianza son menores, ya que los permisos se orientan a recursos concretos, en lugar de ofrecer libre acceso a una herramienta.

Los mecanismos que permiten el acceso a diferentes sistemas dentro de un mismo dominio se basan en la **federación de confianza**. Para ello, delegan la gestión y la autenticación de usuarios a una autoridad que pertenece al dominio y en quien se puede confiar. En este caso no los elementos que realizan la integración corren en máquinas del mismo dominio en el que se encuentran los VLE y las herramientas. El principal problema de estos mecanismos es que muchas de las herramientas de terceros que pueden ser integradas están disponibles en la web, y no pueden formar parte de una federación de confianza.

IV. Propuestas existentes para el SSO entre VLE y herramientas

Muchas propuestas de integración atacan el problema para una combinación VLE-herramienta. Por ejemplo, los módulos que permiten integrar Drupal[18] y Wordpress en Moodle requieren que el VLE y la herramienta compartan un mismo dominio y una misma base de datos [10]. En esta línea, Moodlerooms[19] ha desarrollado un módulo específico para integrar Google Apps en Moodle incluyendo SSO dentro de una federación de confianza. Su principal limitación es que requiere disponer de una cuenta de dominio de Google Apps, algo que no es asumible para la mayor parte de instituciones educativas. Otro caso concreto es la autenticación compartida de LAMS en su integración en Moodle o Sakai [14]. A pesar de ello, la especificidad del protocolo de intercambio de información definido, unido a la ausencia de estándares con una mayor aceptación hacen que sea difícil generalizar esta propuesta. Más genérica es la solución Crowd de Atlassian[20], pensada para automatizar la autenticación en ciertas herramientas web. Lamentablemente, a excepción de Google Apps, las aplicaciones que soportan Crowd han sido desarrolladas por la propia empresa que comercializa esta solución. Finalmente, merece la pena destacar *Reverse OAuth* [9], una modificación del mecanismo de autorización delegada OAuth, pensada para el contexto de integración de herramientas externas en VLE. Sin embargo, esta solución presenta varios problemas: el primero es que no considera aquellas situaciones de aprendizaje en las que se requiera el uso de grupos, ya que asume que se dispone de una única credencial institucional en la herramienta; además propone modificar un protocolo que se encuentra en proceso de estandarización, por lo que sus expectativas de implementación en los distintos proveedores es, a priori, muy limitado.

[18] http://drupal.org
[19] http://moodlerooms.com
[20] http://atlassian.com/software/crowd

V. Propuesta de single sign-on en la integración de múltiples herramientas externas en distintos VLE

Las limitaciones de las soluciones presentadas hacen que no puedan ser utilizadas, de forma general, en escenarios como el de la sección II. Por ello, esta sección realiza una propuesta de solución a partir de los requisitos de diseño iniciales.

V-A. Consideraciones previas

Las siguientes consideraciones han llevado a descartar otros trabajos relacionados.

- No puede suponerse que se dispone de una federación de confianza, ya que no es lo habitual en las instituciones educativas, especialmente si son de pequeño tamaño.
- Cada usuario debe tener unas credenciales propias en las herramientas que forman parte de las situaciones de aprendizaje.
- La solución propuesta debe ser válida independientemente de la arquitectura que dé soporte a la integración.
- Existen herramientas que a pesar de requerir autenticación para acceder a su funcionalidad no soportan ningún mecanismo de SSO ni ofrecen una API programática de autenticación.

V-B. Propuesta de solución

La propuesta consiste en combinar varios mecanismos de autenticación a través de un elemento externo, para facilitar el SSO con el mayor número de VLE y herramientas. Para ello, se utiliza un servidor LDAP que gestiona el almacenamiento, la publicación, y la utilización de credenciales. Esta decisión está condicionada por el hecho de que LDAP es el único protocolo soportado actualmente por los principales VLE.

- *Almacenamiento*. La base de datos asociada al servidor LDAP almacena un conjunto de credenciales válidas en distintos VLE y herramientas para cada uno de los estudiantes y educadores, asociando las cuentan de usuario en los VLE a las sus credenciales en las herramientas. Esta asociación incluye credenciales genéricas como las de OpenID, y específicas, para diferentes proveedores externos.
- *Publicación*. La información en el servidor LDAP debe almacenarla cada usuario de forma distribuida a fin de evitar el aumento de la carga del administrador. La interfaz de publicación de credenciales debe ser externa al VLE, de tal forma que no se introduzcan requisitos adicionales sobre estos proveedores.

- *Utilización*. Los elementos que componen la arquitectura de integración acceden al servidor LDAP para recuperar las credenciales correspondientes y utilizarlas para realizar el SSO. Únicamente se requiere indicar la referencia a la cuenta de usuario y a la herramienta concreta o al tipo de credencial.

El problema relacionado con el posible uso de elementos de terceros se resuelve incluyendo una lista de sitios de confianza en los módulos que extienden la funcionalidad de los VLE. Además, para probar su identidad y evitar cualquier tipo de suplantación, cada uno de estos sitios debe disponer de un certificado emitido por una autoridad certificadora externa, como por ejemplo CAcert.org[21] que ha de incluir en sus comunicaciones con otros elementos. La Figura 1 recoge la visión general de la propuesta.

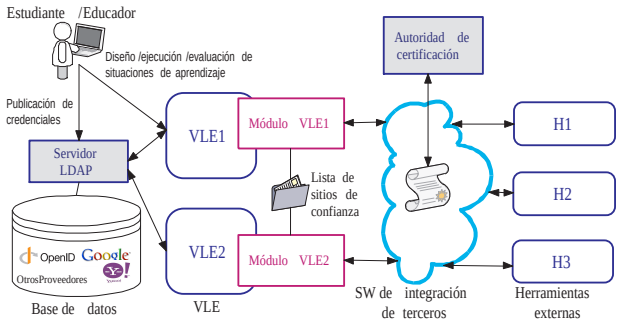


Figura 1: Propuesta de *single sign-on* en la integración de múltiples herramientas externas en distintos VLE

V-C. *Análisis de la propuesta*

El hecho de que los **VLE sean el punto de entrada** del SSO condiciona la decisión de sincronizar la información sobre las cuentas de usuarios en un servidor LDAP accesible desde los VLE, y relacionarlas con las credenciales en las diferentes herramientas. Esta relación es la que permite dar **soporte al SSO de educadores y estudiantes** a lo largo de las situaciones de aprendizaje. Para ello, se solicitan al servidor externo las credenciales de cada usuario en la medida en que sean requeridas por las herramientas. Es importante destacar que la solución es bastante **general**, ya que puede dar soporte al SSO en un gran número de herramientas. Para ello, se utilizan como base las credenciales de los usuarios en OpenID, Google o Yahoo!, pudiendo añadirse las de otras herramientas específicas. En este punto hay que comentar que el sistema debe estar preparado para seguir funcionando aun en los casos en los que los usuarios no hayan publicado aún sus credenciales; simplemente no podrá facilitarse el SSO. La solución propuesta **no impone requisitos a los proveedores de herramientas o de VLE**. Únicamente se debe añadir una lista de sitios de confianza y la capacidad de preguntar por los certificados como parte de la lógica de los módulos que extienden la funcionalidad de los VLE. Finalmente, el **administrador del sistema reduce su carga** ya que confía la gestión de credenciales a un elemento externo. Si bien es cierto que la propuesta requiere configurar y sincronizar el servidor LDAP, esta tarea se realiza una única vez, por lo que no supone un esfuerzo de administración considerable.

[21] http://cacert.org

VI. Conclusiones y líneas futuras

Este artículo presenta una propuesta que da soporte al SSO en la integración de múltiples herramientas externas en distintos VLE, utilizando un servidor externo y relacionando las credenciales de los educadores y estudiantes en distintas herramientas, con las cuentas en los VLE. Además, la propuesta cubre los problemas de suplantación que pueden surgir al utilizar *software* mantenido por terceros. Esta solución cumple con los requisitos de diseño iniciales y además, se diferencia de otras propuestas existentes en su generalidad, y en la no imposición de requisitos a los proveedores de herramientas y VLE. Su principal limitación es que impone que los estudiantes y educadores dispongan de credenciales propias en las herramientas que van a utilizar. Las líneas futuras pasan por la aplicación de esta solución a algunas propuestas de integración de herramientas ya desarrolladas [1], y su validación en situaciones de aprendizaje que incluyan múltiples herramientas que requieran seguridad.

Agradecimientos. Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación (TIN2008-03023) y por la Junta de Castilla y León (VA106A08).

Referencias

[1] C. Alario-Hoyos, J.I. Asensio-Pérez, M. Bote-Lorenzo, E. Gómez Sánchez, G. Vega-Gorgojo, y A. Ruiz-Calleja. Integration of external tools in Virtual Learning Environments: main design issues and alternatives. En *Actas de la Décima Conferencia Internacional en Advanced Learning Technologies, ICALT 2010 (aceptado para publicación)*, Sousse, Túnez, julio 2010. IEEE Computer Society.

[2] M. L. Bote-Lorenzo, E. Gómez-Sánchez, G. Vega-Gorgojo, Y. A. Dimitriadis, J. I. Asensio-Pérez, y I. M. Jorrín-Abellán. Gridcole: A tailorable grid service based system that supports scripted collaborative learning. *Computers and Education*, 51(1):155–172, 2008.

[3] C. Severance, J. Hardin, y A. Whyte. The coming functionality mash-up Personal Learning Environments. *Interactive Learning Environments*, 16(1):47–62, 2008.

[4] S. Wilson, P. Sharples, D. Griffiths, y K. Popat. Moodle Wave: Reinventing the VLE using Widget technologies. En *Actas del Segundo Workshop Internacional en Mashup Personal Learning Environments, (MUPPLE09)*, pp. 47–58. Niza, Francia, septiembre 2009.

[5] L. Fuente-Valentin, Y. Miao, A. Pardo, y C. Delgado-Kloos. A Supporting Architecture for Generic Service Integration in IMS Learning Design. En *Actas de la Tercera Conferencia Europea en Technology Enhanced Learning, (ECTEL08)*, pp. 467–473, Maastricht, Holanda, septiembre 2008. Springer-Verlag.

[6] Top 100 Tools for Learning 2009. URL: http://www.c4lpt.co.uk/recommended/. Última visita: marzo 2010.

[7] Lightweight Directory Access Protocol (LDAP): The Protocol. URL: Última visita: marzo 2010.

[8] A. Pashalidis y C.J. Mitchell. A Taxonomy of Single Sign-On Systems. En *Information Security and Privacy, Octava Conferencia de Australasia, ACISP 2003*, pp. 249–264, Wollongong, Australia, julio, 2003. Springer-Verlag.

[9] J. Fontenla, M. Caeiro, M. Llamas, y L. Anido. Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems. *Computers & Security*, en prensa, *corrected proof*, 2009.

[10] Moodle. Modules and Plugins. URL: http://moodle.org/mod/data/view.php?id6009. Última visita: marzo 2010.

[11] L. Kagal, T. Finin, y A. Joshi. Trust-Based Security in Pervasive Computing Environments. *Computer*, 34:154–157, 2001.

[12] OpenIDDirectory. URL: http://openiddirectory.com/. Última visita: marzo 2010.

[13] OAuth Core 1.0. URL: http://oauth.net/core/1.0a/. Última visita: marzo 2010.

[14] LAMS and 3rd Party App Integration Mechanism. URL: http://wiki.lamsfoundation.org/display/lams/LAMS+and+3rd+Party-+App+Integration+Mechanism. Última visita: marzo 2010.

SFDL: definición de vistas dinámicas optimizada para flujos de trabajo

Emilio García, Diego Moreno, Sandra Aguirre, Juan Quemada
Departamento de Ingeniería de Sistemas Telemáticos (DIT)
Universidad Politécnica de Madrid
ETSI de Telecomunicación. Av. Complutense, s/n. 28040 – Madrid
{egarcia, dmoreno, saguirre, jquemada}@dit.upm.es

***Resumen*- La gestión de procesos basada en sistemas de workflow es una tendencia creciente en los entornos colaborativos. Así, cualquier optimización en las tecnologías que facilitan dicha labor, como los flujos de trabajo (workflows), multiplica los beneficios aportados a la colaboración entre individuos. Con el objetivo de mejorar las técnicas de workflow se ha diseñado un nuevo lenguaje de definición de vistas dinámicas denominado SFDL, orientado a la adaptabilidad en distintos entornos, con representaciones en diferentes formatos y pensado para su fácil integración en distintas arquitecturas. Para la validación del diseño expuesto se ha llevado a cabo su implementación en un escenario real, recibiendo realimentación y refinando las especificaciones. El trabajo se ha basado en el uso de estándares ampliamente usados en el ámbito web (XML, YAML, JSON, Atom y REST). Además, en el presente artículo se dan directrices que facilitan la adopción de la solución.**

***Palabras Clave*- Flujo de trabajo (*workflow*), SFDL, trabajo colaborativo, interfaz de usuario (*user interface*)**

I. INTRODUCCIÓN

Los flujos de trabajo (*workflow*) como herramienta para la gestión de grupos de trabajo en un entorno colaborativo ha tomado una papel creciente en el éxito de las empresas, habitualmente involucrando equipos de trabajo a través de distintas organizaciones. La investigación desarrollada en este artículo se ha centrado en la mejora de los sistemas de workflow basados en una interacción web con los usuarios. Se ha diseñado un lenguaje de definición de vistas de usuario de generación dinámica pensado para integrarse fácilmente dentro de un motor de ejecución de workflow. Dicho lenguaje de definición, denominado *Simple Form Definition Language* (SFDL) [1], tiene dos características claves:

- Es representable en tres posibles variantes, XML, YAML y JSON, que le permiten adaptarse y ser óptimo en muchos escenarios.
- Integra la ejecución de funciones, tanto en cliente como servidor, lo que le confiere la capacidad de integrarse en la lógica de un motor de ejecución de workflow.

Además de la especificación formal del lenguaje, en el presente artículo se propone una arquitectura de integración de SFDL en un sistema de ejecución de workflow genérico, en el marco de un entorno bancario. En este entorno, los workflows se tienen que poder desarrollar ágilmente, otorgando a los diseñadores el control de todo el proceso, desde la funcionalidad hasta el diseño de la interfaz para el usuario final.

Toda la propuesta es totalmente compatible con el Modelo de Referencia [2] de la WfMC para su fácil integración en otros sistemas. Además, se basa en estándares como Atom, REST y Wf-XML-R.

El resto del artículo está organizado de la siguiente manera: la Sección II describe el estado del arte y los trabajos previos relacionados con la investigación. En la Sección III se ilustra el entorno de implantación objetivo al que va dirigida la propuesta planteada. La especificación formal de SFDL es introducida en la Sección IV. La Sección V presenta los aspectos a tener en cuenta para la integración de SFDL en un motor genérico de workflow. La validación de toda la propuesta se relata en la Sección VI. Y por último, en la Sección VII se enumeran las conclusiones.

II. ESTADO DEL ARTE

La solución propuesta en este trabajo se centra en la evolución de la interacción con el usuario, incorporando enlaces a la gestión interna de los flujos de trabajo.

Los formularios son, hoy en día, el mecanismo más común y sencillo para permitir el desarrollo de aplicaciones web interactivas. Existen diferentes alternativas para la generación de formularios web: HTML ha sido el lenguaje tradicionalmente usado para la creación de formularios, evolucionando hacia HTML5 [3] para añadir dinamismo; XForms [4] es la recomendación del W3C dentro de la especificación XHTML que permite separar la presentación del contenido, reutilizar esquemas y una reducción de accesos al servidor; MXML [5] es un lenguaje XML usado para los interfaces de usuario en la plataforma Flex de Adobe. Sin embargo, todas las alternativas mencionadas tienen un inconveniente: la dependencia con la sintaxis del lenguaje de script para ejecutar funciones en el lado del servidor.

SFDL se presenta como solución para la integración de la capa de presentación con los sistemas de gestión de workflow, Para ello, se proponen pequeñas modificaciones en las siguientes interfaces del Modelo de Referencia:

- Interfaz 1: el lenguaje de definición de procesos (OpenWFE [6] en nuestro caso, aunque bien podría ser BPEL o XPDL) será extendido para soportar una definición más amplia del workflow, incluyendo definición de vistas e información para el acceso dinámico a los datos.

- Servicio de Ejecución de Workflow: el motor requerirá cambios mínimos para soportar las nuevas características, especialmente aquellas relacionadas con el acceso al modelo de datos.
- Interfaz 2: se ha hecho una propuesta para reusar y extender el protocolo de comunicación basado en Atom de la Interfaz 4, manteniendo la coherencia con la Arquitectura de Referencia.

III. ESCENARIO

Nuestro escenario se desarrolla dentro del proyecto ITECBAN [7], el cual tiene como misión dotar de herramientas de software orientadas a las actividades colaborativas de una organización virtual para la construcción y evolución de los principales sistemas de información de una organización bancaria. ITECBAN debe soportar diferentes actividades colaborativas tales como el proceso de desarrollo de software dentro de un núcleo bancario, videoconferencia, gestión de contenido, etc. El sistema de gestión de workflow debe satisfacer los siguientes requerimientos funcionales:

- Diseño sencillo de formularios que permitan la especificación de tareas, reglas, roles de usuario y tipos de datos de entrada y salida que son necesarios en la ejecución de un workflow.
- Acceso del usuario a través de cualquier navegador web, usando estándares (como REST y Atom).
- Uso de un sistema de gestión de workflow de código abierto.
- Conexión con diferentes bases de datos como MySQL, LDAP –para gestión de roles/usuarios- y CMDB.

En concreto, el trabajo se centra en el diseño de workflows para la gestión de incidencias, cambios, problemas y órdenes de trabajo, con interfaces de usuario sencillos, flexibles, y modificables en cualquier momento.

Teniendo en cuenta los requerimientos descritos, es conveniente realizar una instanciación (Fig. 1) del modelo de referencia WfMC que describe en un alto nivel los principales componentes de un sistema de gestión de workflow, con énfasis en aquellas entidades e interfaces encontradas relevantes para el enfoque presentado en este escenario.

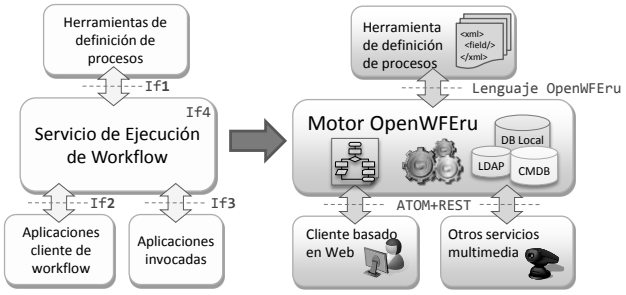


Fig. 1. Instanciación del modelo de referencia WfMC.

IV. SFDL: SIMPLE FORM DEFINITION LANGUAGE

Las extensiones propuestas a la arquitectura de un sistema de workflow están orientadas a la generación de formularios web, para la definición flexible de vistas desde el mismo proceso de diseño; y las operaciones básicas desde el lenguaje para acceder al modelo de datos. De este modo, un diseñador de workflows puede no sólo establecer el patrón de interacción, sino también definir las reglas básicas de la interfaz a través de la cual el usuario final hará uso de toda la funcionalidad subyacente, usando un único lenguaje: SFDL.

A. Definición del lenguaje SFDL

El Lenguaje Simple de Definición de Formularios (*Simple Form Definition Language*, SFDL) es un lenguaje de propósito especial definido teniendo en cuenta todos los requisitos funcionales previamente detallados. En particular:

- Soporta multitud de elementos de formularios web: selectores, tablas, elecciones, campos de entrada/salida…
- Es autocontenido: toda la información necesaria –componentes y estilo– está en un único fichero.
- Múltiples pantallas por vista: una única actividad en un workflow puede estar compuesta por varias pantallas en el cliente, que deben ser completadas antes de enviar la información de vuelta al servidor.
- Puede ser expresado en distintos lenguajes de marcado estándares, lo cual reduce la complejidad en el lado servidor.
- Soporta la ejecución de funciones en el servidor, para gestionar el modelo de datos desde/hacia las vistas.

Frente a otras alternativas de lenguajes de presentación, SFDL tiene ventajas:

- XForms comparte la orientación a diseño de formularios de SFDL, pero carece de un modo sencillo de ejecución de funciones. Además, su complejidad es elevada (usa CSS para definir los estilos) y su soporte en los clientes web actuales es prácticamente inexistente.
- Los formularios HTML5 gozan de un creciente soporte en los navegadores, pero no pueden ser fácilmente serializados para su proceso en JavaScript. Además, HTML no incluye llamadas anidadas a funciones.

Los ficheros en SFDL pueden estar definidos en una de tres posibles variantes: SFDL-X, -J o -Y (en XML, JSON o YAML), los cuales, aun siendo completamente equivalentes en funcionalidad, tienen sus propias particularidades que convierten a cada uno en adecuado para un entorno diferente.

B. Definición de vistas en SFDL

Para definir vistas dentro de las actividades de un workflow se usa un esquema simple basado en etiquetas para indicar la posición, tipo y valor de cada elemento, junto con algunos parámetros que definan con más precisión su estilo o funcionalidad. La Tabla 1 resume todos los campos.

Etiqueta	Descripción	Valores
type	Funcionalidad del elemento	label, input_text, text_area, text_block, selector, table, dynamic_table, link, attach, checkbox
params	Estilo del elemento	halign, width, height, hint…
value	Valor del elemento	Numérico, alfanumérico, función
result	Resultado de la interacción del usuario con el elemento	

Tabla 1. Campos de una vista.

Cada elemento está precedido de un identificador numérico que define la posición que tendrá en la pantalla del usuario. Por ejemplo, la Fig. 2 muestra la definición de un campo de tipo etiqueta en SFDL-Y, estando su valor definido como el resultado de la ejecución de la función *user-data*. El elemento se posicionará en las coordenadas (04, 30).

```
- id: 0430
  type: label
  value:
    function-name: user-data
    attribute-name: telephone
  params:
    halign: left
    width: "60"
```

Fig. 2. Definición de un campo en SFDL-Y.

Es importante destacar en este punto el hecho de que todos los formatos SFDL-* son equivalentes. La Fig. 3 muestra la definición del campo antes mencionado, pero ahora en SFDL-X (XML), con la particularidad de que este formato, una vez haya sido procesada la función, será idéntico al enviado al cliente a través de la Interfaz 2.

```
<field>
  <_>
   <id> 0430 </id>
   <type> label </type>
   <value>
    <_>
     <function-name> user-data </function-name>
     <attribute-name> telephone </attribute-name>
    </_>
   </value>
   <params>
    <halign> left </halign>
     <width> 60 </width>
   </params>
  </_>
</field>
```

Fig. 3. Definición de un campo en SFDL-X.

C. Funciones de acceso al modelo de datos

Uno de los requisitos más importantes de SFDL es ofrecer acceso al modelo de datos desde la definición de los formularios, empleando funciones. En este punto es necesario clarificar los dos modos posibles de ejecución de funciones:

- En tiempo de ejecución de workflows, cuando el motor de procesos ejecuta la definición.
- En tiempo de presentación, cuando se presenta el formulario al usuario final.

Para soportar ambos comportamientos se ha definido un mecanismo para llamar a las funciones tanto desde el lenguaje OpenWFE como desde las definiciones en SFDL, siguiendo un modelo funcional.

1) Funciones en tiempo de workflow

Las llamadas a función desde el lenguaje de definiciones han sido implementadas como referencias a un participante especial, siendo éste uno de los métodos más directos en OpenWFE. No obstante, la generalidad de esta aproximación queda garantizada en el sentido de que todo lenguaje tiene algún modo de añadir funciones externas. Manteniendo la línea del ejemplo de la Fig. 2, la llamada a *functions* para obtener el número de teléfono de un usuario sería la mostrada en la Fig. 4:

```
<participant ref="functions"
             function-name="user-data"
             attribute-name="telephone"
             out-field="phone"/>
```

Fig. 4. Llamada a función definida en un workflow.

Para este trabajo se ha implementado en el motor un conjunto de funciones que cubren las operaciones básicas de entrada/salida desde/hacia el modelo y las bases de datos empleadas en la arquitectura (LDAP, CMDB): *read-attribute*, *write-attribute*, *cmdb-out*, *user-data*… Sin embargo, el mecanismo de definición de funciones, permite fácilmente la extensión del conjunto inicial.

2) Funciones en tiempo de presentación

Las funciones que se ejecutan cuando el usuario abre una vista específica están definidas en el mismo lenguaje que dicha vista: SFDL, en cualquiera de sus variantes (-X, -J o -Y). Algunos ejemplos ya se han visto en la Fig. 2 y la Fig. 3. Esta aproximación tiene dos aspectos positivos de gran utilidad:

- Las funciones pueden ser anidadas y, siendo un lenguaje funcional, pueden ser usadas en cualquier punto de una definición de vista SFDL en lugar de un valor concreto.
- Hay una sola biblioteca de funciones en el sistema, con un único conjunto de nombres y parámetros (es decir, una sola interfaz de llamada), de modo que las llamadas desde SFDL son idénticas a aquellas realizadas desde OpenWFE, dando consistencia a la solución.

V. Implantación en un motor de workflow genérico

Una de las principales premisas en el diseño de SFDL ha sido la independencia con el motor de workflow. Para conseguir esta independencia, se ha reducido el acoplamiento con el motor, limitando los puntos de integración. De esta forma, se consigue la adopción de SFDL en cualquier motor con los mínimos cambios.

El único requisito para la inclusión de SFDL en un motor de workflow es la capacidad de llamar a funciones externas al propio motor en dos momentos distintos: en primer lugar, durante la ejecución del flujo de trabajo y, en segundo lugar, en el momento de presentar información al usuario. El objetivo es poder ejecutar las mismas funciones independientemente del momento. Así, todas las funciones disponibles estarán empaquetadas en una biblioteca común.

Para un motor de workflow con SFDL, una posibilidad muy recomendable es que su comunicación con los clientes se realice a través de una interfaz REST basada en Wf-XML-R [8]. La representación de las variables necesarias para la generación dinámica de formularios va más allá del ámbito de Atom y Wf-XML-R. De esta forma, en el ámbito de esta investigación se ha creado una extensión, con su espacio de nombres propio, para la adopción de SFDL dentro de Atom.

VI. Validación

Nuestro trabajo ha sido validado en el escenario bancario ya presentado. Para los flujos de trabajo definidos dentro de ITECBAN se realizó el proceso de identificar las variables y operaciones a tener en cuenta en la ejecución de los flujos, así como las interfaces de usuario requeridas. Las primeras

fueron codificadas con el lenguaje OpenWFE y ejecutadas con el motor correspondiente. Las interfaces de usuario se especificaron a través del lenguaje SFDL (la Fig. 5 recoge un extracto del código para la primera vista).

```
screens:
  - id: default
    title: "%title.incident.register%"
    fields:
      - id: "0204"
        value:
          function-name: read-attribute
          attribute-name: launcher
        type: label
        params:
          halign: left
      - id: "1001"
        type: result_table
        params:
          data_source: cmdb
          dynamic_columns: true
          height: "110"
      - id: "2405"
        value:
          1:
            id: urgency.high
            name: "%urgency.high%"
          2:
            id: urgency.low
            name: "%urgency.low%"
        type: selector
        params:
          default: urgency.high
[…]
      - id: "2611"
        value: submit
        type: button
        params:
          button_text: "%incident.open%"
          button_result: "open"
          compulsory_fields:
            - "1001"
```

Fig. 5. Definición en SFDL-Y

La Fig. 6 representa la vista o interfaz de usuario para registrar o crear una nueva incidencia generada en el flujo de gestión de incidencias. Esta interfaz corresponde al primer paso del workflow ("Registrar Incidencia").

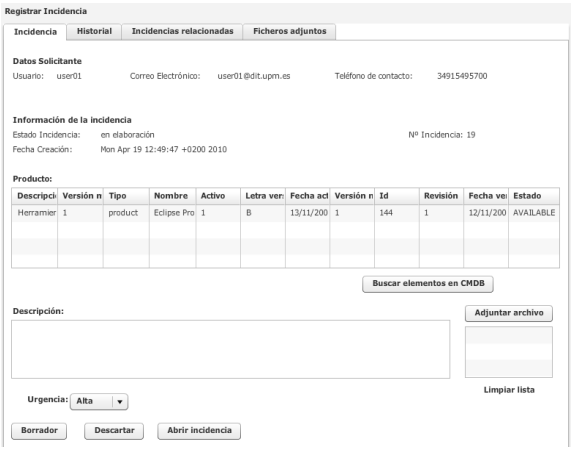


Fig. 6. Pantalla generada en SFDL: Registrar Incidencia.

La pantalla generada a partir de código SFDL tiene un alto grado de funcionalidad, sin sacrificar la usabilidad.

Nuestro enfoque ha permitido a los gestores de workflows del escenario presentado, reducir sus esfuerzos en la creación y ejecución de workflows, permitiéndoles ganar productividad.

