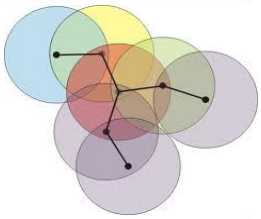
SOLICITUD DE CONTRIBUCIONES

SEGURIDAD EN REDES INALÁMBRICAS AD HOC

Granada – Octubre 2013



Los sistemas inalámbricos se han constituido por derecho propio en el soporte de transmisión más extendido y utilizado hoy en día por los usuarios para sus comunicaciones. Dentro de este tipo de entornos, las redes ad hoc están tomando cada vez más relevancia a lo largo del tiempo, con aplicaciones diversas en ámbitos muy diferentes: militar, medioambiental, industrial, etc. MANETs (*Mobile Ad hoc NETworks*) y WSN (*Wireless Sensor Networks*) son algunos ejemplos característicos de este tipo de redes.

Su naturaleza abierta y ausencia de infraestructura, entre otras características propias, hacen de estos sistemas un entorno especialmente sensible a ataques contra la seguridad de servicios y usuarios. Así, por una parte, riesgos y vulnerabilidades habituales en otras redes se hacen especialmente críticos en los sistemas ad hoc: interferencias (*jamming*), suplantación de identidad, nodos egoístas (*selfish*), etc. Adicionalmente, aparecen otros tipos de ataques más específicos como, por ejemplo, el falseo de rutas multi-salto y, a partir de ello, la alteración de las comunicaciones origen-destino.

En suma, la seguridad, ya de por sí importante en todo entorno de red y comunicaciones, resulta crítica en las redes y sistemas ad hoc; especialmente si tenemos en cuenta que, en ocasiones, los dispositivos involucrados pueden presentar serias limitaciones en cuanto a su capacidad de cómputo, almacenamiento y/o batería.

El objetivo principal de esta solicitud de trabajos, celebrada en el contexto de *JITEL 2013*, es pues, en consecuencia con todo lo anteriormente expuesto, aunar esfuerzos y conseguir avances en la consecución de nuevos logros significativos en relación a aspectos diversos de la seguridad en entornos inalámbricos en general, y en redes ad hoc en particular.

TÓPICOS DE INTERÉS:

Los diversos aspectos a cubrir por los trabajos solicitados se refieren, aunque no se limitan, a los siguientes tópicos principales:

- Autenticación y confianza
- Casos de estudio de comportamiento y prestaciones
- Defensas ante ataques de confabulación
- Detección de actividades ilegítimas
- Esquemas de respuesta y tolerancia
- Esquemas distribuidos para la seguridad
- Estrategias de ataque y modelado
- Localización segura
- Mecanismos de prevención
- Nuevas arquitecturas de seguridad en redes ad hoc
- Protocolos de *routing* seguros
- Seguridad y RoQ
- Supervivencia de sistemas y servicios
- Suplantación de identidad

CONTRIBUCIONES:

Los trabajos deberán ser originales en el campo objeto de estudio y estar escritos en español o inglés correctos, con un estilo comprensible para el lector. El formato y estilo general es el mismo que para *JITEL 2013*, de manera que la información y plantillas correspondientes pueden descargarse de *www.jitel.org*.

El procedimiento de envío de contribuciones a esta solicitud de trabajos será el mismo que el seguido para *JITEL 2013*, debiéndose especificar como única diferenciación el nombre del *workshop*: SERIA.

FECHAS RELEVANTES:

Envío de trabajos: 10 de mayo de 2013
Comunicación de aceptación: 29 de junio de 2013
Trabajos definitivos: 20 de septiembre de 2013

CONTACTO:

Pedro García Teodoro *(pgteodor@ugr.es)*
Dpto. Teoría de la Señal, Telemática y Comunicaciones
ETS Ingenierías Informática y de Telecomunicación
Universidad de Granada
C/ Periodista Daniel Saucedo Aranda, s/n
18071 – Granada (Spain)

JITEL 2013