VII. CONCLUSIONES

El resultado de esta investigación ha sido la especificación de un nuevo lenguaje de definición de vistas dinámicas, SFDL, optimizado para motores de workflows. Por un lado, a través de la definición de flujos, un motor de workflow puede generar formularios dinámicos con usabilidad mejorada con la posibilidad de interactuar con servicios web y el acceso al modelo de la base de datos. Por otra parte, un usuario con un navegador web puede interactuar con el sistema de workflow a través de estos formularios de workflow dinámicos. Nuestro trabajo se ha basado en el uso de estándares ampliamente aceptados y propuestas abiertas, siendo posible la definición del lenguaje SFDL en XML, YAML y JSON.

La arquitectura propuesta ha recibido bastante realimentación ya que ha sido validada dentro de un escenario bancario real; ha permitido ofrecer a los diseñadores de workflow los mecanismos para incluir especificación de vistas dentro de la definición de procesos. Asimismo se ha permitido establecer una serie de métodos de acceso al completo modelo de base de datos dentro del lenguaje para asegurar que el workflow sea dinámico. Adicionalmente, la arquitectura diseñada es simple, y mantiene la compatibilidad con el Modelo de Referencia (por ejemplo, reutilizando protocolos como el Wf-XML-R), sin renunciar a la portabilidad (evitando introducir profundas modificaciones específicas de una plataforma determinada) y manteniendo la flexibilidad y extensibilidad, las cuales son esenciales en este tipo de proyectos. De esta manera, se recomienda el uso de estos formatos validados y arquitecturas en escenarios con similares requerimientos.

VIII. AGRADECIMIENTOS

Este trabajo ha sido soportado por el proyecto ITECBAN, el cual ha sido financiado por el CDTI (Centro para el Desarrollo Tecnológico e Industrial) y el Ministerio de Industria, Turismo y Comercio. Asimismo, los autores agradecen a INDRA Sistemas, S.A. (http://www.indra.es/) su valiosa contribución a este trabajo.

REFERENCIAS

[1] The SFDL definition: a Simple Form Definition Language. http://sfdl.dit.upm.es/

[2] D. Hollingsworth, "The Workflow Reference Model Version 1.1". Winchester, UK: Workflow Management Coalition, WFMC-TC-1003, Jan. 1995.

[3] W3C HTML 5. Available at http://dev.w3.org/html5/spec/. Mar. 2009.

[4] W3C XForms 1.0 (Third Edition). Available at http://www.w3.org/TR/xforms/. Mar. 2009.

[5] C. Coenraets, "An overview of MXML: The Flex markup language", Adobe Systems. March 2004. Available at http://www.adobe.com/devnet/flex/articles/paradigm.html. Mar. 2009.

[6] OpenWFEru – open source ruby workflow engine. http://openwferu.rubyforge.org/. Last accessed March 2010.

[7] ITECBAN. http://caching.indra.es/sites/default/files/Itecban_baja_0.pdf

[8] M. Zukowski, P. Cappelaere, K. Swenson, "A RESTFul Protocol for Run-Time Integration of Process Engines". Draft 5. Apr. 2008.

Servicios telemáticos sobre nubes privadas en plataformas virtualizadas y distribuidas

N. Arbós, L. M. Amorós, D. González, A. Oller, J. Alcober

Departamento de Ingeniería Telemática
Universitat Politécnica de Catalunya, Fundació i2cat
Esteve Terradas, 7 - 08860 Castelldefels.
noemi.arbos@i2cat.net, luismi.amoros@i2cat.net, david.gonzalez@i2cat.net, antoni.oller@upc.edu, jesus.alcober@upc.edu

***Resumen* – En la actualidad, el modelo para proporcionar servicios basados en alojar cada aplicación en un servidor físico no es el modelo óptimo, ya que los avances tecnológicos tanto en hardware como en software hacen que se produzca un desaprovechamiento de los recursos ofrecidos. Por este motivo, este trabajo presenta un nuevo modelo basado en un clúster de servidores con sistema de ficheros distribuido en red y virtualización de sistemas operativos que mejora la utilización de los recursos disponibles. Esta nueva arquitectura ofrece una nube privada que simplifica la gestión de los servicios y aporta una disminución del coste de mantenimiento, además de añadir flexibilidad, dinamismo y escalabilidad al sistema.**

***Palabras Clave*- Virtualización, Clúster, NFS, Cloud Computing, Iaas.**

I. INTRODUCCIÓN

Actualmente, la mayoría de entidades y empresas utilizan una gran cantidad de hardware, en especial servidores, para proporcionar sus servicios de infraestructura. Por cuestiones de seguridad y redundancia se ha ido siguiendo un modelo de un equipo para cada servicio. Sin embargo, el crecimiento exponencial de las capacidades de computación del hardware que ofrece el mercado [1], propicia que este modelo de utilización de los recursos no sea óptimo [2].

Por este motivo surge la virtualización, que trata de ofrecer una mejor utilización de los recursos de una máquina creando una capa de abstracción entre el hardware de la máquina física y el sistema operativo de la máquina virtual, el cual es totalmente independiente lo que permite que los posibles errores de funcionamiento de la máquina virtual no provoquen efectos colaterales a las demás.

Por otro lado, las arquitecturas de servicios evolucionan, y en este contexto, el paradigma de computación en nube, Cloud Computing [3], permite ofrecer un nuevo punto de vista para la construcción de servicios de computación sobre internet. Bajo este esquema y en una modalidad de nube privada se intenta potenciar el concepto de IaaS, Infraestructure as a Service, donde la arquitectura propuesta ofrece un nuevo modelo de servicio orientado especialmente a infraestructura.

El trabajo que se presenta, realiza una propuesta arquitectónica de nube privada basada en diferentes tecnologías, todas ellas independientes, reemplazables y adaptables a las diferentes herramientas existentes. Se trata de una plataforma virtualizada, dinámica y distribuida formada por dos tipos de nodos. Un primer tipo de nodos de alta capacidad de procesamiento y un segundo tipo de nodos que proporciona el espacio de almacenamiento. Mediante un sistema de ficheros distribuido y utilizando protocolos de red, se integran ambos nodos. Este sistema distribuido mejora la escalabilidad y el tiempo total que el sistema está funcionando (Uptime) respecto a otras arquitecturas.

II. VIRTUALIZACIÓN

Virtualización es un término que se refiere a la abstracción de los recursos de una máquina. Esta capa de abstracción, más conocida como Hypervisor, se encarga de manejar y gestionar los recursos de hardware principales, CPU, disco, memoria RAM, etc. Por tanto, Hypervisor es el encargado de repartir estos recursos entre las diferentes máquinas virtuales que se estén ejecutando sobre la misma máquina física.

Dependiendo del hardware y del sistema operativo podemos distinguir hasta cuatro tipos de virtualización diferentes:

1) *Emulación o simulación*: el sistema operativo padre simula un hardware completo.

2) *Virtualización a nivel de Sistema Operativo*: se basa en crear celdas de usuarios independientes, sin acceso entre ellas.

3) *Paravirtualización*: la máquina virtual no simula un hardware, sino que ofrece una interfaz al sistema que sólo puede usarse mediante la modificación del kernel del sistema operativo de la máquina virtual.

4) *Virtualización nativa:* la máquina virtual simula un hardware subyacente completo para permitir un sistema operativo sin modificar en la máquina virtual.

Estas técnicas de virtualización ofrecen grandes mejoras y ventajas respecto a un sistema de hardware nativo:

- **Ahorro:** Mejora substancialmente el aprovechamiento de los recursos de hardware, lo que se traduce en un gran ahorro en cuanto a coste del hardware y también un ahorro en cuanto a energía consumida y espacio.
- **GreenIT [4]:** Al reducir el número de máquinas, reducimos la cantidad de energía utilizada, no sólo en alimentar el servidor sino que también se reduce el

consumo de refrigeración tanto eléctrico como las emisiones de aire caliente.

- **Flexibilidad:** En una misma máquina podemos tener funcionando juntos un sistema operativo Windows y un sistema basado en GNU/Linux [5].
- **Escalabilidad y Uptime:** La virtualización ofrece un sistema totalmente homogéneo a las máquinas virtuales.

III. Arquitectura del Sistema

Tal como ilustra la figura 1, la arquitectura propuesta consta de 3 tipos de elementos:

- **Un Servidor Máster:** está conectado a una cabina de discos y su función es orquestar y controlar los servidores esclavos utilizando los recursos de la nube según sea necesario.
- **Clúster de Servidores Esclavos:** está formado por N servidores esclavos. Este tipo de nodos carecen de disco duro y, en consecuencia, son equipos limitados ya que sólo disponen de memoria RAM y CPU. Por lo tanto, los datos han de ser almacenados en la cabina de discos del servidor máster.
- **Máquinas Virtuales:** se crean dinámicamente sobre los nodos esclavos, aprovechando los recursos libres que el máster les asigna.

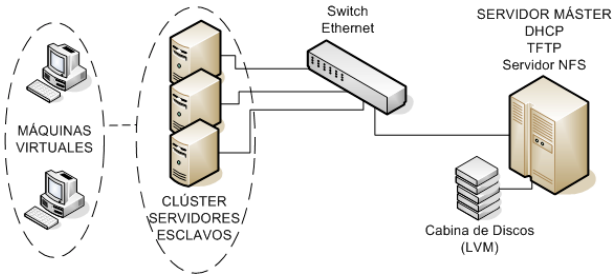


Fig. 1. Arquitectura del sistema.

Uno de los puntos críticos de la arquitectura es el proceso de inicialización. Los servidores esclavos cargan sus sistemas operativos a través de la red. Para solventar este problema se utiliza el protocolo PXE [G1], que consiste en la combinación de dos protocolos. El servicio DHCP [6], se utiliza para obtener una dirección IP y localizar el servidor de arranque. El servicio de TFTP [7], se utiliza para transferir un microkernel desde el servidor máster hasta el nodo esclavo. Una vez descargado el kernel se ejecuta en la memoria RAM. En nuestro caso, este kernel ha sido compilado con las opciones de virtualización y el sistema de ficheros esclavo ya dispone del software de virtualización Xen [8]. Se ha escogido Xen como sistema de virtualización ya que dispone de una versión open source muy eficiente y potente, que permite tanto paravirtualización como virtualización nativa, dependiendo de las necesidades, en contraste con otras plataformas como VirtualBox [9] o VMware [10].

Para conseguir dinamismo, el sistema de ficheros de los servidores esclavos se reserva en la cabina de discos mediante LVM [G2] y se monta utilizando el protocolo NFS [G3], lo que permite a las máquinas montar particiones en un sistema remoto y usarlas como si estuvieran en un sistema de archivos local. Este sistema nos permite ejecutar máquinas virtuales sobre los servidores esclavos. Para facilitar la flexibilidad del sistema, estas máquinas virtuales montan el sistema operativo a través de NFS mediante LVM en la cabina de discos, de forma similar a los servidores esclavos.

Un ejemplo del funcionamiento del sistema lo podemos observar en la figura 2, donde encontramos un servidor esclavo (E.1) que ha arrancado el sistema operativo por red, mediante el protocolo PXE, y tiene el sistema de ficheros ubicado en la cabina de discos del servidor máster gracias al uso de NFS. También hay N máquinas virtuales ejecutándose en el esclavo (M.V.1, … , M.V.N). Cada una de ellas hace uso de una proporción de RAM y CPU del servidor según sus necesidades, y tienen alojado el sistema de ficheros en la cabina de discos mediante NFS.

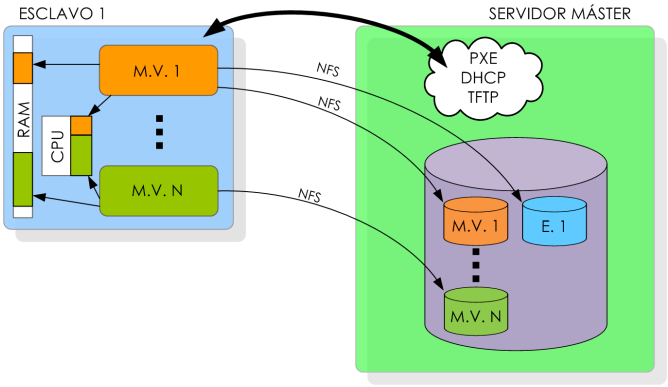


Fig. 2. Funcionamiento del sistema.

Este sistema nos ofrece flexibilidad debido a que, los ficheros/datos (tanto S.O como datos de usuario) están alojados en el máster y se puede orquestar y decidir donde se ejecutan las máquinas virtuales. Estas características nos permiten:

- *Live migration:* migración en tiempo real de las máquinas virtuales.
- Una gran tolerancia a fallos: si uno de los servidores esclavos falla, la plataforma, de manera dinámica, detecta la caída y se migran las máquinas virtuales a otro nodo.
- Balanceo de la carga: si un esclavo está saturado podemos migrar las máquinas a otro nodo.
- Escalabilidad: el numero N de servidores esclavos no tiene cota, viene definido únicamente por las necesidades totales.
- Todas las ventajas que aporta la virtualización.

IV. Escenario de Pruebas

El escenario de pruebas consta de dos tipos de nodos con las siguientes características:

- **Servidor Máster:** utilizamos un equipo Supermicro X8DTN+ que dispone de un procesador Quad Core Intel Xeon E5504 Nehalem de 64 bits, 12 GB de memoria RAM DDR3 y una cabina de discos de 15 TB.
- **Servidores Esclavos:** utilizamos 10 equipos Supermicro 5016T-MRB que dispone cada uno de un procesador Quad Core Intel Xeon E5504 Nehalem de 64 bits y 12 GB de memoria RAM DDR3.

El escenario, tal como muestra la figura 3, está formado por 2 segmentos de red. En el primero utilizaremos direccionamiento privado y se utilizará para el PXE y el NFS de los servidores esclavos, en el segundo segmento utilizaremos direccionamiento público para acceder a Internet y el NFS de las máquinas virtuales.

Por lo tanto, todos los servidores han de disponer de dos tarjetas de red, una para la red privada y otra para la red pública. Las máquinas virtuales, sin embargo, sólo tendrán acceso a la red pública.

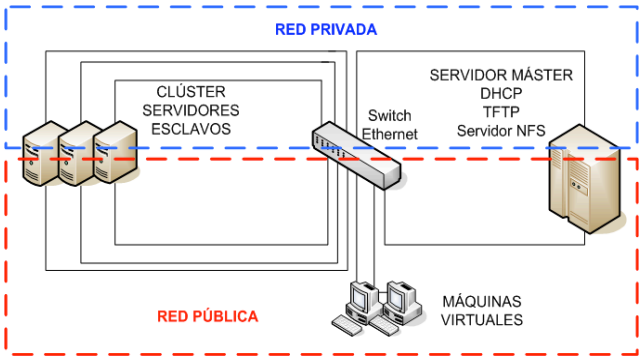


Fig. 3. Escenario de pruebas.

El servicio de NFS está configurado para funcionar utilizando TCP, que asegura que llegan todos los datos de un punto a otro sin errores, con permisos de escritura y lectura para el usuario remoto. También se ha configurado de tal manera que los usuarios remotos pueden actuar como *root* en el sistema local. Como método de escritura, se ha escogido la opción de escritura síncrona, es decir, todas la escrituras en el disco se realizan antes de devolver el control al cliente remoto, aunque esta opción puede disminuir el rendimiento se asegura que no se pueden perder datos si el servidor principal cae o se apaga.

V. PRUEBAS DE RENDIMIENTO

El modelo de innovación de esta arquitectura se basa en la flexibilidad que ofrece el sistema de discos por red y la nube de servidores esclavos.

Este sistema tiene un inconveniente principal, la pérdida de rendimiento respecto a un sistema en local debido al uso del protocolo NFS. Por esta razón, se han realizado pruebas tanto de lectura como escritura en disco comprobando el rendimiento de los servidores esclavos y las máquinas virtuales a través de NFS y de esta forma validar el sistema. Todas las pruebas han sido realizadas con la herramienta Spew [11].

Pruebas de escritura en disco: consisten en la escritura de un megabyte de datos utilizando bloques de 512 bytes en un fichero determinado. Se han realizado 50 iteraciones de este proceso y se ha extraído la media aritmética de las tasas de escritura.

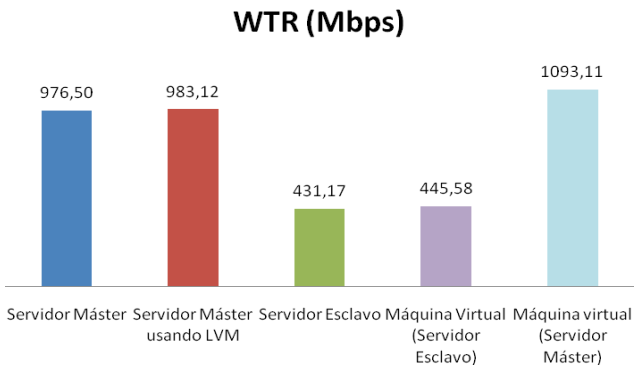


Fig. 4. Resultados de Write Transfer Rate.

Según los resultados obtenidos en las pruebas de escritura en disco, tener el sistema de ficheros de los servidores esclavos y las máquinas virtuales mediante NFS causa que la tasa de escritura disminuya entre un 50-55% respecto al servidor principal.

La causa de esta pérdida de rendimiento del NFS en escritura se debe a que utilizamos escritura síncrona, por lo tanto, se realizan todas las operaciones de escritura en disco solicitadas antes de devolver el control al cliente. De esta forma, disminuye el rendimiento obtenido, pero por otra parte, nos aseguramos que los datos se guardan correctamente

Además, el hecho de utilizar TCP puede provocar retransmisiones en caso de errores en la transmisión. Este hecho podría causar una disminución del rendimiento de nuestro sistema NFS, tanto en lectura como en escritura. Es cierto que se podría haber utilizado UDP ya que se trata de una red de área local donde la tasa de error es realmente baja, pero un pequeño error en el envío de información podría haber causado la inutilización del servicio alojado en las máquinas virtuales.

Pruebas de lectura en disco: consisten en la lectura de un megabyte de datos utilizando peticiones de 512 bytes de un fichero determinado. Se han realizado 50 iteraciones de este proceso y se ha extraído la media aritmética de las tasas de lectura.

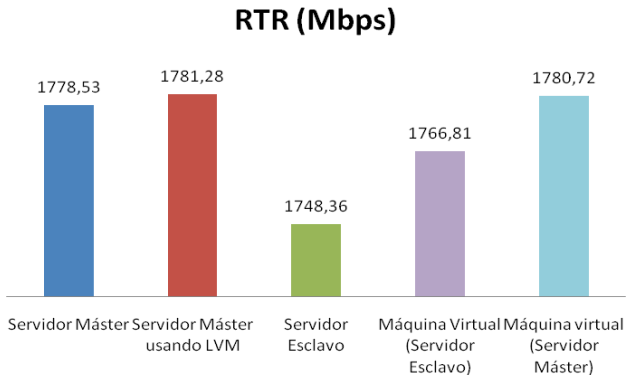


Fig. 5. Resultados de Read Transfer Rate.

Las pruebas realizadas en lectura de disco han sido satisfactorias, ya que la pérdida de tasa de lectura respecto al servidor principal ha sido de entre un 1-2%, en el caso de un servidor esclavo; y de entre un 0,5-1% en las máquinas virtuales ejecutadas en un servidor esclavo, lo que nos indica un rendimiento muy alto en lectura.

VI. Aplicaciones y Beneficios

Una de las principales ventajas es la mejor utilización del rendimiento de un servidor físico para crear más de un servidor virtualizado, dedicando una máquina virtual para cada aplicación. Esta alternativa permite utilizar la mayor parte de esos recursos creando servidores virtuales aislados entre si de forma que existen varios servicios con una única máquina física.

La arquitectura propuesta, basada en un servidor físico que aloja varios servidores virtuales, además de extraer un mayor rendimiento de los recursos, es una solución escalable, barata y fácil de mantener. El hecho de utilizar máquinas virtuales hace posible trasladarlas de una máquina física a otra en caso de fallo de una de éstas, mediante *Live migration*: mover máquinas virtuales entre servidores físicos sin detener la prestación de servicios, proporcionando una gran flexibilidad. Además, el mantenimiento del hardware y el coste energético disminuye respecto a la arquitectura un servidor físico sobre un servicio, ya que utilizamos menos máquinas físicas para muchos más servicios.

Otro de los beneficios que aporta esta nueva arquitectura, es que los sistemas operativos virtualizados no tienen dependencia del hardware, ya que se crea una capa de abstracción entre el sistema operativo utilizado y el hardware real. De esta forma, podemos tener máquinas virtuales con sistemas operativos diferentes en una misma máquina física.

Desde el punto de vista del usuario final, el hecho de que los servidores físicos monten su sistema de ficheros principal por NFS y arranquen mediante PXE, es totalmente transparente. Lo mismo ocurre con el hecho de utilizar máquinas virtuales para alojar los servicios, ya que cada servidor virtual tendrá las mismas prestaciones que un servidor físico tradicional.

VII. Conclusiones

En este artículo se ha presentado un nuevo sistema con unas características que hacen que sea una opción eficiente frente a otro tipo de arquitecturas, esto es debido al modelo de arquitectura presentado en este trabajo y las caracteristicas y dinamismo que ofrece.

Por otra parte, se ha comprobado que el rendimiento final que se puede obtener es satisfactorio ya que a pesar que las perdidas que genera la arquitectura pueden llegar a suponer un coste de casi un 50% en la tasa de escritura, la flexibilidad que ofrece esta arquitectura compensa con creces estas pérdidas en entornos donde la escritura en disco no supone un requerimiento muy importante. En cambio, los resultados de las tasas de lectura en disco son muy buenos, ya que se obtienen valores similares a las tasas de lectura en un entorno de acceso físico al espacio de almacenamiento. Esto es especialmente importante en entornos de servicios, en especial web, donde se reciben miles de peticiones de lectura por segundo y prima más el tiempo de respuesta ante fallos y la capacidad de escalar el sistema que la tasa de escritura en disco.

Los diferentes protocolos utilizados, como PXE, NFS, TFTP, etc., y la virtualización son totalmente transparentes al usuario final, de esta manera, se consiguen todas las ventajas de utilizar esta nueva arquitectura sin afectar a la visión del usuario final del sistema que acceda a una de los servicios ofrecidos.

Esta arquitectura puede ser ampliada para hacer más sencilla la tarea de administración del clúster de servidores y máquinas virtuales mediante un sistema de gestión o controlador. También se puede mejorar la creación y monitorización de las máquinas virtuales a través de una herramienta de gestión especifica, como por ejemplo OpenNebula [12] o Ganeti [13].

De esta manera, se ofrece una plataforma distribuida con un paradigma basado en nube potenciando la infraestructura como servicio, y ofreciendo una arquitectura sobre la que desplegar servicios.

Agradecimientos

Este trabajo ha sido apoyado por el MCyT (Ministerio de Ciencia y Tecnología del Gobierno de España) en el marco del proyecto TSI2007-66637-C02-01, parcialmente financiado por el FEDER.

Referencias

[1] Ley de Moore
[http://es.wikipedia.org/wiki/Ley_de_Moore]

[2] J. Pujal; A. Oller; J. López; C. Fanning; F. Minerva; J. Alcober; Escritorios remotos en máquinas virtuales aplicados en grandes corporaciones; Boletín de RedIRIS, nº 85-86, marzo-2009 Pág. 42-49.
[http://www.rediris.es/difusion/publicaciones/boletin/85-86/ponencias85-5.pdf]

[3] M. Armbrust; A. Fox; R. Griffith; A. Joseph; R. Katz; A. Konwinski; G. Lee; D. Patterson; A. Rabkin; I. Stoica; M. Zaharia; Above the Clouds: A Berkeley View of Cloud Computing; UCB/EECS; Technical Report No. UCB/EECS-2009-28, febrero-2009.
[http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html]

[4] GreenIT – sustainable information technology
[http://www.greenit.net/]

[5] Linux
[http://www.linux.org/]

[6] R. Droms; RFC 2131 "Dynamic Host Configuration Protocol"; marzo-1997.
[http://www.rfc-editor.org/rfc/rfc2131.txt]

[7] K. Sollins; RFC 1350 "Trivial File Transfer Protocol"; julio-1992.
[http://www.rfc-editor.org/rfc/rfc1350.txt]

[8] Xen
[http://www.xen.org/]

[9] VirtualBox
[http://www.virtualbox.org/]

[10] VMware
[http://www.vmware.com/es/]

[11] Spew
[http://spew.berlios.de/]

[12] OpenNebula
[http://opennebula.org/]

[13] Ganeti
[http://code.google.com/p/ganeti/]

[14] D. González; A. Oller; Desarrollo de una plataforma de virtualización; Bachelor thesis, UPC, EPSC, 3-abr-2008.
[http://upcommons.upc.edu/pfc/handle/2099.1/4798]

[15] J. Pujal; Proposal of remote virtual desktops architecture working with thin client devices; Master thesis, UPC, 16-jul-2008.
[http://upcommons.upc.edu/pfc/handle/2099.1/5320]

Glosario

[G1] PXE: Preboot eXecution Environment
[http://es.wikipedia.org/wiki/PXE]

[G2] LVM: Logical Volume Manager
[http://es.wikipedia.org/wiki/LVM]

[G3] NFS: Network File System
[http://es.wikipedia.org/wiki/Network_File_System]

3DTour - Mundos virtuales 3D aplicados al sector turístico

Miguel Coronado, Carlos A. Iglesias
Departamento de Ingeniaría de Sistemas Telemáticos
Universidad Politécnica de Madrid
Avda. Complutense, 30. CP:28040 Madrid
miguelcb@gsi.dit.upm.es, cif@gsi.dit.upm.es

Guillermo Hernández
Idea Informática
Grupo Gesfor
C/ San Sotero, 11 CP:28037 Madrid
ghernandezc@grupogesfor.com

***Resumen*—El artículo presenta el mundo virtual 3DTour. El objetivo del proyecto es recrear un hotel dentro de un mundo virtual y poblarlo con empleados y clientes controlados por bots a través del desarrollo de un módulo para la integración de bots en mundos virtuales. El objetivo es estudiar la viabilidad de utilizar dicho escenario como un expositor para clientes de los servicios ofrecidos por hoteles, y evaluar el comportamiento de los usuarios del mundo virtual ante la presencia de avatares controlados por bots para poder determinar si la actitud de estos frente a un bot difiere al desconocer la naturaleza del mismo.**

***Palabras Clave*—Mundo virtual, OpenSimulator, chatbot, AIML, turismo**

I. Introducción

Prácticamente desde el comienzo de la andadura de los ordenadores, los programadores han tenido la ambición de crear programas que fueran capaces de mantener una conversación con un interlocutor humano. Posiblemente comenzaron como un juego o entretenimiento para el programador pero hoy en día están muy extendidos y cada vez más perfeccionados. Los primeros bot conversacionales o chatterbots, como son conocidos, datan de la década de los 60, era necesario un ordenador dedicado a su funcionamiento y sólo una persona podía utilizarlos a la vez. En la actualidad, con el gran desarrollo de la Web es imposible imaginarlos desligados de Internet y son capaces de atender multitud de conversaciones simultáneamente. Ya no sólo aparecen como aplicaciones de demostración en la página del autor sino que se encuentran integrados, por ejemplo, en canales de IRC, como agentes en sistemas de mensajería instantánea, agentes expertos en FAQ, servicios de atención al cliente, sistemas domóticos... Por supuesto forman parte de numerosas aplicaciones comerciales.

La evolución en la interfaz de usuario de los ordenadores ha sufrido una evolución más vertiginosa si cabe. Desde las primera pantallas de caracteres en blanco y negro hasta las modernas pantallas en 3D o desde el primer teclado hasta los dispositivos apuntadores inalámbricos como el Wii Remote. Cada avance en este campo ha abierto las puertas a un gran número de nuevas aplicaciones: la aparición del ratón y la mejora en la tecnología de monitores permitió la aparición de sistemas operativos con ventanas, con los joystick y pads apareció una nueva generación de videojuegos, la mejora en la potencia de las tarjetas gráficas la reproducción de vídeo de alta definición...

Los mundos virtuales, se encuentran entre las últimas innovaciones en interfaces de usuario. Al igual que las descritas anteriormente, los mundos virtuales despliegan un abanico de posibles aplicaciones y negocios en torno a ellos. Son el escenario de juegos multijugador, albergan telereuniones de empresas o sirven para promoción turística mediante la recreación de museos y monumentos destacados.

Los mundos virtuales ven supeditado su valor global al uso que los usuario hacen de ellos. El mundo virtual con mayor nivel de detalle en la construcción del escenario no tendrá valor alguno si no hay una comunidad de usuarios que lo pueble diariamente, ya que ningún usuario querrá utilizar dicho mundo si no hay nadie con quien interaccionar.

La tecnología de bots puede ayudar a suplir esta carencia, puesto que se se pueden incluir avatares en el mundo virtual asociados a bot conversacionales de manera que otros usuarios no solo perciban su presencia, sino que puedan mantener una conversación en lenguaje natural o incluso llevar a cabo transacciones dentro el mundo virtual.

En este artículo de describe un sistema en el que se ha completado con éxito la integración de bots en un mundo virtual, un escenario actualmente en auge, y orientado hacia una aplicación corporativa del sector turístico. La plataforma integra un mundo virtual creado utilizando OpenSim y diversos bots con distintas personalidades creados utilizando la tecnología de bots AIML.

Este trabajo se ha desarrollado dentro del proyecto 3DTour Mundos virtuales 3D aplicados al sector turístico para la creación de un mundo virtual que contenga varios agentes expertos en información turística de Madrid.

El resto del artículo se estructura como sigue. La sección II presentan los retos tecnológicos que se presentan al acometer este proyecto. A continuación, la sección III presenta la arquitectura del sistema centrándose en los dos componentes principales, el mundos virtual en OpenSim y el servidor de bots con la base de conocimieto desarrollada para este proyecto. Por último, la sección IV recoge las principales conclusiones y los trabajos futuros.

II. Retos Tecnológicos

Desde el punto de vista tecnológico, el proyecto 3DTour plantea diversos retos. Por un lado, se pretende innovar utilizando la tecnología de mundos virtuales 3D en auge actualmente, sobre todo en el sector de ocio, enfocándolo hacia una aplicación corporativa del sector turístico. Se pretende así explotar la interactividad e inmersión presente en todo mundo virtual para ofrecer una visión lúdica que permita captar de manera eficaz la atención de los usuarios. Por otro lado, para dotar de más realismo a los servicios que se ofertarán en el

mundo virtual se integrará la tecnología de bots, que además facilitará el acceso a la información a los clientes. Puesto que el entorno es propicio para camuflar los bots como otros usuarios humanos se incluirán también otros bots con el papel de usuarios en el mundo virtual y no solo empleados de manera que el usuario que se conecta perciba actividad en el escenario y se encuentre acompañado mientras explora el entorno virtual diseñado para 3DTour.

A. Aplicaciones y escenarios de mundos virtuales

La tecnología de mundos virtuales abre un amplio abanico de posibles aplicaciones y escenarios. Su principal baza es ofrecer al usuario la posibilidad de hacer algo que no puede hacer, en ese momento y en ese lugar, en la vida real. El avatar del usuario, puede transportarse inmediatamente a puntos del mundo virtual pudiendo visitar cualquier monumento y lugar de interés recreado en el entorno virtual, permite realizar varias acciones a la vez pudiendo mantener varias conversaciones al mismo tiempo o mientras se asiste a una exposición o una reunión.

Muchos mundos virtuales están orientados a entornos profesionales -los que no están orientados al ocio- y son utilizados en escenarios de colaboración y formación inmersiva en grandes organizaciones.

Como ocurre con otras tecnologías innovadoras, la tecnología de mundos virtuales se está aplicando a la educación [9] y formación de personal. También son una herramienta con múltiples posibilidades en la propagación y preservación de la cultura [7]. Actualmente existen varios mundos virtuales para fomentar el turismo y el acceso a la cultura. Todos ellos se centran en la recreación de monumentos, museos, ciudades u oficinas de turismo, los cuales únicamente proporcionan información. Este es el caso del casco histórico de Gijón o la plaza mayor de Valladolid.

Con 3DTour y gracias a la tecnología de los mundos virtuales y su integración con bots, se pretende dar valor añadido e ir más allá de la meramente informativa para que los usuarios además puedan interactuar entre ellos y con la empresa, así como proporcionar distintos servicios reales que puedan ser consumidos en el mundo virtual.

B. Tecnología de bots en mundos virtuales

Con el desarrollo tecnológico de la Web la tecnología de bots está cada vez mas presente en Internet, aumenta gradualmente el número de sitios Web que dan servicios de hosting de bots [1] o que tienen un negocio relacionado con servicios de bots. Sin embargo, aunque podemos encontrar numerosos bots en páginas dedicada a la demostración de los mismos o en sistemas de mensajería instantánea, no es tan frecuente encontrarlos en la página Web de una organización o de una empresa. Los mundos virtuales ofrecen un escenario idóneo para incorporar masivamente estos bots en un entorno en el que tienen muchas más capacidades de las que tienen en una página Web. De hecho, un usuario y un bot que controla un avatar en un mundo virtual tienen las mismas capacidades, de manera que, salvando las distancias están en igualdad de condiciones.

El mero hecho de que los bots sean fácilmente reconocidos como máquinas hace que los interlocutores humanos descuiden la conversación al comunicarse con ellos. Esto hace complica la evaluación de la base de conocimiento de un bot, pues lo usuarios tienden a dirigir la conversación con palabras clave en lugar de construir frases correctas. Los mundos virtuales constituyen un escenario idóneo para la evaluación de bots conversacionales pues cualquier usuario que converse con ellos tiende a considerarlos, a priori, como otro usuario del sistema [3]. De esta manera se las conversaciones registradas en el logger pueden ser utilizadas para la mejora de la base de conocimiento del bot.

Por otro lado, la integración de tecnología de bots en el mundo virtual supone una aporte de valor añadido para al mundo virtual. Añade un mayor grado de interacción, pues permite realizar acciones tales como reservar una sala de juntas, consultar las reservas disponibles o a través de una conversación en lenguaje natural, dando así una mayor dosis de realismo al escenario. En general los usuarios valoran muy positivamente los sistemas con los que se puede interactuar a través del lenguaje natural para desempeñar una tarea [8].

La inclusión de bots en el mundo virtual también convierte a este en un mundo más acogedor, pues el usuario percibe mayor grado de actividad al encontrar un mayor número de avatares en el escenario [2]. Este concepto, ha llevado a la práctica en [6] con la inclusión de bots en foros con el propósito de responder rápidamente a las preguntas cuya respuesta conoce el sistema y dar así una sensación de eficiencia en el servicio.

C. Bots en el sector turístico

Al igual que los mundos virtuales, los bots conversacionales están siendo utilizados en diversos campos de aplicación como agentes que sirven información o ofrecen promociones a través de mensajería instantánea, agentes expertos en FAQ incrustados en páginas Web, servicios de atención al cliente o sistemas domóticos.

En general, para que un bot conversacional sea apto para realizar una tarea es necesario que el volumen de conocimiento que necesita conocer sea acotado. Este es precisamente el caso del sector turístico, el conocimiento que necesita el bot se restringe a conocimientos generales acerca de la región en que se encuentra y conocimientos más a fondo del monumento u hotel para el que trabaja. Los bots en el sector turístico constituyen una opción de valor pues prácticamente pueden desempeñar el trabajo que realizan los empleados de una oficina de turismo o un recepcionista de un hotel.

Fig. 1. Avatar de un bot recepcionista en 3DTour

III. Arquitectura del sistema

Para 3DTour se ha desarrollado un mundo virtual que representa un complejo hotelero con diversas dependencias: hall, salones, habitaciones, sala de reuniones, recepción... Dicho escenario está integrado en un mundo virtual de OpenSim, por lo que los usuarios pueden moverse e interactuar con el mundo. Para dotar al mundo de mayor realismo se han desarrollado varios bots que han sido integrados en el mundo virtual, de manera que el usuario pueda interactuar con ellos, tanto dialogando como solicitando la reserva da una habitación, de la sala de juntas o información acerca del hotel.

A. OpenSimulator

OpenSim es un servidor 3D de código abierto que permite crear ambientes virtuales (mundos virtuales) que pueden ser accedidos a través de una gran variedad de visores (clientes) o protocolos (software y web). OpenSim es configurable para suplir sus necesidades y puede ser extendido usando módulos. La licencia de OpenSim es BSD, permitiendole ser de código libre y al mismo tiempo ser usado en proyectos comerciales.

Para la integración de los bots en el mundo virtual ha sido necesario desarrollar un módulo de servidor, de tal manera que OpenSim fuera capaz de acceder al servicio de bots. La aplicación de cliente de OpenSim no ha tenido que ser modificado ya que para dicha aplicación la conversación con un bot no discierne en nada de una conversación con otro usuario pues es el servidor en el que maneja las conversaciones.

B. GSIbot

El servidor de bots GSIbot es una plataforma para el despliegue de servicio de bots conversacionales, que permite desplegar y gestionar, a través de un panel de administración Web, un número ilimitado de bots conversacionales. GSIbot ofrece facilidades para el acceso a los servicios de bots que proporciona, pues presenta diversas interfaces de acceso que permiten a múltiples aplicaciones y servicios de terceros acceder los bots por medio del protocolo HTTP a través de una url, a través de protocolos de mensajería instantánea o por medio de el estándar de comunicación FIPA-ACL utilizado en el sistema multiagente JADE [5].

AIML

Los bots son desarrollados utilizando la tecnología AIML [4]. El lenguaje AIML, acrónimo de Artificial Intelligence Markup Language, es un dialecto de XML específicamente diseñado para crear bots conversacionales. La especificación de AIML no solo describe los elementos del lenguaje sino también el comportamiento de los programas que los procesan. AIML es un lenguaje fácil de aprender que permite ampliar el conocimiento de un bot existente o crear uno desde cero en muy poco tiempo.

El servidor de bots

El servidor de bots es la aplicación principal, que permite desplegar bots con conocimiento expresado en AIML. El sistema se ha desarrollado con tecnología Java Enterprise Edition y se despliega en el contenedor de servlets Apache Tomcat.

El servidor está basado en la plataforma programD como intérprete de AIML. ProgramD es la plataforma de código abierto para bots AIML más utilizada en el mundo. Implementa todas las capacidades de AIML y soporta un número ilimitado de bots. ProgramD es altamente configurable por medio de un conjunto de ficheros de configuración, que permiten activar o desactivar muchas de sus características. Una de las más interesantes es la posibilidad de definir múltiples bots con distintas personalidades, es decir, que contengan el conocimiento de distintos archivos AIML.

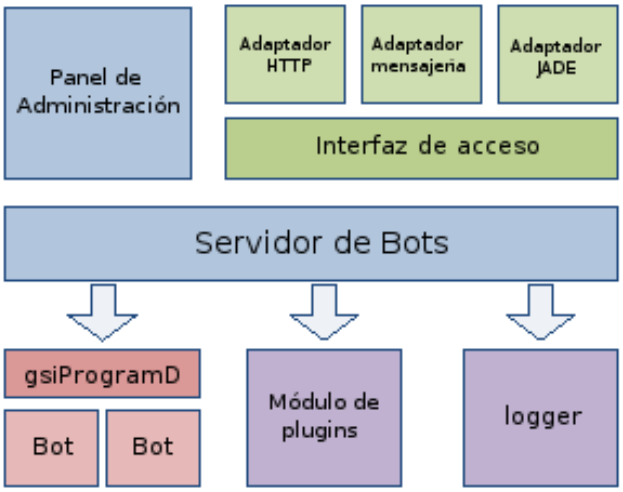


Fig. 2. Arquitectura de Gsibot

Tal y como se muestra en la figura 2, el servidor de bots añade otros módulos y adaptadores a programD con el fin de proporcionar nuevas funcionalidades.

Interfaz Web de acceso

El servidor ofrece una interfaz sencilla para facilitar su integración con los clientes (Web, IM, JADE), según la URI:

```
http://<url-servicio>?q=<consulta>&bot=<id-bot>
[&type=<response-type>]
```

La respuesta ofrecida por el bot no sólo contiene la cadena de respuesta que el bot da a la consulta sino también el valor de todos los parámetros definidos en el AIML para esa respuesta, el nombre del bot, el usuario y la última consulta del usuario.

C. Herramientas para gestión y prueba del corpus

Para programar la base de conocimiento de un bot con capacidad para hablar razonablemente acerca de un determinado tema hace falta una gran cantidad de patrones AIML. En el caso de un bot con el conocimiento equivalente al de un empleado de un hotel, como es el caso de los bots programados para 3DTour hacen falta en torno s 4500 patrones. Realizar esta programación manualmente es un trabajo repetitivo, lento y complicado; pues es necesario escribir patrones con la misma estructura repetidas veces y por ello existe el riesgo de que al añadir un nuevo patrón se esté interfiriendo con uno incuído anteriormente o viceversa.

Para facilitar esta tarea se han diseñado una herramientas de asistencia en el desarrollo de bots escritos en AIML que cubren estás dos dificultades, el corpus tester garantiza que

una base de conocimiento está libre de errores y el gestor de conocimiento permite al usuario trabajar en la base de conocimiento de un bot sin tener conocimientos en AIML.

Corpus Tester

El módulo de pruebas automatizadas, CorpusTester, es una herramienta de mantenimiento y gestión de bases de conocimiento que permite garantizar la calidad integridad de una base de conocimiento o la independencia de dos bases de conocimiento pudiendo así mezclarse archivos de estas sin que interfieran entre sí. Con esto se soluciona el problema existente en AIML con interferencia entre patrones y la agregación de bases de conocimiento.

Es un componente independiente que por medio de la interfaz ofrecida por bot accede a la base de conocimiento para realizar las pruebas. El funcionamiento de las pruebas está basado en un archivo XML, (Knowledge Test File) en el que se recoge el comportamiento deseado de un bot. Este archivo está formado por un conjunto de pruebas (testcase). Cada una de las pruebas está formada por una o más entradas de usuario: las que se envían al bot sucesivamente, y una o más comprobaciones: que se llevan a cabo sobre la respuesta obtenida. Tras ejecutar todas las comprobaciones el programa proporciona un informe detallado con las pruebas que se han realizado y aquellas que no se han superado.

Aplicación de gestión de conocimiento.

La aplicación gestión de conocimiento permite ampliar una base de conocimiento en AIML, hace que el bot aprenda. Éste es un proceso delicado, requiere el uso de algoritmos que garanticen el funcionamiento de los patrones incluidos y a la vez que no interfieran en el conocimiento ya existente. Para ello se basa en el diseño de prioridades entre patrones de AIML para incluir patrones más ajustados al concepto para los que se garantiza que no hay interferencias y otros patrones más ambiguos que pretenden adivinar lo que el usuario quiere decir. Gestión de conocimiento está integrado con corpus tester, de manera que cada modificación en la base de conocimiento es verificada automáticamente a través de la herramienta de pruebas.

Se pueden plantear muchas formas de automatizar la fase de enseñanza al bot. El sistema puede ser más o menos autónomo en función de la cantidad de decisiones que se toman sin consultar al usuario, decisiones de las que –por tanto- el sistema debe estar seguro –o bastante seguro. A medida que la autonomía del sistema aumenta también aumenta la probabilidad de cometer un error y por tanto, crear una entrada en la base de conocimiento que sea incorrecta: al aumentar la autonomía disminuye la fiabilidad.

Se pretende liberar de trabajo al usuario y desarrollar una interfaz intuitiva cuyo uso necesite la menor explicación posible. Para ello se ha alcanzado un compromiso entre autonomía y la fiabilidad desarrollando una interfaz semiautomática o asistida. El sistema toma aquellas decisiones sobre las que posee certeza absoluta. En el resto de casos presenta al usuario las decisiones tomadas y pide su corroboración. En estos casos se traducen las consideraciones propias de AIML a términos fácilmente entendibles por el usuario.

A modo de ejemplo, consideremos que el usuario de la aplicación pretende ampliar la base de conocimiento para que el bot sea capaz de recomendar al usuario qué lugares visitar para hacer turismo. Primeramente el usuario debe introducir

Fig. 3. Ejemplo de mapa de patrones generados

un conjunto de frases que pregunten por ese concepto. A partir de ellas la aplicación deduce cuales son las palabras clave. A partir de las cuales se genera un conjunto de patrones AIML para introducir el conocimiento en el bot. La lógica de patrones AIML responde al mapa mental mostrado en la figura 9. Gracias al diseño de prioridades que sigue AIML el bot siempre escogerá la respuesta más adecuada.

IV. Conclusiones

La integración de bots en mundos virtuales se plantea como una asociación muy positiva para el producto final; los usuarios valoran muy positivamente los sistemas con los que se puede interactuar a través del lenguaje natural para desempeñar una tarea [8].

El proyecto ha concluido satisfactoriamente de manera que se estudia seguir otras vías de trabajo en la integración de tecnología de bots con mundos virtuales; tales como integrar el control del avatar a través del AIML, desarrollar una base de conocimiento con la capacidad de recolectar información del usuario de tal manera que la implementación de un sistema recomendador conectado al servidor que permita a los bots aconsejar a su interlocutor sobre espectáculos y actividades.

Las pruebas realizadas con el prototipo de gestión de conocimiento con usuarios no técnicos han mostrado la facilidad de las herramientas de gestión de diálogos para generar conversaciones sin requerir conocimientos técnicos.

Agradecimientos

El proyecto ha sido llevado a cabo conjuntamente por el Grupo de Sistemas Inteligentes de la Universidad Politécnica de Madrid, Idea Informática empresa del Grupo Gesfor y Skyworks.

Referencias

[1] D. Aimless. Pandorabots - a multilingual chatbot hosting service.
[2] R. Bartle. *Designing Virtual Worlds*. New Riders Games, 2003.
[3] D. J. H. Burden. Deploying embodied ai into virtual worlds. *Know.-Based Syst.*, 22(7):540–544, 2009.
[4] N. Bush. Aiml - the artificial intelligence markup language. http://www.alicebot.org/aiml.html, 2005.
[5] D. G. Fabio Bellifemine, Giovanni Caire. *Programming with JADE - Basic Features*. Michael Wooldridge, Telecom Italia, Italy; Whitestein Technologies AG, Switzerland, 2006.
[6] D. Feng, E. Shaw, J. Kim, and E. Hovy. An intelligent discussion-bot for answering student queries in threaded discussions. In *IUI '06: Proceedings of the 11th international conference on Intelligent user interfaces*, pages 171–177, New York, NY, USA, 2006. ACM.
[7] Y.-S. Kim, T. Kesavadas, and S. M. Paley. The virtual site museum: a multi-purpose, authoritative, and functional virtual heritage resource. *Presence: Teleoper. Virtual Environ.*, 15(3):245–261, 2006.
[8] S. Negi, S. Joshi, A. K. Chalamalla, and L. V. Subramaniam. Automatically extracting dialog models from conversation transcripts. In *ICDM '09: Proceedings of the 2009 Ninth IEEE International Conference on Data Mining*, pages 890–895, Washington, DC, USA, 2009. IEEE Computer Society.
[9] E. Prasolova-Førland. Analyzing place metaphors in 3d educational collaborative virtual environments. *Comput. Hum. Behav.*, 24(2):185–204, 2008.

Pixtream: Sistema de Streaming P2P

Manuel A. Cerón E., Pablo A. Magé I.
Facultad de Ingeniería Electrónica y Telecomunicaciones,
Linea de Investigación en Ingeniería de la Colaboración - Grupo IDIS,
Universidad del Cauca,
ceronman@unicauca.edu.co, pmage@unicauca.edu.co

***Resumen*—El proyecto Pixtream pretende implementar un sistema P2P para realizar *media streaming* con el objetivo de contrarrestar el problema del cuello de botella en el uso de ancho de banda de salida,si presente en los sistemas de *streaming* tradicionales basados en una arquitectura cliente/servidor.**

Para alcanzar este propósito, se seleccionaron y analizaron los trabajos relacionados con el tema de *streaming* P2P que se consideraron más relevantes, con el fin de establecer las características comunes de estos tipos de sistema y reflejarlos en el diseño del protocolo Pixtream, el cual posteriormente fue implementado en un prototipo de software.

El prototipo Pixtream fue probado en un entorno real. Aspectos como la continuidad de la transmición, la latencia y el rendimiento de la red, fueron medidos y comparados con un sistema de *streaming* tradicional y también con los resultados de las simulaciones planteados en los trabajos seleccionados y analizados.

***Palabras Clave*—pixtream, p2p, streaming, bittorrent**

I. Introducción

La tecnología de *media streaming* permite a un cliente recibir audio y vídeo sin necesidad de esperar a que todo el contenido sea descargado. Sin embargo, para que el proceso pueda realizarse en tiempo real, se requiere un ancho de banda considerable, debido a que los archivos multimedia suelen ser muy grandes [1].

Los sistemas de *media streaming* tradicionales utilizan una arquitectura cliente/servidor basada en conexiones *unicast*. En un sistema *unicast*, cada cliente tiene una conexión directa con el servidor. Esto tiene la ventaja de ser fácil de implementar y generar relativamente poca latencia. No obstante, existe una gran desventaja: debido a que se tiene que generar una conexión diferente por cada cliente, el ancho de banda de salida requerido para una sesión de *streaming* crece linealmente con el número de clientes [2]. Esto se traduce en unos costos muy altos a la hora de transmitir contenido a una audiencia grande.

Los sistemas P2P como Bittorrent [3] han probado que pueden solucionar problemas similares encontrados en la transferencia de archivos por Internet. De la misma manera, el uso de este tipo de sistemas para realizar *media streaming*, constituye una buena estrategia para contrarrestar el problema del consumo del ancho de banda.

Durante la última década, varias propuestas de sistemas de *media streaming* P2P se han hecho. Varios autores las han analizado y clasificado de acuerdo con la topología que toma la red superpuesta: Topología de árbol, topología de bosque y topología de malla [4]. No obstante, la mayoría de las propuestas sólo se han planteado a un nivel teórico y sus resultados sólo han sido evaluados a través de simulaciones. Todo esto genera preguntas como ¿Cuál es la propuesta que mejor soluciona el problema del ancho de banda? ¿Qué características de las diferentes propuestas son más importantes para un sistema de *media streaming* P2P? ¿Cómo se compararían los resultados teóricos obtenidos para las propuestas con los resultados prácticos obtenidos por una implementación real?

El objetivo del proyecto Pixtream es desarrollar un sistema P2P para realizar *media streaming* de forma escalable y evitando, en la medida de lo posible, el cuello de botella del ancho de banda en el servidor. Para lograr esto, el proyecto no pretende comenzar desde cero, sino, en cambio, examinar y analizar las propuestas que se han hecho hasta el momento, buscando las características comunes entre todas ellas y cómo ha sido evaluado su rendimiento.

Tomando estos datos como base, Pixtream nace como un prototipo de un sistema P2P que implementa las características comunes más importantes observadas en las propuestas hechas anteriormente.

Una vez teniendo el prototipo de Pixtream implementado, fue posible entonces realizar pruebas en entornos reales para medir sus capacidades y compararlas con un sistema cliente/servidor tradicional y también con los resultados de las simulaciones descritos por los trabajos estudiados y analizados. Esto con el objetivo de determinar qué tan efectivas son estas propuestas más allá del planteamiento teórico y simulado.

II. Bases y antecedentes

A. Trabajos relacionados

El uso de redes P2P para solucionar el problema del uso de ancho de banda en *media streaming* se ha propuesto anteriormente en diferentes formas, tanto en la industria como en la academia [4]. Son varias las propuestas que se han hecho, comenzando desde las más simples como PeerCast [5] y ZigZag [6] que se basan en la idea de construir un árbol *multicast* en la capa de aplicación del modelo OSI, hasta los más elaborados que plantean una topología de malla en la cual los pares crean un enjambre o *swarm* que permite una sesión más escalable y resistente a fallas.

Varios estudios como los realizados por Magharei *et al.* [7], Carra *et al.* [8] y Marfia *et al.* [9] sugieren que las propuestas basadas en topologías de malla presentan un mejor rendimiento y mayor flexibilidad que las propuestas iniciales basadas en árboles *multicast*. Cronológicamente es fácil observar esta tendencia: las propuestas de malla se destacan como aquellas que más se plantean en trabajos recientes. Por esta razón, para el estudio realizado en Pixtream se tomaron 6 propuestas recientes y que usan la topología en malla. Estas propuesta se describen a continuación:

1) Modificaciones a BitTorrent: por Shah *et al.* [10], que propone varias modificaciones al protocolo BitTorrent [3], agregando un sistema de ventana deslizante para compartir sólo un pedazo del flujo multimedia al tiempo y elimina el algoritmo *tit-for-tat* al inicio de la transferencia para acelerar el proceso de creación del enjambre.

2) BEAM: por Purandare *et al.* [11], que propone un sistema de enjambre similar al de BitTorrent pero con el concepto de alianzas entre pares que permitan un intercambio más rápido, evitando latencia en la sesión de *streaming*.

3) AnySee: por Liao *et al.*[12], que propone un sistema de múltiples redes simulataneas en forma de árbol multicast.

4) Gnustream: por Jiang *et al.*, que se basa en el protocolo Gnutella [13], y utiliza varios pares simultáneos para obtener partes del flujo multimedia.

5) PULSE: por Pianese *et al.* [14] que propone una red no estructurada enfocada en agilizar el proceso de *streaming* en redes inestables como Internet.

6) DONet/Coolstreaming: por Zhang *et al.* [15] que no sólo se ha quedado en propuesta sino que ha sido implementado en Roxbeam, un servicio comercial de *media streaming* en China [4]. DONet/Coolstream probablemente sea el sistema de *media streaming* P2P más exitoso construido hasta el momento [9].

III. Diseño e implementación

A. Visión del sistema

El objetivo de Pixtream no es lidiar con todas estas operaciones propias de los contenidos multimedia, como codificación y decodificación, sino que se enfoca exclusivamente en el sistema de transporte que se usa para hacer que el contenido multimedia llegue desde su fuente hasta el espectador. Para lograr esto, olvidándose de las operaciones multimedia complejas, se decidió que Pixtream debería actuar en medio de un sistema tradicional de *streaming* cliente/servidor. Para esto, Pixtream deberá tener componentes que actúen como un cliente multimedia y como un servidor multimedia al mismo tiempo.

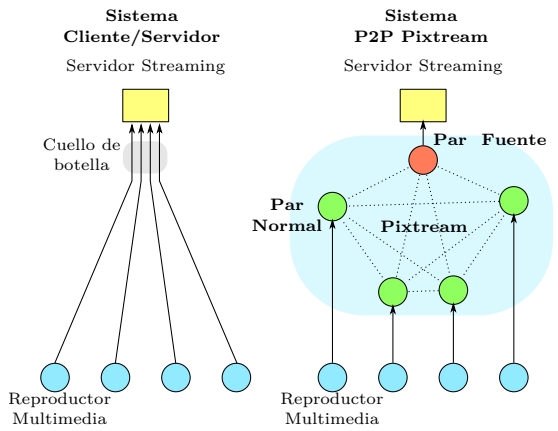


Fig. 1. *Streaming* tradicional frente a *streaming* P2P.

La figura 1 contrasta la forma en la que funcionan un sistema de *media streaming* basado en arquitectura cliente/servidor tradicional y Pixtream. Como se puede observar, Pixtream actúa en el medio del reproductor multimedia y el servidor. El número de conexiones salientes desde el servidor se reduce a una; logrando el objetivo básico de utilizar redes P2P para *media streaming*: reducir el cuello de botella en el uso de ancho de banda en esta parte del sistema.

B. Componentes del sistema

1) Rastreador: El *rastreador* de Pixtream es el componente que sirve de puerta de entrada para los pares en la red. El objetivo principal del *rastreador* es mantener una lista de los pares que están participando de una sesión de *streaming* con Pixtream y darlos a conocer a todo par nuevo que desee ingresar a la red.

2) Par normal: El *par normal* es el componente principal de Pixtream. Lo normal en una sesión de *streaming* es que existan varias instancias de este componente, todas interactuando entre sí. La arquitectura de un *par normal* está formada por tres capas: Conexión, Control e Interfaz.

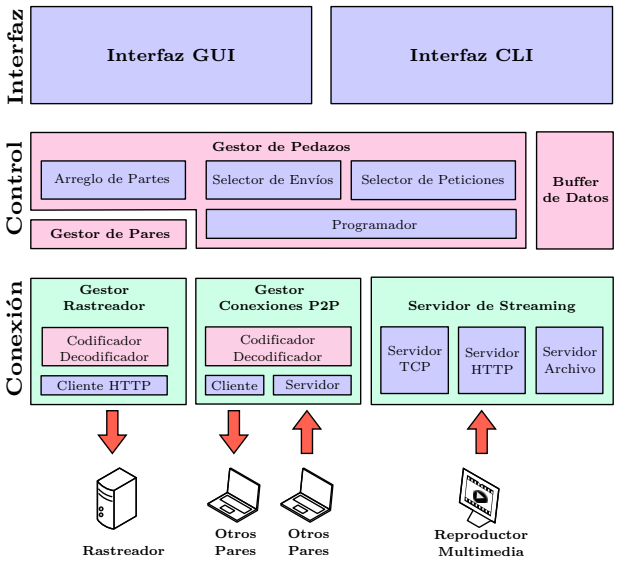


Fig. 2. Arquitectura del par normal de Pixtream

La capa de conexión se encarga de controlar la interacción del par con otras entidades a través de la red. Pixtream es un sistema distribuido complejo y, por lo tanto, existen varias formas de comunicación por red entre procesos y programas independientes. Esta capa tiene tres módulos: El gestor de *rastreador*, el gestor de conexiones P2P y el servidor de *streaming*.

La figura 2, describe la arquitectura de un *par normal* en Pixtream. Las flechas rojas indican las conexiones entrantes o salientes que establece el par y las entidades con las cuales se establecen las conexiones.

3) Par fuente: El *par fuente* funciona como una extensión del *par normal*. Un *par fuente* contiene todos los elementos que un *par normal*, pero con un par de módulos extra: el cliente de *streaming* y el divisor del flujo multimedia.

El cliente de *streaming*, funciona en la capa de conexión y es el componente encargado de recibir el contenido multimedia original. Este componente debe tener la capacidad de conectarse con un servidor de *streaming* tradicional o cualquier otra fuente multimedia. El módulo a su vez está compuesto por varios submódulos, cada uno de los cuales

está diseñado para conectarse al servidor de *streaming* usando diferentes protocolos.

El divisor de flujo multimedia es el componente que toma el contenido recibido por el cliente de *streaming* y lo divide en varios pedazos. Cada pedazo recibe una secuencia y una estampa de tiempo que lo identifica.

C. Protocolo

El protocolo Pixtream contiene todas las reglas y métodos de comunicación usados en un sistema P2P Pixtream. Usando esta especificación de protocolo es posible crear otras implementaciones de Pixtream que sean compatibles.

Esta especificación se divide en dos partes: El protocolo del *rastreador* y el protocolo de la red de pares. El primero describe la comunicación con el *rastreador*, tanto de los pares como de otros servicios. El segundo describe la forma en que se comunican los pares unos con otros.

Desfortunadamente, el espacio en este artículo no es suficiente para describir el protocolo completo.

D. Implementación del prototipo

Utilizando las características seleccionadas de las propuestas estudiadas y el diseño del protocolo creado, se implementó un prototipo de Pixtream con el objetivo de realizar pruebas en un ambiente real. La implementación del prototipo se realizó utilizando el lenguaje de programación Python y el *framework* de sistemas distribuidos Twisted. La implementación se realizó de forma abierta como *software* libre [16] y está disponible en internet en el sitio web del proyecto: http://bitbucket.org/ceronman/pixtream/.

IV. Experimentos

Una vez se tuvo el prototipo implementado y funcionando, se pudieron realizar varios experimentos en los cuales se midieron las capacidades del programa.

A. Parámetros de comportamiento

Con base en los experimentos descritos en las propuestas de sistemas de *media streaming* P2P, se seleccionaron algunas características del comportamiento de Pixtream que deben ser medidos en los experimentos realizados en este proyecto. Al medir estos mismos datos en el comportamiento de Pixtream, es posible después realizar una comparación con los datos que se plantean en los documentos de las propuestas como resultados de las simulaciones. Esto permite realizar un contraste entre las simulaciones y los datos del sistema real.

Los datos que se midieron fueron:

1) Índice de continuidad: Se define por el número de paquetes que llegan a tiempo antes del tiempo límite de la reproducción.

2) Rendimiento de la red: Se refiere a la tasa de transferencia usada durante la sesión de *streaming* con respecto a la capacidad estimada total de los enlaces.

3) Distribución de los recursos en la red: La variación en el uso de ancho de banda en los diferentes nodos de la red. Especialmente se deberá medir el caso del ancho de banda de salida que es el que constituye el cuello de botella en las sesiones de *streaming* tradicionales.

4) Latencia media: Se refiera al tiempo que pasa desde que el contenido multimedia es generado hasta que es reproducido por el cliente final.

5) Tolerancia a fallos: La capacidad que tiene la red para recuperarse de pérdidas de nodos. Esto puede pasar porque las conexiones fallan o simplemente porque los pares se retiran voluntariamente.

B. Escenarios de prueba

Las mediciones se realizaron teniendo en cuenta los siguientes escenarios:

1) Streaming tradicional: En dónde se tomó el caso de un sistema tradicional de *streaming* basado en una arquitectura cliente/servidor. Para este caso se utilizó el sistema VLC[1] en dónde se midió la continuidad de la transmisión y el uso de ancho de banda de salida contrastado con el número de clientes conectados simultáneamente. Este escenario sirve como caso de referencia para comparar el desempeño de un sistema P2P de *streaming*.

2) Escenario estable: En el que se probó el prototipo de Pixtream funcionando en un ambiente en el que todos los nodos entran al mismo tiempo y permanecen conectados a la red de forma estable durante toda la sesión de *streaming*.

3) Escenario inestable: En el que se probó un ambiente en el que algunos nodos se desconectan y re conectan en un intervalo de n segundos. La razón de ser de este escenario es comprobar la flexibilidad de la red frente a errores comunes en una sesión inestable como podría darse en Internet.

C. Resultados

Los resultados de las mediciones realizadas son bastante amplios y se alejan del alcance de este artículo. Sin embargo, vale la pena mencionar aquellos obtenidos en las mediciones más importantes para este estudio como lo son el rendimiento de la red y la continuidad de la sesión de *streaming*.

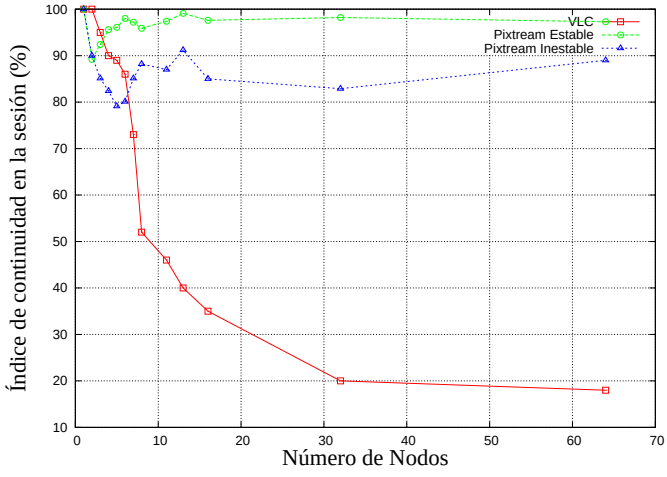


Fig. 3. Comparación de la continuidad en la transmisión entre un sistema de *streaming* tradicional (VLC) y Pixtream

El resultado más importante de los experimentos, es el que ver con la continuidad en el flujo de la transmisión y por consiguiente en la calidad del mismo. El mejor aprovechamiento de los recursos de red da como resultado un mejor índice de continuidad en las sesiones de *streaming*. En la figura 3 se observa como, a diferencia del sistema cliente/servidor, la

[1] VideoLAN Player and Streaming Server: http://www.videolan.org

red P2P conservó un índice de continuidad alto en todas las pruebas realizadas. Algo que vale la pena considerar, es que la continuidad de la transmisión fue mucho mejor en el escenario estable, donde los nodos permanecían conectados durante toda la sesión, que en el escenario inestable. Esto es de especial notoriedad en sesiones con pocos nodos.

También se observa que la efectividad del sistema P2P es mayor cuantos más nodos existen en la red, siendo un sistema cliente/servidor tradicional más efectivo con un menor número de nodos. Esto probablemente debido a la búsqueda de fuentes por parte de los pares.

En comparación con los resultados planteados en simulaciones de otras propuestas, Pixtream obtiene unos resultados, en cuanto a índice de continuidad, ligeramente inferiores a los expuestos por sistemas como PULSE o BEAM. Mientras que estas propuestas señalan un índice de continuidad superior a 98%, Pixtream muestra resultados entre 85% y 98%. Dado que las pruebas en Pixtream fueron realizada en un ambiente real, con trafico adicional externo, pérdida de paquetes y fluctuaciones en la capacidad del enlace de datos, estas diferencias pueden ser explicadas por la diferencia en las condiciones.

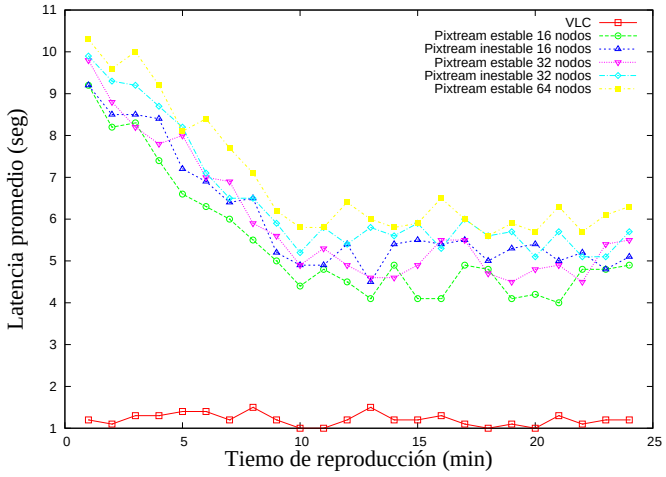


Fig. 4. Comparación de la latencia entre un sistema de *streaming* tradicional (VLC) y Pixtream

Un aspecto en el que claramente el sistema P2P tiene desventaja es en la latencia. En los experimentos realizados, el sistema de control cliente/servidor siempre consiguió una latencia considerablemente más baja que las pruebas realizadas con Pixtream. Esto se debe principalmente a que los datos viajan directamente desde el servidor hasta el cliente, mientras que en una red P2P los paquetes deben ser divididos, distribuidos y reconstruidos. La figura 4 describe los resultados de latencia en diferentes escenarios. Mientras que los resultados de las pruebas en el sistema cliente/servidor muestran una latencia ligeramente superior a un segundo, en Pixtream oscila entre 4 y 10 segundos. Como es natural suponer, las redes Pixtream más grandes presentaron una mayor latencia. Igualmente se puede notar la inestabilidad de los pares como un factor directo que influye en la latencia.

Otro patrón que se puede fácilmente observar en la figura 4 es que la latencia es mayor en las redes Pixtream al inicio de la sesión y tiende a disminuir y a estabilizarse a medida que esta avanza. Esto se puede explicar debido a la influencia de algoritmos como *tit-for-tat* y en la mayor disponibilidad de pedazos del flujo multimedia que puede tener una sesión más madura.

V. Conclusiones

El uso de redes P2P para realizar *media streaming* constituye una solución válida al problema de escalabilidad que tiene los actuales sistemas cliente/servidor. En el proyecto Pixtream se pudo comprobar cómo las características propuestas por varios autores en la academia y la industria son efectivos. No obstante, existen varios problemas que aún debe ser resueltos para lograr un *streaming* de mayor calidad. El punto más importante probablemente sea el de la alta latencia, además de la tolerancia a fallos e inestabilidad en la red.

Además de lo anterior, el proyecto Pixtream también se plantea como una cama de pruebas para introducir nuevos conceptos y algoritmos relacionados con *streaming* P2P a un prototipo de *software* funcional. Dada la naturaleza libre del proyecto, se esperan contribuciones y perfeccionamientos a las técnicas actualmente empleadas, con el objetivo de lograr una mayor calidad de *streaming*.

Referencias

[1] G. Diestro and J. García, "Difusion Multimedia Sobre Internet," *Ampliación en Redes. Universidad de Valladolid*, 2002.
[2] E. Setton and B. Girod, *Peer-to-Peer Video Streaming*. Springer, 2007.
[3] I. Bitorrent, "Sitio Web de Bittorrent." http://www.bittorrent.com/. Sistema de distribución de archivos P2P Bittorrent.
[4] G. Wen, H. Longshe, and F. Qiang, "Recent Advances in Peer-to-Peer Media Streaming Systems," *China Communications*, p. 52, 2006.
[5] H. Deshpande, M. Bawa, and H. Garcia-Molina, "Streaming live media over peers," *Stanford InfoLab*, 2002.
[6] D. A. Tran, K. A. Hua, and T. Do, "ZIGZAG: an efficient peer-to-peer scheme for media streaming," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 2, 2002.
[7] N. Magharei and R. Rejaie, "Understanding mesh-based peer-to-peer streaming," *Proceedings of the 2006 international workshop on Network and operating systems support for digital audio and video*, 2006.
[8] D. Carra, R. L. Cigno, and E. W. Biersack, "Graph Based Analysis of Mesh Overlay Streaming Systems," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 9, pp. 1667–1677, 2007.
[9] G. Marfia, G. Pau, P. Di Rico, and M. Gerla, "P2P Streaming Systems: A Survey and Experiments," *STreaming Day 2007*, 2007.
[10] P. Shah and J. F. Pâris, "Peer-to-Peer Multimedia Streaming Using BitTorrent," pp. 340–347, 2006.
[11] D. Purandare and R. Guha, "BEAM: An Efficient Peer to Peer Media Streaming Framework," *Proceedings 2006 31st IEEE Conference on Local Computer Networks*, pp. 513–514, 2006.
[12] L. Xiaofei, J. Hai, L. Yunhao, *et al.*, "AnySee: Peer-to-Peer live streaming," *Barcelona, Spain: Proceedings of IEEE INFO-COM*, 2006.
[13] M. Ripeanu, "Peer-to-Peer Architecture Case Study: Gnutella Network," vol. 101, 2001.
[14] F. Pianese, J. Keller, and E. W. Biersack, "PULSE, a Flexible P2P Live Streaming System," 2006.
[15] X. Zhang, J. Liu, B. Li, and T. S. P. Yum, "CoolStreaming/DONet: A Data-Driven Overlay Network for Efficient Live Media Streaming," vol. 3, pp. 13–17, 2005.
[16] R. M. Stallman, *Free Software, Free Society: Selected Essays of Richard M. Stallman*. O'Reilly Media, Inc., 2002.

Presence Service for Wireless Sensor Networks: Research and Open Issues

Ernesto García Davis, Anna Calveras Augé
Department of Telematic Engineering
Universitat Politècnica de Catalunya (UPC)

C. Jordi Girona, 31. 08034 Barcelona.

ernesto.garcia@entel.upc.edu, anna.calveras@entel.upc.edu

Abstract – A presence service allows knowing the availability or responsiveness status of entity we want to engage to a communication. Traditionally, only human have made use of this service, however all smart devices could interact with each other thus a presence service could also enhance communication among these devices such as sensor nodes. To achieve this objective we evaluate existing protocols to propose the requirements needed to provide presence service on WSN. Finally, in this paper we present a first approach to cope with presence services in WSN based on publish/subscribe mechanisms.

Keywords- Presence Service, wireless sensor networks, publish-subscribe mechanisms

I. INTRODUCTION

WSN (Wireless Sensor Networks) generally have been deployed for measure and detect physical or environment events like: temperature, pressure, humidity, brightness, velocity, etc. However, the WSN are leaving to be simple networks for data collection to become networks with certain autonomy and intelligence which can take decisions in case of any event occurs.

For instance, a new concept of HAN[1] (Home Area Network) consists on smart appliances (HAN devices), typically a white good or other household appliance, that are capable of receiving messages from the Utility(service provider) and adjusting its operational mode based on Consumer preferences (e.g., energy saving mode, delayed turn on/off). These messages may be used for a variety of purposes from facilitating reduction in energy consumption during peak times, saving consumer's money, to facilitating energy consumption patterns that are more environmentally friendly. This would mean the Utility should have information on whether you are using your computer or not, and if, for example, you simply have a screen saver on while you work around the house. In this case the Utility (in this case electric company) could decide based on your preference turn it off for you.

We consider for the case above mentioned a presence service could enhance communications between HAN devices and Utility equipment. Each HAN device will subscribe its presence to Utility equipment. Utility will check state of presence of HAN devices before to transmit a command. In this manner, only HAN devices with availability status will receive a command, thus Utility only will transmit necessary messages to network. In addition, Presence Service will be useful to group different type of devices.

For this type of application aforementioned, the presence awareness of people or resources is critical in order to determine the proper way or time to transmit a command to entity. Therefore, a pre-knowledge of the corresponding entity's presence can improve the situation because application only will transmit messages to devices accordingly to their status.

The motivation for the work presented in this paper is based on the above observations that an efficient communication among entities is possible if we know entity's (objects or human) presence information. Hence, we would need a presence service to interact among different type of entities such as: human-to-objects, objects-to-human, and objects-to-objects. And these objects could be any entity providing some resources, such as sensor nodes provide temperature, humidity, and light data.

Nowadays, as far as we know there is not a protocol or mechanism providing presence service in WSN. However, we can make use of protocols in WSN based on Publish-Subscribe communication model taking into account that presence service in general is based on this model.

The remainder of this paper is organized as follows: in section II, we provide the background about presence service. In section III we evaluate the feasibility of Internet standard technologies providing presence service on WSN. The Publish-Subscribe Communication model and its benefits for WSN are explained in section IV. In section V we evaluate Publish-Subscribe Protocols on WSN and the useful features to implement presence service on WSN. We end this paper summarizing publish-subscribe protocols presented throughout the paper and give directions and motivation for future research.

II. BACKGROUND ON PRESENCE SERVICE

Presence, at a simple level, refers to the availability status, willingness or responsiveness of an entity (human or object), to engage a communication. This information called presence information, allows application to take intelligent decisions about the management of communication.

The most common example for presence is Instant Messaging System (IM) [2]. Currently, an IM user can keep a roster of contacts (buddies) which is displayed on the user's device upon logon.

Whereas the presence concept has been regarded to human-to-human communication, it is no longer the unique privilege of human users to initiate a conversation; rather all smart devices could interact with each other or address a human user by their own initiation. Therefore, the concept of presence also applies to describe the availability status of ubiquitous resources (objects).

The most common option to implement presence service on WSN should be making use of existing standard protocols on Internet providing this service. Hence the next section presents existing technologies providing presence service and its impact on using them on WSN.

III. EVALUATION OF PRESENCE SERVICE TECHNOLOGIES

This section evaluates the most extended standard existing on Internet, mainly focusing our attention to the fact that should be used over wireless environments and resources-constrained devices such as sensor nodes.

Currently, there are two open Internet Engineering Task Force (IETF) standards in order to provide presence service on Internet: SIP/SIMPLE (Session Initiation Protocol/Session Initiation Protocol for Instant Messaging and Presence Leveraging)[3] and XMPP (eXtensible Messaging and Presence Protocol) [4].

SIP/SIMPLE and XMPP are designed to provide a standard for Instant Messaging on fixed networks and, lately have been used for mobile networks.

We compare these two protocols, considering their ability to adapt to wireless environments, the size of its messages and its energy efficiency, all of them requirements in WSN.

With reference to wireless environment adaptation, SIP/SIMPLE can use TCP (Transport Control Protocol) or UDP (User Datagram protocol) as transport protocol. The ability to use UDP is a great benefit on such environments because is lighter and faster than TCP because UDP does not recover for errors and does not guarantee delivery. However, UDP is not the solution for every situation; we have to consider the requirements of applications. For instance, in some critical reliability scenarios it would be more preferable to guarantee delivery of a message than to increase the speed of message transmission.

Unlike SIP/SIMPLE, XMPP works only over TCP. Therefore the considerable header overhead, connection management, end-to-end flow and congestion control lead to TCP poor performance on wireless environment and resource constrained nodes, such as WSN [5].

Regarding size of message used for both protocols, SIP/SIMPLE is based on request/response model with text messages. Each message contains ASCII strings and allocates one byte for each character and that results in long messages to fit into the size of the message of sensor nodes[1].

On the other hand, XMPP is a protocol based on XML (eXtensible Markup Language) that makes it quite chatty to transmit and requires some computation capacity to parse and interpret messages than could be complex in resources-constrained devices, such as sensor nodes[7].

Regarding energy efficiency, transmitting and receiving data consumes energy proportionally to the size of the message. Hence the large size of the messages both SIP/SIMPLE and XMPP are not suitable for sensor nodes generally working with a limited energy resources (batteries).

On the other hand, in general, presence service on Internet has certain limitations to be used on WSN such as:

- Limited vocabulary to express presence information: A simple status of presence information (such as: offline, busy, away) is not enough to decide how to establish a communication with an entity. Besides regarding interaction with objects there is a need to enrich vocabulary. This could be accomplished using context information that sensor nodes can collect.
- The presence status is generally updated manually: There is not a way to deduce automatically presence status of a user. Some presence technologies can change presence information status to "away" taking into account there is not activity from the user in the device during some period of time. In the case of sensor nodes, should be necessary that they change their status without user interaction.

Considering the issues evaluated in this section, we realize that existing protocols for presence service could not be implemented directly in the WSN because they do not consider aspects which are specific characteristics of this type of networks, such as: energy efficiency, and optimization of communication. However, both standards protocols (SIP/SIMPLE and XMPP) use the publish/subscribe communication model, which also use certain protocols in WSN not intended for presence services on WSN.

In the next section, we describe the Publish-Subscribe Communication Model and its benefits for WSN taking into account that we can use these mechanisms to provide presence services on WSN.

IV. PUBLISH-SUBSCRIBE COMMUNICATION MODEL

This communication model[6] consists in entities called subscribers that register their interest in an event produced by other entities called publishers. This process of registering an interest is called subscription.

Additionally, this communication model employs a central brokerage station called broker, which receives the

[1] We assume a maximum payload size of 127 bytes at the lower layer (IEEE 802.15.4)

information of every subscription and publication of every event. The broker is also responsible to notify a subscriber if an event match occurs with its subscription.

There are some challenges for application development on WSN that could be solved applying the Publish-Subscribe communication model.

For instance, in application for real time monitoring purposes (fire detection or security surveillance) we need to know for future events and in the instant it has occurred. Generally, applications submitted queries to sensor nodes each certain interval of time, however this scheme is useless in this case because we would only obtain past events and maybe no change has occurred in this interval of time.

If we apply publish-subscribe communication model, we can submit a query to the network in advance waiting for notification of the events that match the query in the future. In this case, the sensor nodes submitting the query are called subscriber nodes and sensor nodes that notify event have occurred are called publisher nodes.

The presence service architecture fits into publish-subscribe communication model. This architecture works as follows (Fig. 1): the presence entities called presentities provide their presence information to the presence service. The presence service accepts, stores, and distributes the presence information to everyone subscribed to get the notification about presence changes. The users receiving notification about presence information are called watchers.

Presentities and watchers communicate by exchanging presence events. Presentities are publishers in publish-subscribe communication model and watchers are subscribers that are interested in presence event.

It should be noted that presence service makes use of topic based publish/subscribe communication model [6], because the watchers need to know every changes in presence information of presentities.

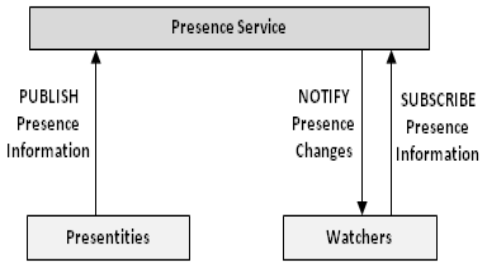


Fig. 1. Presence Service Architecture

In the next section we briefly present publish/subscribe protocols already known in the area of sensor networks, with a focus on the most important design points that we could consider important to implement a presence service on WSN.

V. EVALUATION OF PUBLISH/SUBSCRIBE PROTOCOLS ON WSN

Several authors have proposed protocols making use of publish/subscribe communication model such as MQTT-S [8], MIRES [9] and TinySIP [10], in order to solve problems mentioned in section above for application development on WSN.

A. MQTT-S

MQTT-S (Message Queuing Telemetry Transport for Sensor Networks) is an extension of MQTT [11] originally developed for telemetry applications using constrained devices.

It is based on centralized architecture where a broker node is placed in the backbone network to provide publish/subscribe service to the nodes in this part of the network and in the WSN. MQTT-S provides sleeping nodes support incorporating a mechanism by means clients indicate the time they will be inactive at Broker, and therefore it will buffer messages destined to them for later delivery when they wake up. MQTT-S defines three QoS levels. QoS level 0 offers a best effort delivery service and no retransmission or acknowledgment is defined. QoS level 1 allows the retransmission of messages until they are acknowledged by the receivers; however certain messages may arrive multiple times at the destination because of the retransmissions. The QoS level 2, ensures not only the reception of the messages, but also that they are delivered only once to the destination.

In addition, this protocol considers the size of message to be no longer than 64 bytes of the payload of an 802.15.4 packet (127 bytes) because the remaining 64 bytes should be used by the overhead information required by supporting functions such as MAC layer, networking, security, etc.

B. MIRES

MIRES (Message-Oriented Middleware for Sensor Networks) comprise three components. The first one, unlike MQTT-S, is a content based publish/subscribe service. This service is responsible for advertising and maintaining the topics provided by node application, and publishing messages containing data related to the advertised topics.

The second component is a multi-hop routing algorithm to forward in order to transmit either locally generated or forwarded messages received from the network towards the sink node. In this sense, an advantage of MIRES is the utilization of any multi-hop routing algorithm.

Finally, the third component allows providing additional services such as: in-network aggregation services. Aggregation service occurs inside WSN, hence it reduces messages traffic to sink node.

In MIRES, each sensor node announces its sensor capabilities (temperature, light, etc) to sink node as a topic available to publish. Then, user through application interface subscribes interested topics. User can subscribe for desired policies and aggregation function for event.

Then, MIRES Publish/Subscribe service disseminates through a broadcast message the configuration of the user to the other nodes in the network.

C. TinySIP

TinySIP (Tiny Session Initiation Protocol) is based on SIP protocol. It incorporates a messaging mechanism for accessing sensor-based services. It provides a communication abstraction which allows session

signalling publish/subscribe services and instant messaging features.

Basically, this protocol is based on centralized architecture where a SIP-TinySIP Gateway(s) situated on the edge of WSN and all of communication between clients on outsider networks and WSN nodes is through a SIP-TinySIP Gateway(s).

TinySIP message can be transmitted within as smaller payload, such as the 29-byte of a regular TinyOs payload message.

In addition, we compare the features of these protocols that can be useful for presence service on WSN such as: topic composition, sleeping nodes support, reliability and messaging format.

About topic composition, MQTT-S allows subscribing to one topic and receiving information of several nodes by means of the use of "wildcard". For example, if we have interest in obtaining all data of temperature located at the first floor of a building we should subscribe us to the following topic: "sensors/floor1/+/temperature". This form to operate allows that only it must transmit a message SUBSCRIBE, resulting in an energy saving for the sensors nodes. However with MQTT-S we will not receive aggregated data, but temperature data of each sensor node related with the topic. If we apply this situation to TinySIP, it will require to send a SUBSCRIBE message for each temperature sensor located in the location of interest result in increasing of message traffic. In contrast with previously protocols, MIRES allows define data aggregation function about the information we want to receive of the topic so in the example described above we only will receive one message with the averaged temperature of floor 1.

Regarding sleeping nodes support the presence service could take advantage of this feature provided by MQTT-S in order to buffer messages destined to sensor nodes in sleep mode and delivered later to them when they wake up. In contrast, TinySIP and MIRES do not take into account this particularity from the nodes from WSN, resulting in lost messages that are sent to the nodes that are inactive.

With reference to reliability, the QoS levels 1 and 2 defined by MQTT-S could provide to the presence service of the reliability needed to guarantee the delivery of presence information to subscriber nodes. Therefore, it will allow to subscriber nodes always taking better decision for the communication management. Either TinySIP or MIRES specify any reliability mechanism.

Finally, regarding messaging format, the compact message size used by TinySIP should be more appropriate than used by MQTT-S because involves less consume of energy in the packet transmission. In the case of MIRES, it does not specify the size of the message used.

VI. DISCUSSION AND CONCLUSIONS

In this paper we have focused on publish/subscribe protocols for WSN in order to provide presence service in this type of networks.

There are important issues to mark respect to protocols we have evaluated in this paper. These protocols consider a communication between sensor nodes and external users or vice versa. However, applications mentioned on introduction of this paper and future trends such as "Internet of Things" consider objects can interact among them, thus publish-subscribe protocols should consider publisher nodes not always will send information to the sink as the only destination.

In addition, publish/subscribe communication model employs a centralized broker node generally placed on WSN in the sink node. However if subscriber node and publisher node are placed closer would fall into a waste of extra energy forward the message to the sink node and then forward to subscriber node.

Finally, both MQTT-S and TinySIP do not consider in-network aggregation techniques. However, as we mentioned previously, in-network data aggregation is a well known and essential technique to achieve energy efficiency when propagating data from sensor nodes through reduction of the amount of messages transmitted and to long the lifetime of the WSN.

VII. FUTURE WORK

Our next goal is evaluate the impact of broker node location in the WSN. We consider implementing three scenarios in the following way: the broker acting as sink node, a broker serving for a group of nodes, and a sensor node acting as a broker/publisher.

ACKNOWLEDGMENTS

This research has been funded by The Professional Excellence Program IFARHU-SENACYT-Panama and CICYT-TEC2009-11453.

REFERENCES

[1] Home Area Network Overview. http://www.edisonfoundation.net/iee/issueBriefs/PG&E_HAN_January_2009.pdf

[2] A Model for Presence and Instant Messaging (RFC2778). The Internet Society. February 2000.

[3] A Presence Event Package for the Session Initiation Protocol (SIP) (RFC 3856). The Internet Society. August 2004.

[4] Extensible Messaging and Presence Protocol (XMPP): core (RFC 3920) The Internet Society, October 2004.

[5] Kuorilehto, M., et alt. Experimenting TCP/IP For Low-Power Wireless Sensor Networks. The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06).Sept. 11-14 2006. pp 1-6.

[6] Tran, Duc A., Truong, Linh H. Publish/Subscribe Techniques for Sensor Networks. May 2009.

[7] "IEEE Std 802.15.4-2003", IEEE 802.15 WPANTM Task Group 4, 2003, http://www.ieee802.org/15/pub/TG4.html

[8] Hunkeler, U., et alt. MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks. COMSWARE 2008. 3rd International Conference on Communication Systems Software and Middleware and Workshops. Jan 2008. pp 791-798.

[9] Souto, E., et alt. Mires: a publish/subscribe middleware for sensor networks. Personal and Ubiquitous Computing. Vol. 10, Feb 2006. 1617-4917 (Online).

[10] Krishnamurthy, S. TinySIP: Providing Seamless Access to Sensor-based Services. 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, July 2006. 0-7803-9791-6.

[11] MQTT, http://mqtt.org

Propuesta para el soporte de movilidad IP en redes de acceso MPLS

Javier Carmona-Murillo, José-Luis González-Sánchez, Francisco J. Rodríguez-Pérez, David Cortés-Polo
Departamento de Ingeniería de Sistemas Informáticos y Telemáticos.
Universidad de Extremadura.
Laboratorio GÍTACA, Escuela Politécnica de Cáceres.
Av. Universidad s/n. 10.003, Cáceres.
jcarmur@unex.es, jlgs@unex.es, fjrodri@unex.es, dcorpol@unex.es

***Resumen*- Las redes de comunicaciones móviles de próxima generación plantean nuevos objetivos más allá de ofrecer un servicio sin interrupciones al usuario durante su movimiento. La provisión de calidad de servicio (*Quality of Service*, QoS) es un objetivo a lograr a fin de evitar una degradación del servicio en la conexión del terminal móvil al cambiar su ubicación en la red. La integración de Mobile IP y *Multi-Protocol Label Switching* (MPLS) ha despertado especial interés en los últimos años. Mobile IP es el protocolo de referencia en la gestión de movilidad mientras que las capacidades de fiabilidad y de ingeniería de tráfico de MPLS hacen que sea una buena opción para proporcionar QoS en los escenarios dinámicos que plantean las tecnologías de comunicaciones móviles. En este artículo presentamos una arquitectura de gestión de la movilidad en redes de acceso MPLS que permite reencaminar el túnel LSP en función del movimiento del usuario reduciendo los costes de señalización y proporcionando una baja latencia en el *handover*.**

***Palabras Clave*- Mobile IPv6, Multi-Protocol Label Switching (MPLS), QoS, recuperación de paquetes, análisis del rendimiento.**

I. INTRODUCCIÓN

Las redes inalámbricas son una de las tecnologías de comunicaciones más demandadas en la actualidad. En el diseño de estos sistemas de próxima generación, dos objetivos sobresalen por encima del resto. En primer lugar, mantener la conectividad durante el movimiento de los usuarios entre redes heterogéneas. En segundo lugar, ofrecer a los nodos móviles un nivel de calidad de servicio similar mientras van moviéndose de una red a otra. Para el primero de los objetivos, Mobile IPv6 [1] es el protocolo que se está desarrollando con más fuerza, aunque tiene algunas limitaciones como la alta latencia en el proceso de *handover* o la pérdida de paquetes durante la interrupción del servicio en cada uno de los movimientos que realiza el usuario.

Por otra parte y con respecto al segundo de los retos, es necesario que durante los movimientos de los nodos móviles, éstos reciban una calidad de servicio similar para que el usuario no perciba una degradación en el servicio que está recibiendo [2]. La provisión de QoS en la red visitada requiere de mecanismos de ingeniería de tráfico que permitan que haya una correspondencia entre los atributos específicos de QoS de una red y otra [3].

En este trabajo, proponemos el funcionamiento conjunto del protocolo Mobile IPv6 y MPLS [4]. Realizamos un repaso de los principales trabajos relacionados con el soporte de la calidad de servicio en redes Mobile IP-MPLS y proponemos una arquitectura denominada *LinkWork Mobile MPLS* capaz de reencaminar túneles MPLS cuando se producen movimientos de los usuarios, así como minimizar las pérdidas de forma que se mejore la provisión de QoS. El análisis del comportamiento de este esquema es comparado con otras propuestas que tienen objetivos similares como Mobile IP, Mobile MPLS [5] y FH-Micro Mobile MPLS [6].

El resto del artículo está organizado de la siguiente forma. En la sección II se trata el estado del arte de las tecnologías involucradas en este trabajo. El apartado III presenta nuestra arquitectura de movilidad. En la sección IV planteamos un modelo con el que analizar el comportamiento de los mecanismos propuestos. Finalmente, el apartado V presenta las conclusiones de este trabajo y establece nuevas líneas de trabajo a realizar en el futuro.

II. TRABAJO RELACIONADO

A. Mobile IPv6

En los últimos años, el IETF ha desarrollado Mobile IP como el protocolo de referencia para el soporte de movilidad en Internet. Mobile IPv6 introduce nuevos términos y entidades funcionales que se observan en la Fig. 1 y que se describen a continuación.

El nodo móvil (*Mobile Node*, MN) mantiene una conexión con el CN (*Correspondent Node*) a través de un túnel entre un agente denominado HA (*Home Agent*) y el propio MN. El HA se encarga de interceptar y y de hacer llegar al MN la información dirigida a él durante su movimiento y se encuentra en la red origen (*Home Network*, HN) que es aquella desde donde parte el nodo móvil y cuyo prefijo coincide con el de la dirección permanente (*Home Address*, HoA) del nodo. Cuando el MN se mueve a otra red, obtiene una dirección IP auxiliar (*Care-of Address*, CoA).

Fig. 1. Entidades básicas en Mobile IPv6

B. Mobile IPv6 y MPLS

Recientemente, el interés por utilizar MPLS junto con Mobile IP se basa en las posibilidades que puede ofrecer MPLS a la hora de reservar recursos, utilizar mecanismos de ingeniería de tráfico y permitir un *handover* más rápido [2]. Concretamente, en [5] se propone un esquema para integrar Mobile IP y MPLS, que se ha mejorado en varias ocasiones [7], [8] para solventar algunas de sus limitaciones. De entre el resto de propuestas, cabe destacar Fast Handoff Micro Mobile MPLS [9], que se centra en la gestión de la movilidad dentro de un dominio MPLS. En este artículo proponemos una arquitectura de gestión de la movilidad para redes de acceso MPLS, llamada *LinkWork Mobile MPLS*.

III. Arquitectura Propuesta

A. Funcionamiento de LinkWork Mobile MPLS

Una de las ideas en las que se basa esta arquitectura es la anticipación del movimiento de nivel 3 utilizando funcionalidades de nivel 2, así como la definición de ciertos nodos del dominio MPLS, llamados nodos articulados (NA), que disponen de características especiales, como la capacidad de reencaminar el LSP hacia un nuevo ELER cuando se produce un movimiento o ser el elemento principal del mecanismo de recuperación que se activa durante el proceso de *handover*.

El funcionamiento básico del mecanismo se describe a continuación (Fig. 2). Inicialmente consideramos que el MN se encuentra en una subred a la que da servicio el *router* PELER (Previous Egress LER) y que existe un túnel LSP activo entre el ILER (Ingress LER) y el PELER a través del cual se envían los datos al MN. Cuando el MN entra en una red vecina, recibe mensajes de notificación de L2 de una estación base de dicha subred (paso 1). Tras recibir esta señal, el MN notifica al nodo PELER que puede producirse un *handover*, enviándole un mensaje en el que aparece la MAC del ELER en la que está entrando el MN. Utilizaremos esta dirección MAC para obtener la IP de dicho ELER (paso 2). Estos 2 pasos del mecanismo LW, son similares al propuesto en FH-Micro Mobile MPLS [6]. Una vez que el PELER conoce la IP del NELER, informa al NA del posible *handover* para que comience la señalización de una nueva sección del túnel desde dicho NA al NELER (paso 3).

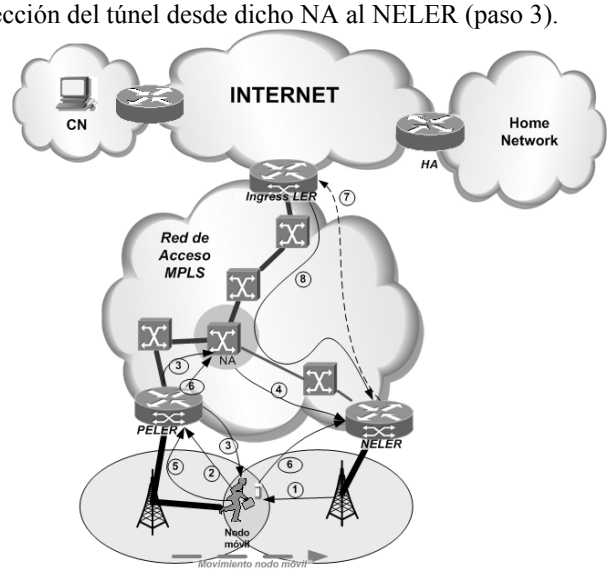


Fig. 2. Funcionamiento de LinkWork Mobile MPLS

En este momento ya se podría crear una nueva sección del túnel LSP entre el NA y el NELER, de forma que permita reencaminar el tráfico hacia la nueva ubicación del usuario móvil (paso 4). Cuando la señal de la red baja por debajo de un nivel determinado, el MN le indica al PELER que va a cambiar de red mediante un mensaje de señalización del movimiento. Se activa el mecanismo de recuperación y se produce el *handover* de nivel 2 (paso 5). Este mecanismo de recuperación tiene como objetivo minimizar las pérdidas de paquetes que se encuentran entre el NA y el MN.

Una vez que el *handover* de nivel 2 se ha completado, comienza el *handover* de nivel 3 con el registro del MN en la nueva red utilizando para ello el registro especificado por MIPv6 (paso 6). La nueva sección del túnel LSP comenzará a utilizarse cuando el NA sea consciente de que la antigua ruta no está disponible. Esto se produce cuando el PELER comienza a devolver los paquetes de datos de vuelta al NA, según se establece en el mecanismo de minimización de pérdidas, tal y como se detallará más adelante.

Por último, el NELER envía la solicitud de registro (*Binding Update, BU*) de Mobile IP al ILER (paso 7). El ILER utilizará el mismo túnel que tenía establecido, ya que será el NA el que se encargue de reencaminar el tráfico hacia la nueva ubicación del MN.

B. Mecanismo de recupueración

El mecanismo aquí explicado se basa en [10] y funciona de la siguiente forma. Una vez que se detecta la situación de problemas en la red, provocada por un inminente movimiento del MN, los paquetes que normalmente se enviarían al MN son devueltos al nodo responsable de la recuperación, en este caso el NA. La novedad de este mecanismo, frente a otros como *Fast Recovery* es que el paquete inicial que envía el PELER al NA y que indica que existe un problema en la red es aceptado por el NA. El nodo articulado marca, con una señal concreta, el siguiente paquete que debe enviarse al MN y lo envía por el camino que tiene problemas. El resto de paquetes del mismo flujo que van llegando al NA no se enviarán, sino que se almacenan en un *buffer* del propio NA mientras va recibiendo los paquetes que el PELER le devuelve y que estaban en vuelo cuando se produjo el movimiento del nodo móvil. Así, irán llegando estos paquetes, que son reenviados por el nuevo LSP establecido hacia el NELER. Esto continúa hasta que se recibe el mensaje que marcó el NA con una señal concreta, lo que significa que todos los mensajes en vuelo han sido recuperados y reenviados por el nuevo LSP hasta el NELER. Entonces, los mensajes almacenados se envían también hacia su nuevo destino. La ventaja de esta propuesta frente a otras similares es que los paquetes se envían al nuevo destino de forma ordenada. En la figura 3 se muestra un ejemplo de este mecanismo.

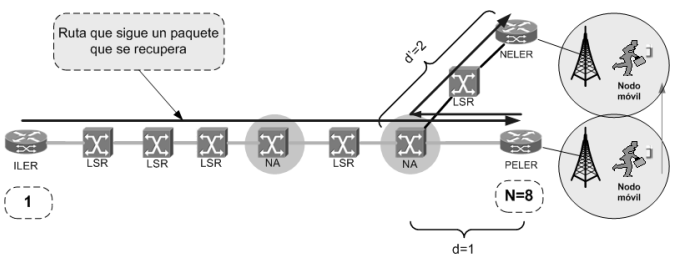


Fig. 3. Funcionamiento del mecanismo de recuperación.

Partiendo del algoritmo de Dijkstra de cálculo de la ruta del mínimo coste, podemos analizar este mecanismo de forma independiente. Consideramos un dominio MPLS como el que podemos tener en la arquitectura LW Mobile MPLS. Este dominio queda definido de la forma $G(U)$, con un conjunto X de n nodos y un conjunto U de enlaces. Sea δ_{ij} el retardo del enlace $(x_i, x_j) \in U$ y sea $\delta(x_i, x_j)$ el retardo de una ruta entre los nodos x_i y x_j que pueden no ser vecinos. El objetivo se centra en analizar el retardo consumido por los paquetes cuando se retransmiten entre dos nodos cualesquiera del *LSP* de *U(G)*, es decir:

$$min\ \delta(x_i, x_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} \delta_{ij}\, x_{ij}\ , \tag{1}$$

sujeto a las siguientes restricciones:

$$\sum_{l=2}^{n} x_{1l} = 1 \tag{2}$$

$$\sum_{i=1}^{n} x_{il} - \sum_{j=1}^{n} x_{lj} = 0,\ l = 2,3,...,n-1 \tag{3}$$

$$\sum_{l=1}^{n-1} x_{ln} = 1\,, \tag{4}$$

donde, $\delta_{i,i} = 0,\ \forall\ i \in N\ ; x_{i,j} = 1,\ \forall (x_i, x_j) \in LSP$ y $x_{i,j} = 0,\ \forall (x_i, x_j) \notin LSP$

Según este modelo, podemos determinar el coste que supone la recuperación de un paquete implicado en este mecanismo. A este coste temporal lo denominamos T_{rA}, y vendrá dado por (5):

$$T_{rA} = \sum_{i=1}^{n-1} \delta_{(i,i+1)} \cdot x_{(i,i+1)} + \sum_{i=n-d}^{n-1} \delta_{(i,i+1)} \cdot x_{(i,i+1)} + \sum_{i=n-d}^{n-d+d'-1} \delta_{(i,i+1)} \cdot x_{(i,i+1)} \tag{5}$$

En esta expresión, el primer sumando es el coste del camino entre el ILER y el PELER, mientras que el segundo es el coste para recorrer el camino de vuelta desde el PELER al NA y el tercero es el coste que supone transportar el paquete por el nuevo segmento del túnel LSP entre el nodo articulado y el NELER en el que se encuentra el nodo móvil tras el movimiento.

IV. Modelado del Sistema

En este apartado analizamos varias medidas que definen el comportamiento de la arquitectura de movilidad propuesta, evaluando el coste de señalización y el rendimiento del *handover*.

Comparamos nuestra propuesta con otros trabajos que tienen un objetivo similar como Mobile IP, Mobile MPLS y FH-Micro Mobile MPLS. Para simplicidad del estudio analítico, asumimos que cada subred está a igual distancia δ (en término de número de saltos) del ILER. Del mismo modo, no consideramos el coste que supone el proceso periódico de actualización de vínculo (*binding update*) entre el MN y el HA para actualizar su caché, tal y como se indica en [9]. Modelamos el comportamiento de la movilidad del MN teniendo en cuenta un escenario de en el que el terminal se puede mover a cualquiera de sus redes vecinas con igual probabilidad. Los parámetros que se utilizarán en el análisis aparecen a continuación.

- T_s Tiempo medio de conexión para una sesión.
- T_r Tiempo medio de permanencia en una red visitada.
- T_{ad} Intervalo de tiempo con la que un agente en la red visitada envía mensajes *Agent Advertisements*.
- N_h Número medio de *handover* de nivel 3 durante una sesión ($N_h = t_s/t_r$)
- N_g Número de vecinos restantes no notificados del nuevo LER cuando existe un handover.
- S_u Tamaño medio de un mensaje de señalización para la actualización de registro.
- S_l Tamaño medio de un mensaje para el establecimiento de un LSP.
- $h_{x\text{-}y}$ Número medio de saltos entre *x* e *y* en la red fija.
- B_w Ancho de banda del enlace fijo.
- B_{wl} Ancho de banda del enlace inalámbrico.
- L_w Latencia del enlace fijo (retardo de propagación).
- L_{wl} Latencia del enlace inalámbrico (retardo de propagación).
- P_t Búsqueda en la tabla de etiquetas o de encaminamiento y tiempo de procesamiento.
- λ_d Ratio de transmisión de un paquete *downlink*.
- T_{inter} Tiempo entre la llegada de los paquetes de datos.

Por otra parte, $t\ (s,h_{x\text{-}y})$ es el tiempo que tarda un mensaje de tamaño *s* en ser enviado desde *x* a *y* a través de los enlaces fijos e inalámbricos correspondientes. $t(s,_{hx\text{-}y})$ puede expresarse de la forma:

$$t(s,h_{x-y}) = c + h_{x-y} \cdot \left(\frac{s}{B_w} + L_w\right) + (h_{x-y}+1) \cdot P_t \tag{9}$$

$$donde \quad c = \begin{cases} \dfrac{s}{B_{wl}} + L_{wl} & si \quad x = MN \\ 0 & si \quad x \neq MN \end{cases}$$

A. Coste de señalización en la actualización de registro

El coste total de señalización para la actualización de registro durante una sesión lo definimos como C_u. Este valor viene dado por la carga de tráfico en el intercambio de mensajes de señalización, es decir, este coste C depende del tamaño de mensajes de señalización y del número de saltos en cada *handover* de nivel 3 durante el tiempo en el que la comunicación del MN permanece activa. Por tanto, el coste viene definido por el tamaño de mensaje multiplicado por número de saltos necesarios.

Todos los movimientos entre subredes adyacentes suponen la generación de distintos mensajes de señalización. En Mobile IP y Mobile MPLS, es necesaria la actualización del registro con el nodo HA, mientras que en FH-Micro Mobile MPLS esa actualización es local con el nodo al que identifican como LERG. Aparte de la señalización propia del protocolo de gestión de la movilidad, algunas propuestas añaden el coste de establecimiento del túnel LSP. Ese es el caso de Mobile MPLS o FH-Micro Mobile MPLS. En el caso de nuestra propuesta, LW Mobile MPLS, el registro de actualización se realiza con el ILER, que es el nodo de entrada al dominio MPLS, mientras que el túnel LSP se establece desde el nodo articulado hasta el nuevo ELER (NELER). De esta forma, tendremos los siguientes valores para el coste de señalización en la actualización de registro:

$$C_u(Mobile\ IP) = 2 \cdot s_u \cdot h_{MN-HA} \cdot N_h \tag{11}$$

$$C_u(MMPLS) = 2 \cdot s_u \cdot h_{MN-HA} \cdot N_h + 2 \cdot s_l \cdot h_{FA-HA} \cdot N_h \tag{12}$$

$$C_u(FH\ MicroMobileMPLS) = 2 \cdot s_u \cdot h_{MN-LERG} \cdot N_h + 2 \cdot s_u \cdot h_{FA-FA} \cdot N_h + 2 \cdot s_l \cdot h_{FA-LERG} \cdot N_g \cdot N_h \tag{13}$$

$$C_u(LW\ MMPLS) = 2 \cdot s_u \cdot h_{MN-ILER} \cdot N_h + 2 \cdot s_l \cdot h_{LN-NELER} \cdot N_h \tag{14}$$

B. Pérdida de paquetes durante una sesión

La pérdida de paquetes durante una sesión la definimos como la suma de los paquetes perdidos en cada uno de los movimientos producidos en dicha sesión. En Mobile IP y Mobile MPLS, todos los paquetes en vuelo se pierden debido a que no existe ninguna técnica de almacenamiento ni recuperación. En FH-Micro Mobile MPLS los paquetes en vuelo que aún no han sido entregados se perderán hasta que se inicia el mecanismo de almacenamiento temporal. Nuestra propuesta LW Mobile MPLS también dispone de un mecanismo de recuperación que permite que se minimice la pérdida de los mensajes que se ven afectados por el tiempo de interrupción que provoca un movimiento a una red adyacente, tal y como se explicó en apartados anteriores. Con el mecanismo planteado en nuestra propuesta, los mensajes en vuelo entre el NA y el PELER se pueden recuperar y ser reenviados por el nuevo segmento de LSP creado para transportar la información hasta el NELER.

Por tanto, el valor P_{loss} para cada propuesta puede definirse de la siguiente forma:

$$P_{loss}(Mobile\,IP) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(MobileIP)\right] \cdot \lambda_d \cdot N_h \quad (15)$$

$$P_{loss}(MMPLS) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(MobileMPLS)\right] \cdot \lambda_d \cdot N_h \quad (16)$$

$$P_{loss}(FH\,Micro\,Mobile\,MPLS) = t(s_u, h_{MN-FA}) \cdot \lambda_d \cdot N_h \quad (17)$$

$$P_{loss}(LW\,Mobile\,MPLS) = t(s_u, h_{MN-NELER}) \cdot \lambda_d \cdot N_h \quad (18)$$

Donde T_h es el tiempo medio de *handover*, que está definido como la suma de tres términos: Tiempo de interrupción, tiempo de establecimiento y $T_{inter}/2$.

C. Tamaño del buffer

En nuestra propuesta, el buffer necesario para almacenar los paquetes en vuelo está situado en el Nodo Articulado. El mecanismo de recuperación de paquetes se activa en el momento en el que el MN notifica al PELER que va a cambiar de red mediante un mensaje de señalización del movimiento. De las propuestas que estamos analizando, la única que utiliza un almacenamiento de paquetes es el esquema FH-Micro Mobile MPLS, por tanto a continuación mostramos el tamaño de *buffer* previsto para esa propuesta y para la que presentamos en este artículo.

$$T_{buffer}(FH\,Micro\,Mobile\,MPLS) = \left(\frac{1}{2}T_{ad}\right) + t(s_u, h_{MN-FA} + h_{FA-FA}) \cdot \lambda_d \quad (19)$$

$$T_{buffer}(LW\,Mobile\,MPLS) = \left(\frac{1}{2}T_{ad}\right) + t(s_u, h_{LN-PELER} + h_{PELER-LN}) \cdot \lambda_d \quad (20)$$

V. Conclusiones y Trabajo Futuro

En este artículo se propone una arquitectura denominada *LinkWork Mobile MPLS* que permite una gestión de la movilidad eficiente en redes de acceso MPLS. Una de las novedades más interesantes de esta propuesta es la existencia de ciertos LSR especiales denominados Nodos Articulados cuyo objetivo es reencaminar el túnel LSP hacia el LER que da servicio al nodo móvil en cada *handover*, así como permitir la recuperación de paquetes que se encuentran en vuelo durante la interrupción del servicio que provoca un *handover*. Esto solventa algunos de los principales problemas de Mobile IPv6.

Con el estudio analítico realizado obtenemos el comportamiento de la arquitectura con respecto al uso de los enlaces, el coste de señalización para la actualización del registro, las pérdidas de paquetes en una sesión producidas durante los distintos movimientos y el tamaño de *buffer* necesario para llevar a cabo el mecanismo de recuperación propuesto. Además, comparando nuestro trabajo con otros similares como Mobile IP, Mobile MPLS y FH-Micro Mobile MPLS, comprobamos cómo el comportamiento de nuestra propuesta responde de forma adecuada en cada uno de los análisis realizados. Cabe destacar el bajo coste de señalización de LW Mobile MPLS y la capacidad para minimizar la pérdida de paquetes frente a otras propuestas.

Con respecto al trabajo futuro, se está trabajando ya en posibles mejoras que optimicen el rendimiento de la arquitectura propuesta. En primer lugar, el hecho de que ciertos nodos LSR (nodos articulados) se encarguen de computar las rutas, puede llegar a suponer una carga adicional que afecte al proceso de *handover*. Desde hace algún tiempo, el IETF está desarrollando una nueva técnica que libere del cómputo de LSPs a los nodos MPLS. La arquitectura PCE (*Path Computation Element*) [11] es el resultado de ese trabajo y se está estudiando su integración con nuestra propuesta.

Agradecimientos

Este trabajo está financiado, en parte, por la Junta de Extremadura, Consejería de Infraestructuras y Desarrollo Tecnológico y el FEDER a través de los proyectos con código No. PRE07035 y PRI08A079.

Referencias

[1] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”. IETF RFC 3775. June 2004.

[2] Langar, R., Bouabdallah, N., and Boutaba, R. 2008. “A comprehensive analysis of mobility management in MPLS-based wireless access networks”. *IEEE/ACM Trans. Netw.* 16, 4 (Aug. 2008), 918-931.

[3] Passas, N.; Salkintzis, A.K.; Wong, K.D.; Varma, V.K., "Architectures and protocols for mobility management in all-IP mobile networks [guest editorial]," *Wireless Communications, IEEE* , vol.15, no.2, pp.6-7, April 2008.

[4] E. Rosen, A. Viswanathan, R. Callon. “Multiprotocol Label Switching Architecture. IETF RFC 3031. January 2001.

[5] Z. Ren, C. Tham, C. Foo, and C. Ko, “Integration of mobile IP and multi-protocol label switching,” in *Proc. IEEE ICC*, 2001, vol. 7, pp. 2123-2127.

[6] R. Langar, S. Tohme and N. Bouabdallah, “Mobility management support and performance analysis for wireless MPLS networks,” Inernational Journal of Network Management, Wiley, 16, 4 (July 2006), 279-294.

[7] Kaiduan Xie; Wong, V.W.S.; Leung, V.C.M.; , "Support of micro-mobility in MPLS-based wireless access networks," *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE* , vol.2, no., pp.1242-1247 vol.2, 20-20 March 2003.

[8] Vassiliou, V.; Owen, H.L.; Barlow, D.; Sokol, J.; Huth, H.-P.; Grimminger, J.; , "M-MPLS: Micromobility-enabled multiprotocol label switching," *Communications, 2003. ICC '03. IEEE International Conference on* , vol.1, no., pp. 250- 255 vol.1, 11-15 May 2003.

[9] Shou-Chih Lo; Guanling Lee; Wen-Tsuen Chen; Jen-Chi Liu; , "Architecture for mobility and QoS support in all-IP wireless networks," *Selected Areas in Communications, IEEE Journal on* , vol.22, no.4, pp. 691- 705, May 2004.

[10] Hundessa, L.; Domingo-Pascual, J.; , "Reliable and fast rerouting mechanism for a protected label switched path," *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE* , vol.2, no., pp. 1608- 1612 vol.2, 17-21 Nov. 2002.

[11] A. Farrel, J. P. Vasseur, J. Ash. “A Path Computation Element (PCE)-Based Architecture”. IETF RFC 4655. August 2006.

Arquitectura para Provisión de Servicios Ubicuos en redes IMS-P2P

Augusto Morales Domínguez, Tomas Robles, Ramon Alcarria, Sergio González-Miranda
Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid
Avenida Complutense 30, Madrid, España
{amorales,trobles,ralcarria,miranda}@dit.upm.es

***Resumen*- La computación ubicua y los servicios de nueva generación plantean la necesidad de unificar todos los tipos de arquitecturas dentro de un contexto tecnológico común. En este contexto se propone una arquitectura que intenta homogeneizar el proceso de publicación, búsqueda y consumo de servicios tanto en redes basadas en infraestructuras fijas como IMS, y redes con topologías dinámicas como P2P, de manera que se asegure una flexibilidad en el despliegue de servicio a su vez que se aprovechan funcionalidades que ya han sido implementadas.**

***Palabras Clave*- IMS,P2P, Arquitectura, Servicios**

I. INTRODUCCIÓN

El creciente avance de Internet sobre la telefonía móvil ha establecido nuevos requerimientos para el despliegue de servicios tanto en la red como en los terminales, y adicionalmente ha propuesto un reto para las operadoras que desean aumentar sus ingresos a través del soporte de nuevas características en las Redes de Nueva Generación (NGN) [1]. Por otra parte la popularización de los servicios basados en redes P2P y todas las ventajas que aportan, suponen nuevos retos para las arquitecturas de redes tradicionales en donde los servicios son provistos, publicados y comercializados por infraestructuras fijas.

En el entorno tecnológico actual existen diversas tecnologías que están disponibles a los usuarios que quieran consumir u ofrecer un servicio en Internet. Por un lado están los servicios que están soportados por una infraestructura fija de servidores, por ejemplo un sitio web o el correo electrónico y, por otra parte, están los servicios que son provistos por una infraestructura dinámica en donde los recursos están distribuidos a lo largo de toda la red. Adicionalmente se observa una convergencia de estos dos dominios de comunicación, orientada a los usuarios finales, en donde los servicios puedan ser creados, consumidos y desplegados de manera ubicua sin importar en qué parte de la topología se encuentren. Por lo tanto existen una serie de requisitos para asegurar esta interacción, que es a su vez se complicada debido a las limitaciones tecnológicas y la existencia de características dinámicas, en donde no se conozcan a priori cuáles serán los servicios que se querrán desplegar y en qué lugar se encuentran.

En este contexto, y siendo el IP Multimedia Subsystem(IMS)[2] un conjunto de especificaciones que describen las NGN, proponemos una arquitectura para el despliegue de servicios en redes P2P [4] e IMS, en donde usuarios de una red móvil puedan consumir servicios desplegados por otros usuarios en una red P2P dinámica y flexible. Ya que existen diversas propuestas [4][5][6]y prototipos de interconexión de redes entre los entornos P2P e IMS se intentará realizar una abstracción del nivel de red y un enfoque en el análisis de los requisitos a nivel de servicio.

La arquitectura propuesta está centrada por lo tanto en abordar los problemas concernientes a la publicación y consumo de servicios dinámicos, disparidad topológica, así como también el mecanismo de establecimiento de sesiones entre clientes y servidores. Siguiendo este enfoque, aspectos relativos a la conectividad a nivel IP no serán abordados, pero sí existirán referencias que permitan identificar la localización de los servicios a nivel topológico, de manera que su búsqueda y consumo puedan ser logradas.

El artículo está organizado de la siguiente manera: la sección II realizará un estudio tecnológico sobre P2P e IMS. En la sección III se propondrá un caso de uso y sus respectivos requerimientos. En la sección IV se propondrá la arquitectura y SDL necesarios para el soporte del caso de uso anterior. Finalmente se expondrán las conclusiones y trabajos futuros.

II. TECNOLOGÍAS

P2P es un modelo de red que ha sido desarrollado en los últimos años en diferentes formas y ha causado un impacto directo e indirecto en el desarrollo tecnológico actual, comenzando desde los proveedores de servicios de internet hasta los usuarios finales. Existen estudios [7] [10] que estiman que el tráfico agregado por las aplicaciones P2P contribuye a aumentar el tráfico de la red. Por esta razón estas aplicaciones utilizadas por usuarios típicos pueden resultar una desventaja para los intereses de los operadores de telecomunicaciones. Sin embargo está claro que esta tecnología está en apogeo y por lo tanto es interesante para los operadores adaptar tanto la red[8] como los modelos comerciales a esta realidad.

IMS es una tecnología que tiene como objetivo unificar las redes móviles con Internet, a partir de la especificación de un núcleo de comunicaciones IP que a su vez puede dar soporte a redes conmutadas por circuitos. Una de las características principales de IMS es que permite una convergencia entre los métodos de acceso hacia las capas de servicio, control y conectividad. IMS utiliza SIP [9] como su protocolo principal de comunicaciones. La arquitectura IMS describe un número de funciones o *enablers* genéricos que pueden ser reutilizados para generar una nueva gama de servicios disponibles en la red. Este enfoque de desarrollo horizontal del IMS va en contraste con el desarrollo vertical en donde existen implementaciones separadas de cada nivel y las funcionalidades no pueden ser reutilizadas.

En principio las redes P2P e IMS tienen diferentes enfoques pero existen estudios [12] que corroboran que una cooperación entre estos dos entornos es el camino óptimo para mejorar la manera en la cual los servicios son provistos en Internet y beneficiar tanto a operadores como a usuarios finales.

III. Casos de Uso

En un escenario enfocado en la convergencia, un usuario accede a un servicio ofrecido por su operador de telefonía móvil. En este contexto, una plataforma IMS por si sola tendría la capacidad para garantizar este servicio, pero a su vez, podrían existir muchos que no sean ofertados por el operador pero interesantes para el usuario. Para ello el IMS establece una serie de interfaces de comunicación con el objetivo de lograr extender la gama de servicios. Sin embargo existe un inconveniente ya que su alcance se limita a infraestructuras fijas en Internet o a redes de terceros. Podemos observar un escenario en el que se contemplan situaciones especiales, como por ejemplo que el servicio que se desea consumir no se encuentra dentro del dominio del proveedor de telecomunicaciones, sino dentro de una nube en Internet, o que el servicio tampoco está en una infraestructura fija sino que se provee desde una red P2P. Como consecuencia, el IMS deberá contar con mecanismos necesarios para asegurar que los terminales puedan encontrar y beneficiarse de este recurso, sin aumentar la complejidad del terminal duplicar características ya implementadas.

En otro escenario más explicito, un usuario móvil se encuentra en una feria tecnológica de grandes dimensiones y desea crear un servicio para que sus amigos puedan seguir su recorrido y localizarlo en todo momento. Como la feria aporta conectividad Wi-fi a sus invitados, el usuario utiliza su teléfono móvil para conectarse a Internet y publicar continuamente mediante *Web Services* información sobre su posición capturada por el GPS de su terminal móvil. El servicio se despliega sobre una red P2P de la cual el usuario ha elegido ser parte ya que la infraestructura de la feria solo aporta conectividad pero no requerimientos específicos para que el servicio pueda ser encontrado y consumido. En el caso de que un usuario IMS desee acceder a este servicio deberá existir un mecanismo que haga de intermediario entre la infraestructura de red del proveedor, la cual es cerrada, y el servicio P2P desplegado en Internet. A simple vista puede pensarse que el usuario IMS podría utilizar directamente una tecnología [6] que le permita unirse a la red P2P y que luego descubra el recurso compartido, al igual que una aplicación común. Esta solución tiene una serie de inconvenientes: la creación de otra red IP superpuesta conllevaría a la pérdida de rendimiento además de todas las mejoras con respecto a calidad de servicio, fiabilidad, convergencia y seguridad que aporta IMS.

Del caso anterior se puede deducir que para hacer factible este tipo de escenarios, deberán existir elementos adicionales dentro de la arquitectura IMS que hagan de pasarela entre el tráfico generado entre ambos entornos, así como también elementos que sean capaces de gestionar la manera en que los servicios son descubiertos, publicados y consumidos.

IV. Arquitectura Propuesta

La arquitectura propuesta hace posible la provisión de servicios desde la red P2P, por parte de un terminal dentro de la red IMS. Las principales características de esta arquitectura son la inclusión de un servidor de descubrimiento y publicación de servicio, además de la definición de un SDL. Este SDL permitirá a clientes existentes en la red P2P procesar y generar información sobre el tipo de servicio ofrecido (requerimientos, disponibilidad), así como permitir a clientes IMS realizar búsquedas sobre estos servicios, todo esto apoyándose en el proveedor. La arquitectura propuesta se ha diseñado tomando como base que la conectividad IP entre las redes P2P e IMS existe a través de una Gateway Application Server (GAS), que resuelve todos los problemas de encaminamiento de paquetes y adhesión del dominio IP como elemento registrado dentro de la red P2P.

A. Arquitectura de Red

La arquitectura de red es necesaria para asegurar la conectividad IP entre los sistemas IMS y P2P. Tomando en cuenta que esta característica no es uno de los aspectos primordiales de este artículo se han analizado distintas propuestas [5][6][7] que intentan resolver este inconveniente. Nuestra contribución la hemos basado principalmente en detectar el enfoque que más se acerca a los requerimientos impuestos por el caso de uso.

Se ha tomado como referencia la arquitectura de interconexión propuesta en el artículo "Interconnecting P2PSIP and IMS" [12] el cual propone como elemento principal la existencia de un GAS instalado en la red IMS y que hace de pasarela con una red P2PSIP. Para esta arquitectura existe una implementación de prototipo que verifica que el mecanismo de acceso y transmisión de datos entre ambas redes es válido. La arquitectura está basada en una comunicación bidireccional en donde los nodos de red IMS son mapeados bajo recursos con dominio específicos. Para ello se realizan operaciones P2P de *put*, que contienen el IP del GAS como dirección de todos los recursos detrás del dominio IMS. Por otra parte, los recursos de la red P2PSIP serían accesibles utilizando parámetros fijados en el núcleo IMS, como Initial Filter Criteria (iFC), de manera que cualquier petición que llevara como destinatario esta red, sería redirigida al GAS

Esta arquitectura resuelve el problema de la conectividad y propone una aproximación de la manera en que un recurso puede ser accedido, pero a su vez hay distintos requerimientos a nivel de servicios que no pueden ser resueltos. El primero se basa en que toda la comunicación se realiza a través del protocolo SIP, por lo que todos los clientes tendrían que implementar este protocolo aún cuando su capacidad de procesamiento sea limitada o las características de la red no lo permitan. Otro aspecto se basa en que no hay un mecanismo flexible de búsqueda y publicación de servicios que permita mantener la separación entre el núcleo de la red IMS y los servicios. Esto se debe a que se implementan Service Point Triggers (SPTs) que sólo son gestionables modificando parámetros del Home Subscriber Server (HSS). Esta característica le resta además independencia a la red, y no permite reutilizar funciones y enablers de IMS, de manera que el desarrollo del servicio no sería horizontal, tal como está recomendado por la Open Mobile Alliance (OMA) [13].

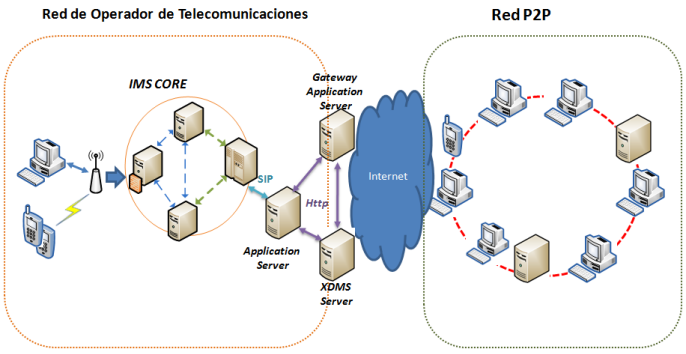


Fig. 1. Arquitectura de Red IMS-P2P

Como extensión a esta arquitectura de red, se propone la utilización de HTTP como protocolo de consumo de servicios, debido a su homogeneidad y a la facilidad de implementación en dispositivos tanto fijos como móviles. Se plantea además independizar la gestión de servicios del núcleo de la red IMS, de manera que puedan existir múltiples implementaciones de servidores que provean más funcionalidades, y a la vez permitir una futura composición y gestión dinámica de servicios. Para esto último se propone la inclusión de un XML Document Management Server (XDMS) [15] para la gestión de SDLs, al igual que un Application Server (AS) que actuará a nivel de servicio como un elemento intermediario entre ambas arquitecturas.

En la figura 1 se representa la arquitectura de servicios que incluye todos los dispositivos de red que realizarán funcionalidades dentro de la arquitectura. El GAS y XDMS server están dentro de la frontera del dominio IMS ya que su implementación no está limitada por la localización física y, además, el servicio que están proveyendo podría ser implementado en una topología distribuida. Una de las ventajas de este enfoque es que dependiendo de las prioridades del operador, pueden proporcionarse aplicaciones desplegadas por terceros, ya que el Application Server es el único elemento con el cual el núcleo IMS tendría interacción directa. Otra característica importante es que, gracias a la utilización del protocolo HTTP, se podrían evitar problemas de filtrado, interoperabilidad etc.

B. Diagrama de Comunicación

La arquitectura desde el punto de gestión y publicación de servicios se enfoca en soportar que, por medio de sesiones SIP, clientes IMS obtengan los parámetros sobre los servicios publicados en la red P2P. La arquitectura sin embargo no considera el caso contrario, por el que usuarios P2P quieren acceder a servicios provistos por clientes IMS.

En la figura 3 se explica el diagrama de secuencia en el cual un cliente IMS consume un servicio que ha sido publicado por un cliente P2P. Para ello se asume que el cliente IMS ya ha sido registrado dentro del núcleo y que existe una conectividad entre las redes P2P e IMS.

El cliente P2P publica a través de una petición (1) un documento SDL con la descripción del servicio, que contendrá todos los parámetros que el cliente necesite para establecer una conexión. Esta publicación se realizará a través de la red P2P utilizando mensajes tipo put(K,Data), en donde *K* es el hash del nombre del servicio, y *Data* el SDL que lo describe. Esta petición (1) será luego procesada y encaminada en un nuevo paquete HTTP (2) por el GAS hacia el servidor XDMS, que contendrá un repositorio de SDL de servicios publicados por clientes P2P. En principio, el servidor XDMS podría no necesitar al GAS, y la comunicación podría ser directa con la red P2P de manera que se soportarían repositorios distribuidos. No obstante, se ha optado por un enfoque centralizado para minimizar la complejidad en la pila de protocolos de este último. Otro aspecto a mencionar es la seguridad. Cuando un cliente P2P desee publicar un servicio en el XDMS deben existir mecanismos que validen tanto el tránsito de la información, como la confidencialidad e integridad del servicio. En nuestro caso asumimos que la seguridad ha sido garantizada por otros mecanismos o capas inferiores.

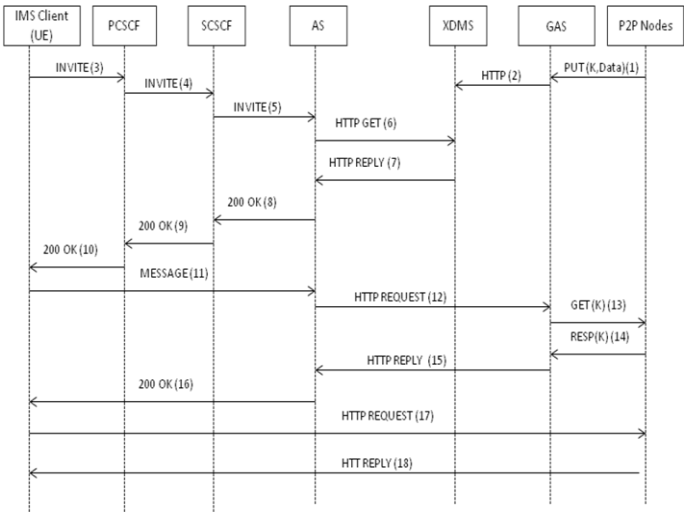


Fig. 2. Diagrama de Secuencia

Tras el proceso de publicación, el servicio está listo para ser consumido. El cliente IMS (UE) no conoce a priori cuáles son los servicios que están disponibles y, en principio, debería ser agnóstico sobre el lugar donde se están ejecutando, por lo que envía un INVITE SIP (3) con las características del servicio que desea consumir. Seguidamente su petición es redirigida (4)(5) entre los distintos elementos del núcleo IMS hacia el AS. El AS procesará esta petición y buscará por medio de una petición HTTP (6)(7) en el XDMS la lista de servicios que han sido publicados y que corresponden con los parámetros enviados por el UE. Dependiendo del perfil del usuario y de los requerimientos de red o terminal el AS enviará la respuesta (8)(9)(10) con la lista de servicios que más se aproximan a su petición.

En el siguiente paso el UE envía un SIP MESSAGE (11) al AS con los datos del servicio que desea consumir. Estos datos son utilizados por el AS para construir una nueva petición HTTP (12) con el nombre del servicio elegido. El AS enviará esta petición al GAS y éste preguntará a la red P2P sobre la localización del servicio mediante un mensaje get(k) (13), siendo *k* el hash del nombre del servicio. El GAS obtendrá una respuesta (14) de la red P2P con la dirección del nodo que efectivamente ha publicado este servicio. Después de que el AS reciba(15) la localización éste genera una nueva información que contendrá el SDL del servicio y la dirección IP en donde podrá encontrarlo. Como paso final, el UE podrá establecer una comunicación directa (17)(18) con el nodo P2P, construyendo un URL con la dirección IP del destinatario, considerando todas las exigencias previamente impuestas.

C. SDL de Servicio

Llamamos SDL a la especificación XML utilizada para definir qué contiene y cómo se comporta un servicio. En concreto, en el entorno propuesto, el documento que contiene la especificación del servicio escrita en un SDL es generado por cada uno de los nodos P2P y se utiliza a lo largo del ciclo de vida del servicio.

Como primer punto, el SDL contiene un apartado de metadatos que facilitarían la búsqueda de los servicios. Dentro de los metadatos el parámetro *resource* se ha definido para flexibilizar el consumo del servicio y que no dependa estrictamente de una dirección IP, de manera que el cliente IMS pueda comunicarse con el nodo P2P mediante URIs.
A continuación se muestra un ejemplo de SDL que describirá un servicio de localización publicado por un nodo P2P.

```
<?xml version="1.0" encoding="UTF-8"?>
<service_description>
<metadata service_name=”SDL_Position", resource="/position/index.html",
description=”This template provides localization service”,
category=”localization”, language=”spanish”, autor="Alice", version=”1.0”,
cost=”free”>
</metadata>
<access_type DHT_type="160bits", backup_ip="",data=””>
</access_type>
<restrictions/>
<security SSL_enabled="yes" port="443">
</security>
</service_description>
```

Fig. 3. SDL de descripción de un servicio

D. Interacción del Application Server y XDMS

La arquitectura actual de IMS está dotada de componentes que permiten distribuir las funcionalidades de manera que puedan ser reutilizadas. De este modo, hemos considerado una propuesta de solución basada en la capa de aplicación mediante la implementación del habilitador de servicios XDMS encargado de almacenar documentos SDL y proveer mecanismos para el acceso a la información contenida en dichos documentos SDL hacia otras entidades. Estas entidades pueden ser nodos publicadores/consumidores o dispositivos más complejos, que posteriormente interpretarán la información para la construcción de servicios avanzados.

En nuestra propuesta, el XDMS implementado como una base de datos centralizada dentro de la arquitectura IMS, adquiere importancia ya que, al extenderlo y adaptar su funcionamiento básico para gestionar documentos SDL que describen servicios, se logra proporcionar una plataforma de gestión de información a todos los elementos involucrados en el proceso de publicación y consumo de servicios.

Por un lado una aplicación que actúa como agente SIP, desplegada sobre el servidor de aplicaciones, se encarga de ofrecer el entorno necesario para la gestión de las transacciones hacia y desde el XDMS, que derivan en la entrega de información compuesta hasta el cliente IMS. Además se encarga de obtener las restricciones impuestas por el cliente IMS y, a partir de estas, seleccionar el servicio óptimo de entre los publicados (en forma de documentos SDL) en el XDMS.

V. CONCLUSIONES

La arquitectura propuesta aborda los problemas de interacción a nivel de servicio entre el IMS y las redes P2P y permite que usuarios de una red puedan publicar y consumir servicios de otra. La arquitectura se enfoca en definir las funcionalidades necesarias a la vez que se intenta reutilizar elementos ya existentes. Otro de los principales aportes es la propuesta de un SDL, que permite estandarizar la manera en que un servicio es tratado durante todo su ciclo de vida.

Finalmente, con esta arquitectura se intenta aportar una solución al ámbito de acceso a los servicios que han sido publicados en redes P2P, y que son consumidos desde una red IMS. Se especifica también un mecanismo de acceso y gestión de documentos SDL mediante XDMS que soporte un despliegue y combinación de servicios homogéneos.

Actualmente se está desarrollando un prototipo, con tecnologías Open Source como: FOKUS IMS en el núcleo, SailFin para los servidores de aplicación y UCT IMS Client para los clientes IMS, con las cuales se espera validar los conceptos expuestos en este artículo.

AGRADECIMIENTOS

Este artículo ha sido cofinanciado por el Ministerio de Ciencia e Innovación a través del proyecto T2C2 (Tecnologías Semánticas para la Colaboración Ciudadana, TIN2008-06739-C04-03).

REFERENCIAS

[1] International Telecommunication Union http://www.itu.int/ITU-T/ngn
[2] 3GPP, “IP Multimedia Subsystem (IMS); Stage 2,” 3rd Generation Parnership Proejct (3GPP), TS 23.228, Dec. 2007. Disponible en: http://www.3gpp.org/ftp/Specs/html-info/23228.htm
[3] IP Multimedia Subsystem (IMS) Handbook. ISBN 978-1-4200-6459-9, página 80.
[4] Radovanovic, I. ; Lukkien, J. ; Shudong Chen ; Molanus, C. ; Ozcelebi, T. “Virtual community management for enabling P2P services in the IMS network” 2nd International Conference on Internet Multimedia Services Architecture and Applications, 2008. IMSAA 2008.
[5] Liotta, A ; Ling Lin; “Managing P2P services via the IMS”. 10th IFIP/IEEE International Symposium on Integrated Nettwork Management, 2007, IM’07
[6] Xiaozhou Ye ; Jiandong Zhang ; Jinlin Wang ; “Architecture of HIKEC: An IMS-based Mobile P2P File Sharing Service”. International Conference on Communication Technology, 2006. ICCT '06.
[7] A. Parker. The true picture of peer-to-peer filesharing. http://www.cachelogic.com , July 2005.
[8] Hiyong Xie, “Explicit Communications for Cooperative internet Traffic Control” PhD Thesis, Yale University 2008.
[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: Session Initiation Protocol,” Internet Engineering Task Force, RFC 3261, Jun. 2002. Disponible en: http://www.rfc-editor.org/rfc/rfc3261.txt
[10] Liotta, A. ; Lin Ling; “The Operator’s Response to P2P Service Demand”. IEEE Communication Magazine, pp 76-83, July 2007
[11] Maibaum, N. ; Mundt, T. ; “JXTA: a technology facilitating mobile peer-to-peer networks” International Mobility and Wireless Access Workshop, 2002. MobiWac 2002
[12] Hautakorpi, J. ; Salinas, A. ; Harjula, E. ; Ylianttila, M. “ Interconnecting P2PSIP and IMS”. The Second International Conference on next Generation Mobile Applications, Services and Technologies, 2008, NGMAST ’08.
[13] Open Mobile Alliance. Enabler Release Definition for IMS in OMA. Disponible:http://www.openmobilealliance.org/technical/release_program/ims_v1_0.aspx
[14] Novotny, M. ; Zavoral, F. “Reputation-based methods for building secure P2P networks” First International Conference on the Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008.
[15] Fraunhofer FOKUS XML Document Management Server. Disponible: http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/xdms/index.html

EVALUACIÓN DE NUEVOS CANALES DE DISTRIBUCIÓN EN SERVICIOS INTERACTIVOS IP

José Ruiz-Mas, José I. Aznar-Baranda, José María Saldaña-Medina, Julián Fernández-Navajas
Grupo de Tecnologías de las Comunicaciones (GTC) Instituto de Investigación en Ingeniería de Aragón (I3A)
Blanca Hernández-Ortega, Lorena Blasco-Arcas, Julio Jiménez-Martínez
Departamento de Investigación y Comercialización de Mercados
Universidad de Zaragoza
C/ María de Luna 1, 50018 Zaragoza, España
e-mail: {jruiz, jiaznar, jsaldana, navajas, bhernand, lorena, jjimenez} @unizar.es

***Resumen*- El presente proyecto pretende definir y evaluar los servicios interactivos IP que, como nuevos canales de distribución, permiten establecer una relación más cercana y directa con el consumidor. Estos servicios interactivos presentan características diferenciadoras que los convierten a priori en un atractivo medio de distribución y han originado la necesidad de analizar los aspectos cognitivos y afectivos experimentados por el usuario en su interacción con los mismos. Para evaluar estos nuevos canales se ha desarrollado un servicio interactivo IP piloto que incorpora las distintas situaciones existentes. Para ello en análisis previos se han establecido las variables más importantes que definen el comportamiento de los usuarios, tanto aquellas experimentadas durante su interacción y compra como aquellas relativas a la valoración de su comportamiento e intenciones futuras de uso. Los resultados obtenidos facilitarán la relación de la empresa con sus clientes, incrementando la implicación de éstos y acrecentando su fidelidad.**

***Palabras Clave*- servicios interactivos IP, canales de compra, televisión interactiva**

I. INTRODUCCIÓN

En los últimos años el entorno empresarial se ha caracterizado por su interés en los nuevos canales de distribución (Internet, terminales móviles), los cuales le permiten captar nuevos clientes y estrechar su relación con otros ya existentes. Estos canales se apoyan en servicios interactivos que potencian el establecimiento de relaciones duraderas, observándose que la retención de los clientes en el largo plazo incrementa los beneficios de la empresa ([1], [2]). Asimismo, el uso de servicios interactivos optimiza las experiencias vividas por los usuarios y origina la adopción de nuevos roles por parte de los mismos. Estos servicios suelen apoyarse en protocolos de Internet, los cuales ofrecen inmensas posibilidades que pueden ser fácilmente aprovechadas en los intercambios comerciales, ya que facilitan el acceso a una mayor base de clientes y mejoran la relación entre ambas partes.

En el ámbito de las TIC es relevante señalar la tendencia a la convergencia de tecnologías y servicios. Así, por ejemplo, en la actualidad los usuarios son capaces de acceder a contenido televisivo desde diferentes canales (cable, satélite y banda ancha) y terminales (televisión, ordenador y teléfono móvil). De este modo, la evolución hacia los servicios interactivos tiene importantes implicaciones desde el punto de vista de la redefinición de modelos de negocio existentes, así como en el papel jugado por el usuario en este proceso. En esta línea, [3] afirma que en los nuevos medios interactivos "el usuario es a la vez la persona que escucha y la que habla, el consumidor y el productor". Además, otra tendencia que se está produciendo en el sector de la televisión generalista es lo que la literatura ha denominado cross-media [4]: la fusión de TIC aparentemente diferentes para ofrecer una experiencia más rica y acercarse a la mayor audiencia posible. Ejemplos de este tipo de enfoque son la participación del usuario enviando un SMS o la referencia a una web para la búsqueda de información adicional.

La convergencia de estas tendencias junto con el propio desarrollo de la tecnología está dando lugar a nuevos servicios interactivos como la televisión IP (IPTV). Este tipo de servicio de TV se integra con el servicio de conexión a Internet permitiendo la consulta de páginas Web, comprar a través de la red, o acceder a redes sociales, a la vez que se está viendo cualquier programa o serie. La principal ventaja de este servicio IP respecto al comercio electrónico por ordenador, consiste en la existencia de una mayor familiaridad del usuario con el medio (la televisión), como soporte de venta. Mientras que el manejo del ordenador requiere un aprendizaje y la adopción de una serie de conocimientos previos, la televisión presenta facilidades de uso que la hacen accesible a un mayor número de usuarios. Esta circunstancia permite acceder a muchos segmentos de la población que suelen ver frecuentemente la televisión pero que son reticentes al empleo de la Internet "tradicional" y las páginas Web (ej. individuos mayores de 60 años). Las distinciones tradicionales de la TV como medio de entretenimiento e Internet como medio para la búsqueda de información desaparece conforme esta convergencia tecnológica se va produciendo. Por tanto, estos nuevos servicios interactivos IP presentan características diferenciadoras que los convierten a priori en un atractivo medio de distribución, más accesible y completo que el comercio electrónico desarrollado en entornos online, pero que deben aún ser investigados para conocer su aceptación y desarrollo como nuevos canales de distribución.

Las investigaciones realizadas suelen enfocar el estudio de los nuevos servicios o la difusión tecnológica aplicando una visión parcial del fenómeno. Por un lado, la investigación realizada en el ámbito socio-empresarial

considera que el estudio sobre el comportamiento del consumidor mejora los beneficios de la empresa; no obstante, no profundiza en dicho conocimiento para implantar mejoras en la tecnología. Por otro lado, las nuevas soluciones tecnológicas no tienen en cuenta las expectativas y percepciones del usuario en la aceptación global de los servicios multimedia ofertados. De este modo, a pesar de las ventajas ofrecidas por los nuevos servicios multimedia, muchas empresas todavía no son conscientes del efecto ejercido por la tecnología subyacente a los mismos sobre el comportamiento final de los usuarios.

Esta es la dirección de trabajo en la que se halla inmerso este grupo de investigación multidisciplinar a partir del proyecto "*Nuevos canales de distribución en servicios interactivos IP: cuantificación de la calidad de la experiencia*", financiado por la Cátedra Telefónica de la Universidad de Zaragoza. Dicho proyecto tiene como uno de sus principales objetivos definir y evaluar la aceptación de los nuevos servicios interactivos que, como canales de distribución, permiten establecer una relación más cercana y directa con el consumidor. A tal fin se propuso desarrollar una plataforma de pruebas propia sobre la que realizar la experimentación requerida. De ahí, el diseño y generación de un servicio interactivo IP piloto que aglutine en diversas situaciones los aspectos más valorados por los usuarios. Análisis previos permitieron definir e identificar estas variables para mejorar el servicio prestado y la satisfacción experimentada por el individuo durante su interacción: facilidad de uso, personalización, interactividad entre pares, control percibido, diversión, curiosidad, etc. Los resultados obtenidos permitirán contrastar la evolución experimentada en las percepciones del usuario durante su interacción con el servicio diseñado. Asimismo, se podrá comprobar si factores vinculados con las emociones experimentadas por el usuario -diversión, entretenimiento, desconexión, curiosidad, etc.- influyen en su valoración de la experiencia vivida y posterior comportamiento y pueden verse modificados por las mejoras incorporadas en la calidad tecnológica del servicio.

Los detalles del trabajo desarrollado se tratan a continuación. La sección II se centra en el diseño del canal de compra desarrollando un servicio interactivo piloto que refleja las distintas situaciones existentes y las variables previamente consideradas. En la sección III se definen y planifican las pruebas a realizar para la obtención de resultados. Finalmente, la última sección detalla las conclusiones del presente trabajo.

II. DISEÑO DEL CANAL DE COMPRA

A. *Análisis previos del usuario: variables a considerar*

La evolución de las tecnologías en los últimos años, así como el desarrollo y perfeccionamiento de nuevas aplicaciones, han permitido desarrollar entornos *online* más sofisticados que facilitan la interacción con el cliente y que a su vez facilitan la consecución de relaciones más estrechas entre ambas partes. En este contexto, el objetivo principal de la investigación es analizar el efecto generado por dos nuevos aspectos relativos al diseño de entornos *online* interactivos: personalización e interactividad, los cuales facilitan la generación de actitudes y comportamientos más proactivos en los usuarios/clientes. En esta línea, consideramos que el hecho de disponer de un entorno personalizado a partir de los gustos y necesidades de cada cliente, así como la posibilidad de éste de interactuar directamente con la empresa y con otros clientes, incrementa la satisfacción y la confianza experimentada, fomentando por lo tanto la lealtad. Desde este punto de vista, profundizar en el efecto generado por estas variables en el entorno de la televisión IP interactiva adquiere especial relevancia, ya que éstas influirán en el comportamiento de compra electrónica debido a la colaboración e implicación directa del cliente en el diseño y creación de dicho entorno.

La personalización como variable relacionada con el comportamiento de compra del consumidor ha sido considerada por los profesionales de marketing en las últimas dos décadas. El desarrollo de las nuevas tecnologías ha incrementado notablemente las posibilidades de personalización, facilitándose la recogida y el tratamiento de la información [5]. Sin embargo, el concepto de personalización ha sido utilizado en diferentes contextos para denominar no siempre las mismas acciones. Por esta razón, en la actualidad dicho término presenta dificultades de aplicación e implementación, ya que su contenido varía en función del tipo de negocio del que se hable [6]. Otro aspecto que ha influido en la conceptualización de la personalización es la relación que plantea con el término *customización*. En [7] definen la personalización como la adaptación de las aplicaciones o atributos del producto en función de las características o beneficios esperados por el cliente, mientras que la *customización* implica el tratamiento de éste de forma diferenciada, basándose en lo que él haya expresado previamente durante su interacción. De este modo, la personalización es realizada por la empresa basándose en la coincidencia entre las categorizaciones de contenido y el perfil del cliente, mientras que la *customización* es realizada por el propio individuo [8].

Respecto a la interactividad, el concepto ha experimentado una gran evolución, pudiendo encontrarse algunos trabajos centrados en la importancia de los atributos tecnológicos [9], mientras que otros analizan las percepciones del usuario al respecto [10]. Esta variedad de definiciones plantean la necesidad de llevar a cabo un esfuerzo integrador que contemple la multidimensionalidad de la variable. En este sentido es destacable la aportación de [11], que examina perspectivas de comunicación y de no-comunicación considerando aspectos tecnológicos, relativos a la comunicación y a las percepciones del usuario. Así pues, la interactividad hace referencia al grado en el que una tecnología de la comunicación permite diseñar un entorno predeterminado, en el cual los participantes tienen la posibilidad de intercambiar mensajes y comunicarse sincrónica y asincrónicamente con una o varias personas a la vez. En la actualidad, la línea de investigación más destacada sobre interactividad insiste en que no pueden ser analizados únicamente procesos y aplicaciones concretas, sino que debe profundizarse en las percepciones y experiencias del usuario [12]. En este sentido es destacable la aportación de [13], con el desarrollo de una escala de 18 *items* de medición de la interactividad percibida, la cual tiene en cuenta los factores más relevantes reflejados en la literatura: control depositado en el cliente, grado de respuesta, extensión del diálogo entre cliente y empresa, implicación, tiempo requerido para la interacción, funciones que faciliten la retroalimentación personalizada, simulación de comunicación interpersonal,

velocidad, retroalimentación, acción y reacción y aspectos multimedia. En este contexto, el presente trabajo analiza la interactividad centrándose en aquellos aspectos relacionados con la experiencia subjetiva del usuario; concepto que ha sido denominado "interactividad percibida".

B. Diseño del servicio interactivo IP piloto

Para evaluar estos nuevos canales de distribución se ha desarrollado un servicio interactivo IP piloto donde los aspectos de su diseño han sido adoptados a partir de la literatura existente y de la medición de las variables previamente consideradas. Este servicio se ha integrado en una plataforma de pruebas como la representada en la Fig. 1.

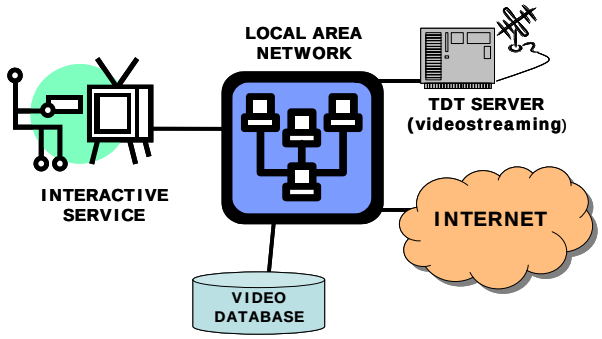


Fig. 1. Plataforma de pruebas del servicio interactivo IP.

Dicha plataforma integra el acceso *on-line* a contenidos de los canales televisivos y la visualización de series, películas y otros contenidos *off-line* con la conectividad a recursos de Internet. Los canales de televisión son provistos al usuario a partir de un servidor de *streaming* conectado directamente a un receptor de TDT. Por otro lado, los contenidos *off-line* se encuentran almacenados en una base de datos, la cual, es accedida por la aplicación cuando el usuario final demanda alguno de estos servicios

Inicialmente, el usuario puede configurar a su medida el servicio y seleccionar los canales que desea recibir (Fig. 2). A continuación, se ofrece al usuario la capacidad de personalizar e interactuar en la compra de productos de distinta naturaleza durante y/o al final de las emisiones recibidas. El servicio se ofrece con distintos grados de personalización e interactividad a fin de modular las variables de comportamiento objeto de estudio (Fig. 3). Los resultados asociados a la variación de los niveles de personalización e interactividad se obtienen a partir de la realización por parte del usuario de cuestionarios integrados en el propio servicio ofrecido (Fig. 4). definición y planificación de pruebas: obtención de resultados

La metodología que se ha utilizado para la obtención de los datos es la experimentación, ya que la naturaleza de las variables analizadas requiere la observación del comportamiento del cliente durante un periodo de tiempo. De este modo, pretende eliminarse la complejidad inherente a la terminología utilizada, la cual dificultaría garantizar que todos los compradores interpretaran lo mismo por personalización e interacción. El uso de la experimentación en la investigación de relaciones causales presenta principalmente dos tipos de ventajas: (1) control sobre las variables analizadas y (2) obtención de datos reales en un proceso que trata de reproducir las mismas condiciones que se darán en un entorno real de compra.

Fig. 2. Configuración del servicio interactivo IP: selección de canales.

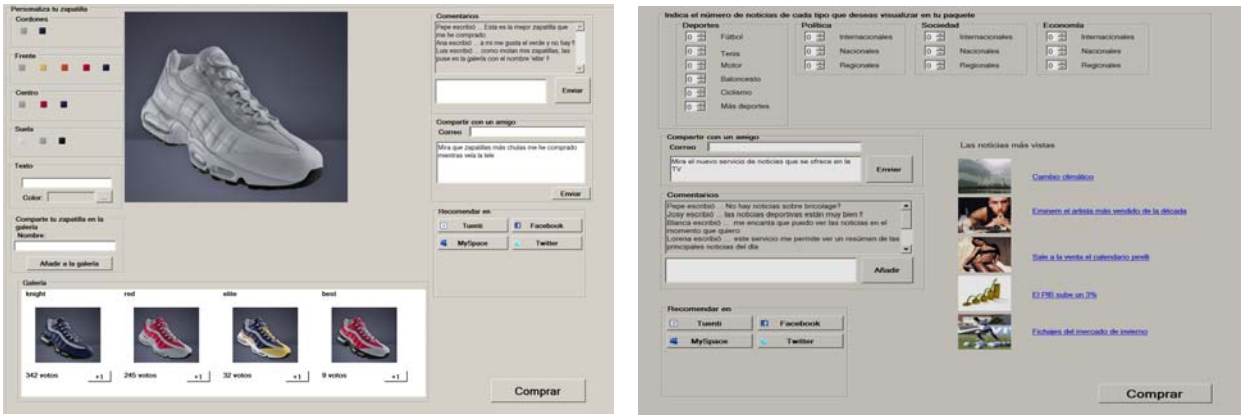


Fig. 3. Personalización e interactividad en la compra de productos de distinta naturaleza (zapatilla y paquete de noticias).

Fig. 4. Ejemplo de cuestionario a completar.

En el experimento las variables a manipular son el nivel de interactividad y de personalización percibidos. Se plantea un diseño factorial entre sujetos 2x2, resultando cuatro grupos experimentales a los que se aplicaron las diferentes situaciones posibles (Fig. 5) en el diseño de la parte de compra a fin de modular las variables objeto de estudio.

Fig. 5. Grupos experimentales.

La cronología del experimento fue la siguiente previa presentación del mismo:

1. Personalización del menú de la televisión en función de las preferencias del usuario, tanto en forma y diseño como en contenidos (canales). Recogida de datos: experiencias pasadas del usuario, su grado de implicación, etc.
2. Visualización de una serie de entretenimiento con la posibilidad de realizar una compra de producto personalizada. Cada grupo recibe un tratamiento diferente en función de las variables analizadas. Recogida de datos: percepciones respecto a las variables a estudio.
3. Compra de un producto audiovisual personalizable (paquetes de noticias). Recogida de datos: percepciones respecto a las variables a estudio.

Los sujetos fueron asignados al escenario experimental correspondiente de forma aleatoria, siendo la muestra total resultante de 300 personas de entre 20 y 25 años, estudiantes de la Universidad de Zaragoza. La elección de este tipo de población objetivo se fundamenta en el hecho de que es la población que mayor uso hace de las nuevas tecnologías de forma intensiva. Según el informe de Telefónica "La Sociedad de la Información en España 2009", el perfil del internauta en España, de forma similar que en Europa es el de una persona de 16 a 24 años (82%), con nivel formativo alto (85%) y estudiantes (91%). La medición de las variables objeto de estudio se realizó mediante cuestionarios insertos en la propia aplicación utilizando escalas *Likert* de 7 puntos.

Los primeros análisis ANOVA ponen de manifiesto que las percepciones de utilidad, facilidad de uso y las evaluaciones de satisfacción y calidad de la experiencia se ven considerablemente incrementadas en el escenario que hay presencia de las variables consideradas frente a los escenarios en los que una de las variables no aparece.

III. Conclusiones

En el proyecto presentado se ha desarrollado una plataforma de pruebas para la evaluación de servicios IP interactivos como nuevos canales de distribución. La plataforma integra el acceso *on-line* a contenidos de canales televisivos y la visualización de contenidos *off-line* con la conectividad a recursos de Internet. Los aspectos del diseño del servicio creado han sido adoptados a partir de la literatura existente y de la medición de las variables consideradas: personalización e interactividad. Los resultados previsibles, aun en fase de análisis, permitirán estrechar los vínculos de la empresa con sus clientes, incrementando la implicación de éstos y acrecentando su fidelidad.

Agradecimientos

Este trabajo esta financiado la Cátedra Telefónica de la Universidad de Zaragoza.

Referencias

[1] Jiang, P. y Rosenbloom, B. (2005). Customer intention to return online: price perception, attribute-level performance, and satisfaction unfolding over time. European Journal of Marketing 39(1-2): 150-174

[2] Ang, L. y Buttle, F. (2006). "Customer retention management processes. A quantitative study". European Journal of Marketing 40(1-2): 83-99.

[3] Christensen, L.H., 2002. The impact of interactivity on television consumption, Working paper Dublin City University.

[4] Ha, L. y Chan-Olmsted, S.M. (2004). "Cross-Media use in electronic media: the role of cable television web sites in cable television network branding and viewership". J. of broadcasting and electronic media 48.

[5] Vesanen, J. (2007). "What is personalization? A conceptual framework". European Journal of Marketing 41(5-6): 409-418.

[6] Kemp, T. (2001). "Personalization isn't a product". Internet Week, No. 864, 4 June, p. 1.

[7] Peppers, D., Rogers, M. y Dorf, B. (1999), "The One to One Fieldbook: The Complete Toolkit For Implementing a 1 to 1 Marketing Program". Double Day, New York, NY.

[8] Cöner, A. (2003). "Personalization and customization in financial portals". Journal American Academy of Business 2(2): 498-504.

[9] Steuer, J.S. (1992). "Defining Virtual Reality: Dimensions Determining Telepresence", Journal of Communication 42(4): 73-93.

[10] Wu, G. (2000). "The Role of Perceived Interactivity in Interactive Ad Processing", unpublished dissertation, University of Texas at Austin.

[11] Kiousis, S. (2002). "Interactivity: a Concept Explication", New Media and Society 4(3): 355-383.

[12] Lee, J.S. (2000). "Interactivity: A new approach". Association for Education in Journalism and Mass Communication, Phoenix.

[13] McMillan, S.J. y Hwang, J.S. (2002). "Measures of Perceived Interactivity: An Exploration of the Role of Direction and Communication, User Control, and Time in Shaping Perceptions of Interactivity". Journal of Advertising 31(3): 29-42.

SymPA: Una herramienta para la caracterización del rendimiento de aplicaciones móviles en entornos celulares

Almudena Díaz Zayas, Pedro Merino Gómez
Departamento de Lenguajes y Ciencias de la Computación,
Universidad de Málaga
Campus Teatinos, Málaga, 29071
almudiaz@lcc.uma.es, pedro@lcc.uma.es

***Resumen*—SymPA es una herramienta de captura de tráfico IP que se ejecuta en el propio terminal. También lleva a cabo la monitorización de parámetros relacionados con la red como la potencia de señal recibida, el identificador de celda, la tecnología de acceso radio (GPRS/UMTS/HSDPA), información sobre el perfil de calidad de servicio asociado a los contextos PDP que se abren para el establecimiento de las conexiones de datos, consumo de energía y localización geográfica del terminal.**

Como principal aportación de esta herramienta cabe destacar que la obtención de información de tan diversa naturaleza nos permite correlar la información obtenida de la red celular con información del tráfico cursado a nivel IP. De esta forma es posible analizar el impacto de las condiciones de propagación y de la configuración de la red celular sobre el tráfico de datos de los usuarios y sobre la calidad de servicio experimentada por los mismos.

***Palabras Clave*—Tráfico de datos, redes celulares, rendimiento, correlación**

I. Introducción

Las redes de telefonía móvil, en sus orígenes, fueron diseñadas para el transporte de tráfico de voz. En este contexto el único actor posible para la explotación de los servicios de voz era el operador. En la actualidad las mejoras introducidas en dichas redes para soportar el tráfico de datos ha abierto el mercado de los servicios de telefonía móvil a terceras partes que pueden ubicar los servidores de aplicación fuera de las redes de los operadores.

Ahora, además del tráfico, en las redes móviles, es necesario medir parámetros relacionados con la propagación como la señal de potencia recibida, la posición geográfica del terminal (para contrastarla, por ejemplo, con la ubicación de la estación base), los perfiles de calidad de las conexión de datos ofrecidas por los operadores, la tecnología de acceso radio en uso (GPRS/UMTS/HSDPA), el consumo de batería, etc. La obtención de información de esta naturaleza es necesaria para complementar las soluciones de monitorización y medida existentes para redes fijas, de forma que podamos detectar el origen de los problemas de rendimiento de los servicios y de los protocolos empleados en el diseño de aplicaciones para dispositivo móviles.

Con este objetivo, se plantea el desarrollo una herramienta que nos permita analizar y caracterizar el comportamiento de las aplicaciones móviles en términos del rendimiento en las comunicaciones sobre redes celulares.

SymPA [1] es una herramienta para el análisis de protocolos que afronta este reto añadiendo la funcionalidad de captura de tráfico en los terminales móviles. Junto con la captura del tráfico de datos también se obtiene información relativa a la potencia de señal recibida, la tecnología de acceso en uso, el identificador de la celda, consumo de batería, etc. La correlación del tráfico capturado a nivel IP con la información capturada a nivel radio y a nivel del contexto PDP permite detectar la fuente de problemas en el rendimiento de la conexión de datos.

Por ejemplo en la figura 1 se puede visualizar la información de los paquetes IP capturados durante una sesión de medidas. También se muestra la información capturada sobre la tecnología de acceso en uso. Los paquetes IP marcados en negro son paquetes perdidos. Si correlamos ambas informaciones podemos concluir que dicha pérdida de paquetes se ha producido durante un handover entre dos tecnologías de acceso radio diferentes (GPRS/UMTS).

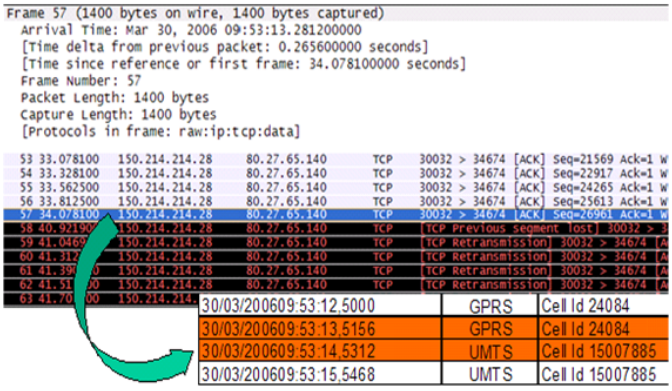


Fig. 1. Pérdida de paquetes debido a un cambio de tecnología de acceso radio

Las principales ventajas de esta herramienta son

- Obtención de medidas independientes de la tecnología de acceso en uso.
- Obtención de medidas del rendimiento de las aplicaciones en terminales comerciales y en condiciones reales de funcionamiento.
- Ofrece soporte para depurar del comportamiento de las aplicaciones sobre redes celulares reales.
- Ofrece el soporte necesario para que los proveedores de servicios y los operadores conozcan la calidad de los servicios en cada punto de la red y en cada instante, de

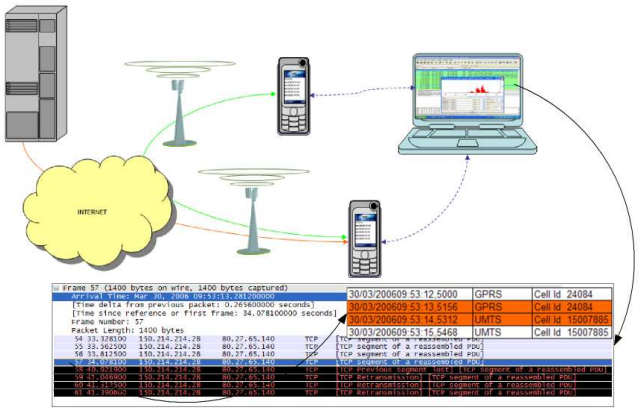


Fig. 2. Escenario de uso de la herramienta SymPA

forma que puedan optimizar la red en base a la calidad de servicio percibida por los usuarios finales.

A. Descripción general

SymPA (Symbian Protocol Analyzer) permite capturar el tráfico IP cursado por el terminal móvil sin interferir con las aplicaciones en ejecución. Entre las funcionalidades proporcionadas por la herramientas destacan las siguientes:

- Captura del tráfico IP
- Conversión del tráfico capturado a un formato estándar que permite visualizar las capturas con herramientas de análisis de tráfico compatibles con el formato pcap.
- Consulta de los parámetros que determinan el perfil de calidad de servicio asociados a los contexto de datos abiertos por las aplicaciones para la transferencia del tráfico IP.
- Monitorización de la tecnología de acceso en uso, monitorización del identificador de celda y de la potencia de señal recibida.
- Monitorización de la ubicación geográfica del terminal basado en el módulo GPS disponible en algunos terminales móviles.
- Monitorización del consumo de batería

Las funcionalidades proporcionadas por SymPA permiten depurar el rendimiento de los protocolos de red sobre redes celulares, detectar posible fallos de la implementación de dichos protocolos en dispositivos móviles o descubrir comportamientos irregulares de los protocolos tradicionales en redes inalámbricas.

La vista principal de la aplicación se muestra en la figura 3. En la parte superior se muestra información de la conexión radio: tecnología de acceso en uso, identificador de celda, potencia de señal recibida y el índice numérico de las barras de señal mostradas por el terminal. Dicha información es actualizada cada segundo.

Las principales funcionalidades proporcionadas por SymPA son introducidas con más detalles en las siguientes secciones.

B. Conectividad IP

La herramienta permite comprobar la conectividad a Internet ofreciendo la posibilidad de establecer una conexión TCP con cualquier otro dispositivo conectado a la red móvil o fija. Una vez establecida la conexión TCP la dirección IP asignada al terminal es también mostrada en pantalla, lo cual permite poner en conocimiento del desarrollador la IP del terminal para realizar comprobaciones de conectividad futuras.

C. Captura de tráfico

Cuando la herramienta se encuentra em modo captura de tráfico se muestra en la parte de superior de la pantalla una ”C”. En dicho modo de funcionamiento la herramienta almacena, sin procesar, todo los paquetes IP que llegan al terminal en un fichero de texto plano. Cuando la captura finaliza la herramienta ofrece la posibilidad de convertir los datos capturados al formato de entrada de la herramienta text2pcap que traduce los ficheros que se le pasan como entrada al formato pcap. La herramienta text2pcap es distribuida de forma gratuita junto con el conocido analizador de tráfico Wireshark. Los ficheros pcap pueden ser analizados directamente con Wireshark, dicha herramienta proporciona una gran variedad de opciones de filtrado de tráfico, análisis estadístico y generación de gráficas. Los menús que proporciona la herramienta para acceder a las funcionalidades de captura se muestran en la figura 4.

D. Información del contexto PDP (Packet Data Protocol)

Esta funcionalidad permite acceder a la información de los interfaces de red, del contexto y del perfil de calidad de servicio negociado durante el inicio del contexto PDP abierto por la aplicación. La figura 5 muestra la información del contexto PDP proporciona por la herramienta.

E. Ping

La herramienta proporciona una utilidad tradicional de red como es el ping, la cual permite estimar el retardo de ida y vuelta de una conexión IP establecida desde el terminal móvil. Los retardos son medidos en microsegundos.

F. Transferencia de ficheros entre móviles

SymPA incorpora una simple aplicación que permite transferir entre dos terminales que ejecuten SymPA un fichero de texto. Esta funcionalidad permite analizar las conexiones directas entre terminales móviles. La captura del tráfico cursado entre los terminales móviles permitirá caracterizar la comunicación móvil-móvil en redes celulares.

G. Monitorización de la información de celda

La herramienta permite consultar la información de red (ver figura 6) o monitorizar y almacenar dicha información en un fichero de texto. En el modo de monitorización la información de red es volcada a fichero cada segundo junto el sello de tiempo del instante en el que se capturó la información del celda. Mientras que la monitorización de red está activa en la parte superior de la pantalla se muestra la letra ”M”.

H. Posicionamiento GPS

La funcionalidad de posicionamiento GPS permite monitorizar la velocidad de desplazamiento del terminal y la ubicación. La información es almacenada cada segundo, junto con los sellos de tiempo, en un fichero de texto. Los datos de la ubicación son utilizados para correlar las medidas con su ubicación geográfica. También existe la posibilidad de mostrar un mapa con la localización actual del terminal.

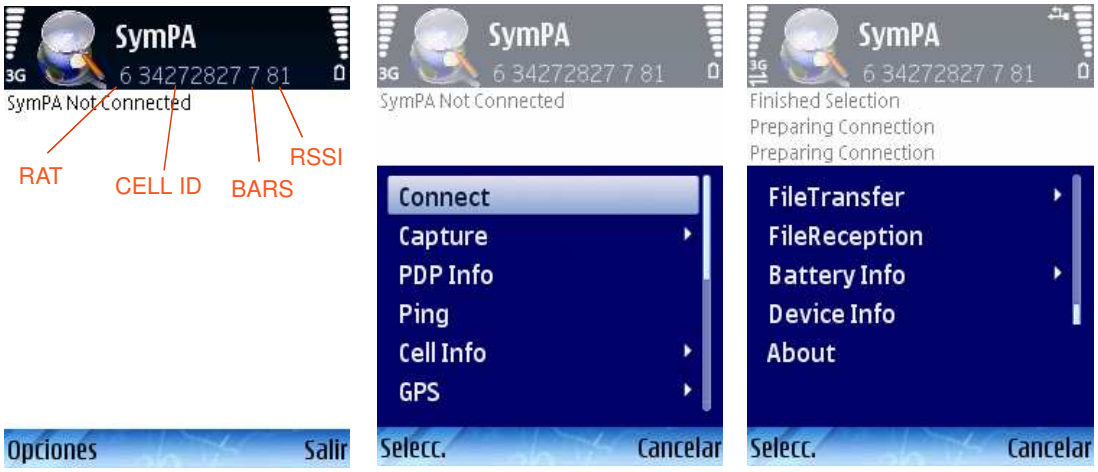


Fig. 3. Menú principal de la aplicación

Fig. 4. Captura de tráfico IP

Fig. 5. Monitorización del contexto PDP

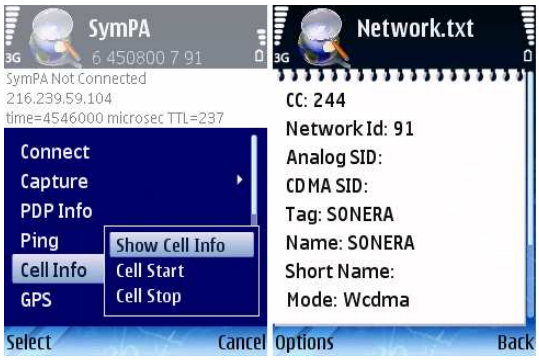


Fig. 6. Monitorización de parámetros de red

I. *Monitorización de la batería*

Al igual que el resto de funcionalidades de monitorización la información del estado de la batería es almacenada en un fichero de texto junto con los sellos de tiempo.

Los formatos de los ficheros generados por SymPa son explicados con mayor detalle en el manual de la herramienta disponible en el sitio Web http://www.lcc.uma.es/∼pedro/mobile/Software/sympa.html.

J. *Caso de uso*

SymPA permite capturar el tráfico cursado por aplicaciones desarrolladas por terceras partes. El uso normal de la herramienta es el siguiente, mientras que la aplicación bajo análisis está en ejecución SymPA se ejecuta en paralelo para capturar el tráfico cursado por la aplicación, los parámetros del contexto abierto por la aplicación, la información de celda y el consumo de energía. Toda la información recopilada es, posteriormente, correlada. En la figura 7 se representa el comportamiento de la tasa de recepción de datos a nivel IP, las variaciones del retardo (jitter), las pérdidas de paquetes y los errores de secuencia durante la recepción en el terminal de un video transmitido desde un servidor mediante el protocolo RTP. Junto con la información del tráfico se presenta la información de la celda y del consumo de batería. Tras la representación de todas los datos recabados por la herramienta se pueden obtener algunas conclusiones interesantes como que las variaciones en la potencia de señal recibida (RSSI) repercuten en un incremento del jitter, las ráfaga de pérdidas de paquetes están asociadas a los cambios de celda (los cambios de celda se representan con líneas verticales discontinuas) o la disminución del consumo de energía cuando la tecnología de acceso en uso es GPRS. En las figuras 8 y 9 se muestran nuevos ejemplos del tipo de resultados que se

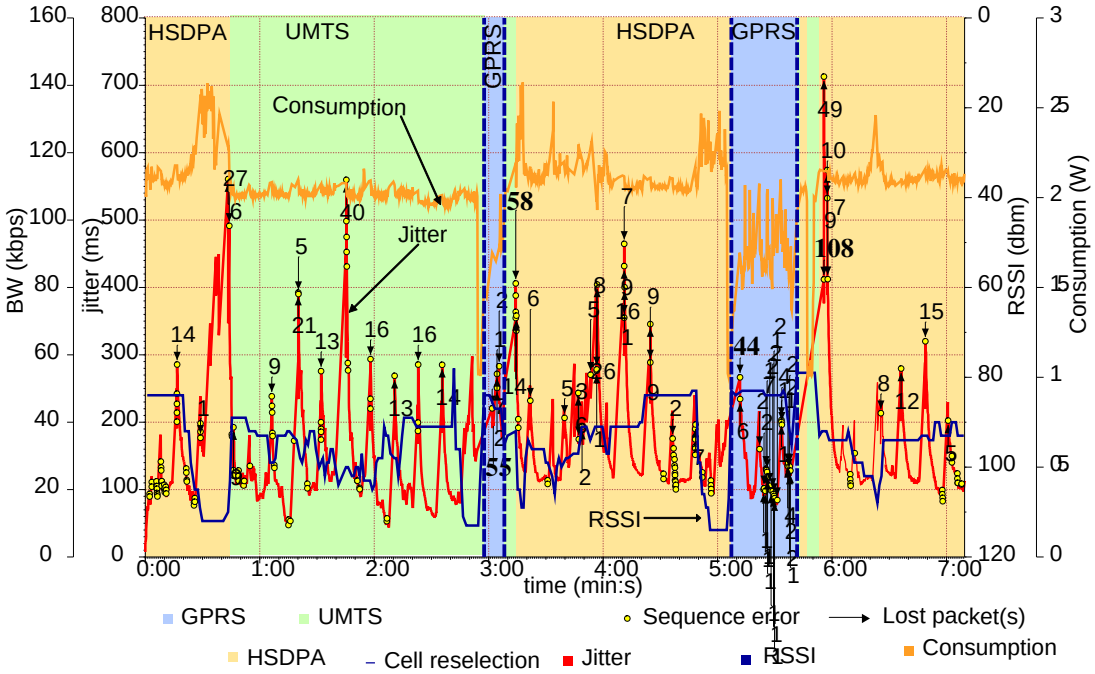


Fig. 7. Datos recopilados durante una sesión de streaming de vídeo mientras el terminal móvil se encontraba en movimiento

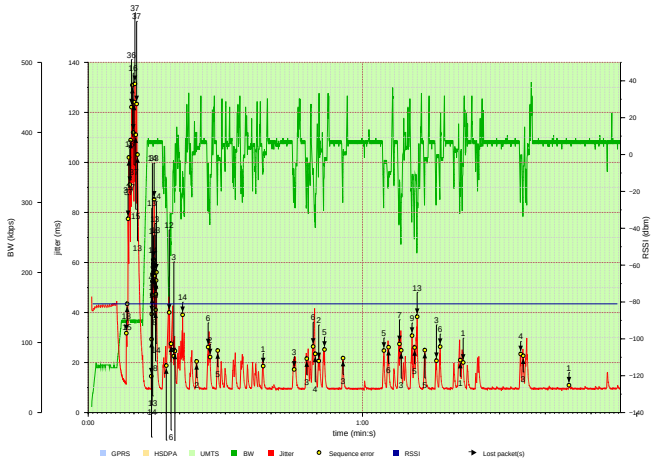


Fig. 8. Pruebas en UMTS. Escenario estático. Degradación de ancho de banda disponible y detección de pérdidas de paquetes.

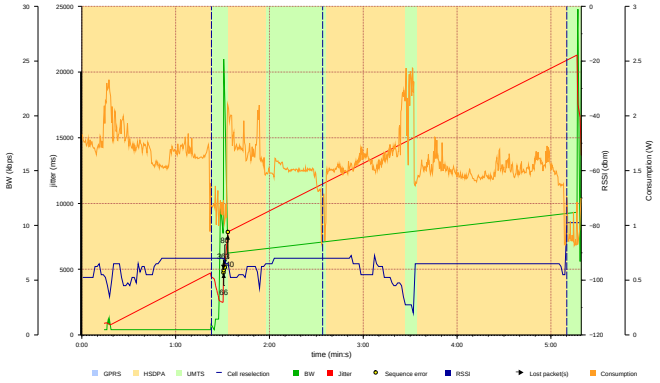


Fig. 9. Pruebas en UMTS/HSDPA. Escenario dinámico. Detección de cambios de tecnologías de acceso radio, detección de pérdidas de paquetes

obtienen mediante la correlación de los datos recopilados.

En la figura 2 se representa el escenario de uso de la herramienta. SymPA ha sido satisfactoriamente utilizada para la caracterización del rendimiento del servicio de video streaming en redes celulares [2], para la caracterización del consumo de energía en dispositivos móviles con capacidades avanzadas de conexión [3] y en la caracterización del impacto de los handovers sobre los conexiones de datos [5] [6].

Referencias

[1] A. Díaz, P. Merino, and F.Javier Rivas, "Mobile application profiling for connected mobile devices," *Pervasive Computing, IEEE*, vol. 9, no. 1, pp. 54 –61, jan.-march 2010.

[2] A. Díaz, P. Merino, and F.Javier Rivas, "Qos analysis of video streaming service in live cellular networks," *Computer Communications, Elsevier*, vol. 33, no. 3, pp. 322 – 335, 2010.

[3] A. Díaz and P. Merino, "A testbed for energy profile characterization of ip services in smartphones over live networks," *ACM/Springer Mobile Networks and Applications (MONET)*, vol. 15, no. 3, pp. 330–343, 2010.

[4] A. Díaz and P. Merino, "Evaluación de los mecanismos de handover implementados en redes comerciales de telefonía móvil," *IX Jornadas de Ingeniería Telemática (JITEL 2010)*, 2010.

[5] A. Díaz and P. Merino, "Evaluación de los mecanismos de handover implementados en redes comerciales de telefonía móvil," *IX Jornadas de Ingeniería Telemática (JITEL 2010)*, 2010.

[6] A. Díaz and P. Merino, "Evaluation of handover implementations in commercial gprs/umts/hsdpa networks," *IEEE Global Communications Conference (GLOBECOM 2010)*, 2010.

PPStop: dispositivo electrónico Bluetooth para el tratamiento de la enuresis

Oriol Ciurana Adell, Mario Viktorov Mechoulam, Josep Pegueroles Vallés
Departamento de Ingeniería Telemática
Universidad Politécnica de Cataluña
Jordi Girona, 1-3, Campus Nord - B3, 08034 Barcelona
{oriol.ciurana, mario.viktorov, josep.pegueroles}@entel.upc.edu

***Resumen*- El uso de las TIC para mejorar la calidad de vida de las personas ha sido una constante a lo largo de los últimos años. Buen ejemplo de ello es el impulso de los sistemas de telecomunicación para la mejora de tratamientos médicos. En este artículo se describe el diseño e implementación de un dispositivo electrónico basado en Bluetooth que tiene como finalidad el tratamiento de la incontinencia urinaria (enuresis). El desarrollo se ha realizado conjuntamente con el Hospital Sant Joan de Déu de Barcelona y la empresa Electrónica Feixas.**

***Palabras Clave*- Enuresis, Bluetooth.**

I. INTRODUCCIÓN

La enuresis es el término médico utilizado para definir el trastorno consistente en la presencia de micciones de orina incontroladas más allá de la edad en que se debería llegar a adquirir el control vesical. Estudios científicos y psicológicos indican que la enuresis puede tener tanto un tratamiento activo como pasivo. El dispositivo descrito en este artículo hace referencia al tratamiento pasivo de la enuresis, más conocido como "método de la alarma sonora"[1]. Se trata de activar artificialmente un estímulo sobre el paciente, de forma que sea consciente del momento de la micción y así aprenda a reconocer el vaciado inminente de la vejiga y pueda corregir el problema.

El método de la alarma no es nuevo, hace años que existen dispositivos que desempeñan la función de alarmar al paciente cuando se detecta una micción, aunque todos consisten en sistemas cableados, aparatosos e incómodos para el paciente. El dispositivo que se ha diseñado e implementado (denominado *PPStop*) pretende modernizar el tratamiento haciendo que el sistema de alarma se lleve a cabo de manera inalámbrica. El paciente percibe la alarma sonora a través de una aplicación que se ejecuta en su teléfono móvil y que desempeña la función de timbre (ver figura 1). Así no hace falta una conexión cableada entre el dispositivo detector de humedad y el timbre; sino que la tecnología Bluetooth[2] es la que posibilita el intercambio de datos entre el sensor de humedad y el móvil (mediante una PAN).

El objetivo principal del sistema diseñado es pues el de detectar la micción de orina y generar una conexión Bluetooth al terminal móvil del paciente que permita generar la alarma sonora. Esto debe lograrse de forma rápida para no deteriorar la efectividad del tratamiento (se entiende que el método es efectivo para un tiempo de alarma inferior a los 3 segundos) y minimizando el consumo energético global del dispositivo sensor para alargar su tiempo de vida. No obstante, no se trata del único objetivo pues el dispositivo electrónico tiene que ser capaz de recibir órdenes del terminal móvil del paciente para modificar su configuración. Además para la comodidad del paciente dicho dispositivo debe ser de reducidas dimensiones y debe poder ser mojado sin deteriorarse. A continuación se detalla el diseño del dispositivo y su implementación, y como se han solventado todas estas premisas.

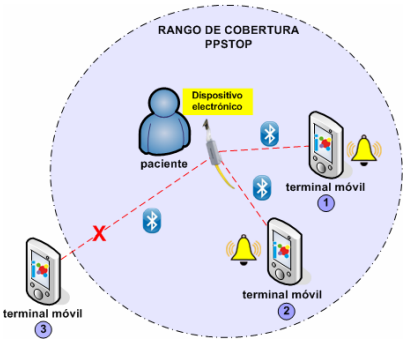


Fig. 1. Sistema *PPStop* para el tratamiento de enuresis.

II. TOMA DE DECISIONES

Para que el dispositivo electrónico pueda cumplir con su funcionalidad hay que dotarlo de algún tipo de inteligencia que sea capaz de recibir eventos externos y llevar a cabo unas acciones tras su detección. Es por ello que el dispositivo incorpora un microcontrolador. Los microcontroladores permiten ejecutar código (una unidad de control por ejemplo), activar puertos, modificar valores de registros, percibir eventos a través de interrupciones, almacenar datos en memoria, etc., por lo tanto su uso es imprescindible. Además, para la detección de la orina se requiere un sensor de humedad, de sensibilidad ajustable y que permita generar adecuadamente la interrupción hacia el microcontrolador. Para generar los avisos de alarma mediante Bluetooth hay que incorporar algún componente que realice búsquedas de terminales Bluetooth en su rango de cobertura y llevar a cabo una conexión para realizar el intercambio de datos pertinentes. Para ello existen transmisores Bluetooth que implementan su pila de protocolos y permiten realizar estas acciones a partir del envío de unas determinadas órdenes (comandos) especificadas por su fabricante. Finalmente, se precisa una fuente de energía que permita el correcto

funcionamiento de estos componentes, dotando al dispositivo de una autonomía suficiente. Teniendo en cuenta estas necesidades, se han elegido los componentes del dispositivo electrónico.

Como sensor de humedad se ha escogido un sensor convencional de doble pista en forma de "tira" que con la conducción entre sus pistas mediante la orina provoca el paso de corriente eléctrica y, en consecuencia, una caída de tensión.

Como microcontrolador se utiliza el modelo de 8 bits *XC864* del fabricante *Infineon*[3]. Este microcontrolador tiene un consumo relativamente bajo, tiene una capacidad de memoria flash de 4kB para código de aplicación y tiene una memoria ROM, RAM y capacidad de procesamiento suficientes para la funcionalidad que se le quiere dar. Además, permite ser "dormido" para ahorrar energía y ser "despertado" a través de la recepción de una interrupción.

Como transmisor Bluetooth se ha utilizado el componente de *Infineon PBA31308/2 eUniStone*[4]. Este transmisor es de clase 2, lo que permite conseguir un alcance de unos 10m, funciona con Bluetooth 2.0 + *Enhanced Data Rate (EDR)* e implementa toda la pila de protocolos Bluetooth. Se controla mediante el envío de comandos AT específicos de *Infineon* i el intercambio de datos se lleva a cabo a través de la UART. Tiene implementado el perfil de Bluetooth *Serial Port Profile (SPP)* necesario para el intercambio de datos por radiofrecuencia a través de comunicación serie. Sólo soporta una conexión simultánea y tiene un consumo razonable. Con el objetivo de minimizar el consumo global del dispositivo electrónico, se le hace trabajar siempre como master, es decir, toda comunicación con el terminal móvil siempre es iniciada desde el dispositivo electrónico, tanto en la generación de las conexiones de alarma como de las conexiones para la recepción de órdenes procedentes del terminal móvil del paciente. Adicionalmente al transmisor, se precisa una antena PCB que lo complemente y permita que pueda transmitir al entorno radio.

La batería incorporada en el dispositivo es una batería de litio de reducidas dimensiones modelo *CR1/3N*[5] del fabricante *EEMB*, que ofrece una capacidad y voltaje nominal suficientes para las exigencias de corriente de los distintos componentes y tiene un tiempo de vida suficientemente largo.

Al margen de todos los componentes citados, se debe dotar el dispositivo de la circuitería necesaria para definir un determinado nivel de sensibilidad del sensor de humedad i determinar el estado de la batería del dispositivo. Para el primer caso se utiliza un comparador con una tensión de referencia variable y controlable a través del microcontrolador. En el segundo, se monitoriza la tensión proporcionada por la batería y se cuantifica mediante un conversor AD.

Para finalizar, todos los componentes a excepción del sensor de humedad deben ser perfectamente encapsulados y sellados para que se mantengan aislados de cualquier tipo de humedad procedente de las micciones de orina o del lavado del dispositivo.

III. Preparación del dispositivo

Para la implementación del dispositivo electrónico se ha construido un chip de 5.5cm x 2.5cm que contiene todos los componentes electrónicos interconectados adecuadamente. La figura 2 ilustra la estructura del dispositivo y la disposición de los componentes.

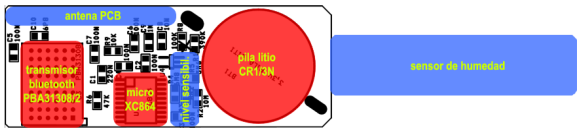


Fig. 2. Estructura y componentes del dispositivo electrónico.

El módulo marcado como nivel de sensibilidad es una agrupación de componentes que permiten definir 5 niveles de sensibilidad distintos en el sensor. Dicha agrupación se muestra en la figura 3. Se puede apreciar como la pista del sensor está conectada a un comparador (entrada 3) que tiene establecida una tensión de referencia en la otra entrada (entrada 4). Esta última es la que determina el nivel de sensibilidad del sensor, es decir, a partir de esta tensión el comparador activa la señal de *"wake up"* que genera la interrupción para despertar el microcontrolador. La resistencia R_8 actúa como protección de la entrada 3 del comparador. La resistencia R_1 se encarga de limitar el consumo cuando hay conducción en el sensor. Finalmente, las resistencias R_2, R_3, R_4 y R_5 permiten establecer los distintos valores de referencia a través de un divisor de tensión en función de que cada una de ellas esté conectada a 3.3V o a masa según convenga. Este hecho viene determinado por el valor de los puertos $P_{3.0}$, $P_{3.1}$, $P_{2.7}$ y $P_{0.1}$ del microcontrolador.

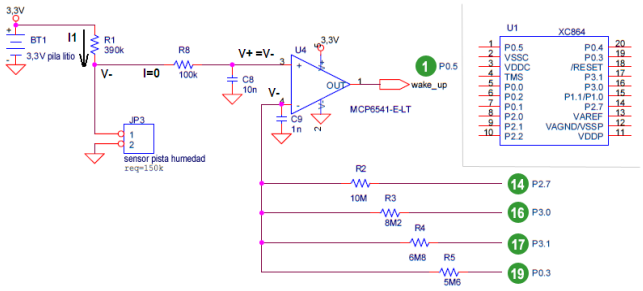


Fig. 3. Circuitería que define el nivel de sensibilidad del sensor.

IV. Unidad de control

La lógica del dispositivo electrónico se define a través de la unidad de control programada en el microcontrolador. Dicha lógica debe emular todo el comportamiento del sistema y ceñirse al protocolo establecido para la comunicación entre el dispositivo electrónico y el terminal móvil. El comportamiento del sistema es el que se muestra en el diagrama de flujo de la figura 4, que describe como debe actuar el dispositivo des del momento en que se genera el evento externo a través del sensor de humedad hasta que el microcontrolador debe volver a su estado de reposo (durmiendo).

A partir del diagrama de flujo y teniendo en cuenta los comandos AT del fabricante *Infineon* que permiten realizar

ciertas acciones sobre el transmisor Bluetooth y sus posibles respuestas, dicho diagrama se puede traducir en una máquina de estados que define plenamente la unidad de control.

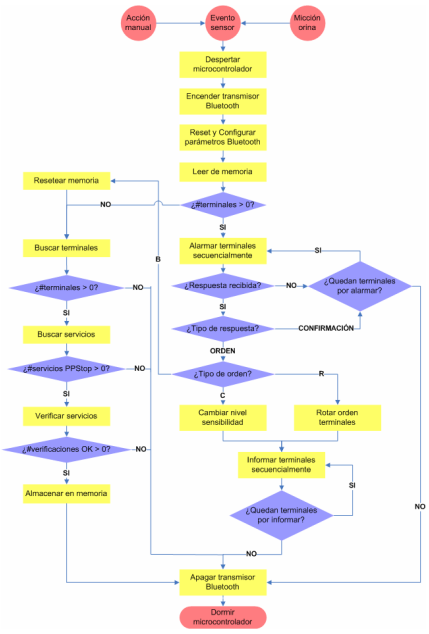


Fig. 4. Diagrama de flujo general del sistema.

Los comandos AT de *Infineon*[6] siguen el formato estándar *AT+[código_orden]=[parámetros]*. En cambio solamente existen dos tipos generales de respuesta; las de confirmación a comandos AT al transmisor Bluetooth (*ROK*, *OK* o *ERR=-[valor]*) y las que genera directamente el transmisor debido a la ejecución de las órdenes que se le envían por la UART. Estas últimas tienen el formato *+[código_respuesta]=[parámetros]*. A continuación se muestra una tabla que describe los comandos AT útiles para nuestro propósito y otra que describe sus posibles respuestas.

Comando AT	Descripción
AT+JRES	Resetea el dispositivo Bluetooth
AT+JSEC=1,1,1,04,1111	Establece el modo de seguridad: Modo 1; Informa sobre la clave de enlace; PIN variable; PIN de longitud 4; PIN=1111
AT+JSLN=06,PPSTOP	Establece el nombre del dispositivo Bluetooth: Nombre de longitud 6; NOMBRE=PPSTOP
AT+JDDS=0	Inicia la búsqueda de dispositivos (DDP): Sin límite de resultados
AT+JSDS=@mac,1101	Inicia la búsqueda de servicios en un dispositivo (SDP): Dirección MAC destino; UUID=1101 (SPP)
AT+JCCR=@mac,#canal	Crea una petición de conexión: Dirección MAC destino; Canal del servicio
AT+JSDA=longitud,datos	Envía datos al dispositivo remoto: Longitud de los datos (bytes); Datos a enviar

Tabla. 1. Descripción de los comandos AT utilizados.

La máquina de estados resultante para la unidad de control del microcontrolador es la mostrada en la figura 5, donde para cada estado del sistema se puede apreciar las posibles respuestas que se esperan del transmisor Bluetooth y cómo debe actuar el microcontrolador, ya sea realizando una acción interna o enviando un nuevo comando AT al transmisor Bluetooth a través de la UART. Sólo basta traducir la máquina de estados al lenguaje de programación C y grabar[7] dicho programa en la memoria del microcontrolador para definir su comportamiento.

Respuesta	Descripción
ROK	Reset realizado correctamente
OK	Comando ejecutado correctamente
ERR=-código	Error en la ejecución del comando
+RDDSRES=@mac,nombre, tipo	Nuevo dispositivo hallado durante el DDP: Dirección MAC remota; Nombre dispositivo remoto; Tipo de dispositivo remoto
+RDDSCNF=estado	La búsqueda de dispositivos (DDP) ha finalizado
+RSDSRES=nombre,#canal	Nuevo servicio hallado durante el SDP: Nombre del servicio remoto; Canal de operación del servicio remoto
+RSDSCNF=estado	La búsqueda de servicios (SDP) ha finalizado
+RDAI=longitud,datos	Datos recibidos: Longitud de los datos (bytes); Datos recibidos
+RDII	El dispositivo remoto se ha desconectado
+RCCRCNF=MTU,estado	Respuesta a una petición de conexión: Tamaño de la MTU; Estado de la conexión (0: OK, 1: KO)

Tabla. 2. Descripción de posibles respuestas a los comandos AT.

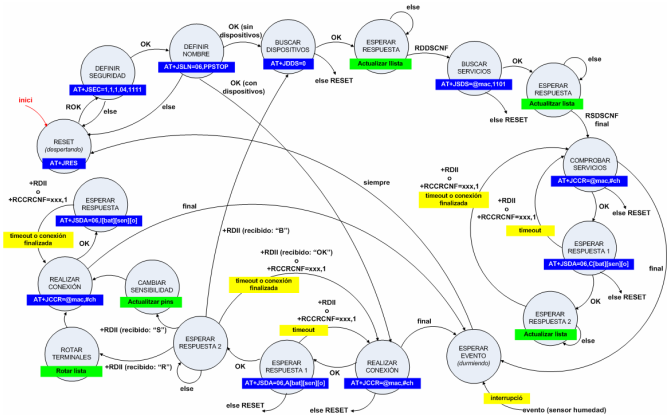


Fig. 5. Diagrama de estados de la Unidad de Control.

Se observa como el proceso de encendido del transmisor Bluetooth y su posterior configuración se realiza siempre que se genera una interrupción a través del sensor. El hecho que el proceso continúe realizando la búsqueda de dispositivos (DDP), búsqueda de servicios (SDP) y verificación de los mismos o bien realice directamente las conexiones de alarma depende únicamente de que haya terminales móviles *PPStop* almacenados en la memoria del microcontrolador. En este último caso, se genera una conexión de alarma para cada terminal almacenado en memoria de manera secuencial y se analizan las respuestas obtenidas del terminal móvil, realizando una acción sobre el propio microcontrolador (como por ejemplo un cambio de sensibilidad) en caso que se reciba una orden. Posteriormente se apaga el transmisor Bluetooth y se procede de nuevo a dormir el microcontrolador.

V. BALANCE ENERGÉTICO

El balance energético del dispositivo electrónico permite hacer una estimación de su tiempo de vida. Para ello, se han

considerado los distintos consumos del dispositivo en función del estado en el que se encuentra el microcontrolador y el transmisor Bluetooth. Los valores resultantes son los mostrados en la tabla 3, donde se pone en evidencia un elevado consumo en el caso en que ambos están trabajando (microcontrolador despierto y transmisor Bluetooth encendido y transmitiendo), en contraposición a un consumo prácticamente despreciable cuando ambos no están haciendo ninguna tarea (microcontrolador dormido y transmisor Bluetooth apagado).

Estado dispositivo electrónico	**Consumo**
Micro despierto + Transmisor Bluetooth ON (sin transmisión)	20 mA
Micro despierto + Transmisor Bluetooth ON (en transmisión)	47 mA
Micro dormido + Transmisor Bluetooth OFF	18 µA

Tabla. 3. Consumo del dispositivo electrónico según su estado.

Teniendo en cuenta que la batería *CR1/3N* del dispositivo tiene una capacidad nominal de 160mAh, suponiendo una búsqueda inicial de terminales de duración aproximada de 6 segundos y considerando en el peor caso una activación de alarma diaria (típico de un paciente que recibe este tipo de tratamiento) y de 3 segundos de duración de conexión, se puede hacer la siguiente estimación:

$$batería = 160\,mAh = 576000\,mAs \quad (1)$$

$$búsqueda\ terminales = 20\,mA \cdot 3s + 47mA \cdot 3s = 201\,mAs \quad (2)$$

$$alarma\ diaria = 20\,mA \cdot 2s + 47\,mA \cdot 1s = 87\,mAs \quad (3)$$

$$resto\ del\ día = 18\mu A \cdot 86397\,s = 1555{,}146\,mAs \quad (4)$$

Teniendo en cuenta los cálculos 1, 2, 3 y 4, para un uso razonable del dispositivo se obtiene un tiempo de vida del dispositivo electrónico de aproximadamente 1 año:

$$576000mAs = 201mAs + (87mAs + 1555{,}146mAs) \cdot N \quad (5)$$

$$N \approx 350\,días \approx 1\,año \quad (6)$$

VI. Resultados y Conclusiones

Una vez programado el microcontrolador y soldados los componentes electrónicos en la placa, se ha encapsulado de forma hermética para protegerlo de la humedad externa, obteniendo así un prototipo que permite testear su funcionalidad en el sistema global. En la figura 6 pueden verse cuatro prototipos del dispositivo electrónico.

A partir de los prototipos se han realizado pruebas de funcionamiento global del sistema, de cobertura del dispositivo, de tiempo de respuesta de alarma para 1 y 2 terminales móviles y de sensibilidad del sensor de humedad. El rango de cobertura real del dispositivo es de unos 10-15 metros en función del número de obstáculos materiales que se encuentran entre el dispositivo electrónico y el terminal móvil; a más obstáculos menor rango de cobertura como se esperaba dada la naturaleza de Bluetooth. Las pruebas de cambio de sensibilidad han permitido percibir los distintos niveles de sensibilidad del sensor y, por lo tanto, verificar el correcto funcionamiento de la circuitería encargada de tal finalidad. No obstante, la prueba más crítica ha sido la del tiempo de respuesta de alarma que aún siendo satisfactoria está al límite del requisito de tiempo máximo de alarma de 3 segundos para el primer terminal móvil.

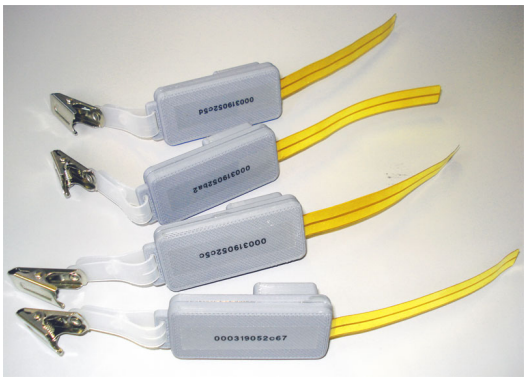


Fig. 6. Prototipo de dispositivo electrónico *PPStop*

Se ha procedido a tomar medidas del tiempo de alarma para el caso de un único terminal móvil a distancia 1m, 5m y 10m, y para el caso de dos terminales móviles en los siguientes casos secundarios: que el primer y segundo móvil están en rango de cobertura y que el primer móvil no esté en rango de cobertura pero el segundo sí. Además, el experimento se ha hecho con dos modelos de terminal móvil distintos para a la vez poder detectar una posible dependencia del modelo de terminal móvil en el tiempo de alarma. Los resultados obtenidos se muestran en la tabla 4.

Modelo	**1 terminal**			**2 terminales**					
				1º ok, 2º ok			**1º ko, 2º ok**		
	1m	**5m**	**10m**	**1m**	**5m**	**10m**	**1m**	**5m**	**10m**
Nokia E50	3100	3330	4800	8700	8940	11160	9170	9680	11680
Nokia 6124	2560	3030	4670	2560	3030	4670	-	-	-

Tabla. 4. Medidas de tiempo de alarma (ms) en función de la distancia, para 1 y 2 terminales

Se puede apreciar como el tiempo de alarma para el primer terminal a 1m de distancia (caso equivalente a que el terminal sea el terminal móvil del paciente) está en torno a los 3 segundos y que además las diferencias de tiempo entre los dos modelos de terminal móvil no representan una diferencia significativa. En cambio las alarmas para distancias superiores incorporan un retardo adicional debido a dicha distancia. De aquí se puede concluir que el tiempo de alarma es suficientemente reducido como para no deteriorar la efectividad del tratamiento, pues el retardo introducido para distancias superiores a 1m no es relevante por no tratarse del paciente quien percibe la alarma.

Referencias

[1] Dr Santiago García-Tornel. Utilidad de las alarmas nocturnas en la enuresis.

[2] Bluetooth SIG. Bluetooth SIG Membership Website.

[3] Infineon Technologies. *XC864 4KB Flash 8-bit Microcontroller Series Product Brief*, 2008.

[4] Infineon Technologies. *eUniStone (BT 2.0 + EDR) PBA31308/2 Product Brief*, 2008.

[5] EEMB Corporation. *CR1/3N Lithium Manganese Dioxide Battery Brief Datasheet*, 2009.

[6] Infineon Technologies. *eBMU PBA31308/2 SPP-AT Application Software Description (Revision 2.0)*, 2008.

[7] Infineon Technologies. *XC86x EK Getting Started*. Examples for XC864, 2008.