COMUNICACIONES SEGURAS SOBRE REDES MÓVILES AD HOC

Rocabado,S./Arias Figueroa,D./Sanchez, E.
C.I.D.I.A. (Facultad de Ciencias Exactas.) / Universidad Nacional de Salta
Dirección: Av. Bolivia 5150 – Salta Capital (4400)
Tel.: +543874258614
Mail: srocabad@cidia.unsa.edu.ar;daaf@cidia.unsa.edu.ar; esanchez@cidia.unsa.edu.ar

RESUMEN

En este proyecto se ha planteado investigar diferentes mecanismos para realizar comunicaciones seguras utilizando redes móviles ad-hoc, esto permitirá aprovechar las características inherentes de este tipo de redes, para llevar información crítica de forma segura a lugares donde no se disponga de acceso a redes de infraestructura.

El resultado final será una propuesta que servirá de base para el desarrollo e implementación de sistemas móviles para emergencias médicas y también como material de consulta para futuras implementaciones seguras sobre redes móviles ad-hoc y/o entornos que requieran integrar MANETs a redes de infraestructura.

Palabras clave:
Redes Móviles Ad Hoc, Seguridad, MANET, Movilidad.

CONTEXTO

El presente proyecto de investigación: "*Comunicaciones Seguras sobre Redes Móviles Ad Hoc*", se desarrolla en el ámbito del C.I.D.I.A. – Centro de Investigación y Desarrollo en Informática Aplicada dependiente de la Facultad de Ciencias Exactas de la Universidad Nacional de Salta.

1. INTRODUCCION

Las Redes Móviles Ad Hoc (o MANETs, del inglés Mobile Adhoc NETworks) son un tipo de redes inalámbricas donde no es necesaria ninguna infraestructura previa para comunicarse a través de la red. Los equipos o nodos que forman parte de ella (Notebooks, PDAs, Celulares), se organizan por si mismos para ayudarse los unos a los otros en el proceso de transportar paquetes de datos entre un origen y un destino.

Las MANET constituyen una tecnología ideal para el establecimiento instantáneo de la comunicación entre nodos que son móviles y en lugares en donde no es posible construir un backbone de comunicaciones debido a inconvenientes físicos y/o económicos o a la falta de tiempo para la construcción de la infraestructura requerida. Esta tecnología es especialmente útil en escenarios que requieren de estrategias rápidas y eficientes de comunicación, como son las operaciones de emergencias en caso de incendios, inundaciones y cualquier otro tipo de accidente que requiera asistencia médica en sitio. En la mayoría de estos accidentes, resulta de mucha utilidad llevar la información del paciente al sitio, brindándole al profesional la posibilidad de tomar decisiones sin necesidad de trasladar al paciente (por el riesgo que esto implica) hasta un lugar que disponga de la infraestructura necesaria para acceder al sistema de información.

Debido a la criticidad y sensibilidad de la información que se almacena en la base de datos de historias clínicas, es necesario utilizar protocolos de seguridad en la capa de transporte que permitan garantizar una comunicación segura entre un nodo fijo de la intranet (servidor) y un nodo móvil (cliente).

En la figura 1 se plantea un escenario de estudio, en el se observa la posibilidad de acceder desde un equipo móvil en zona de emergencia (sin cobertura de red) a un servidor conectado a la intranet, utilizando

para esto 2 MANETs y una red GSM/GPRS como medios de comunicación intermedios.

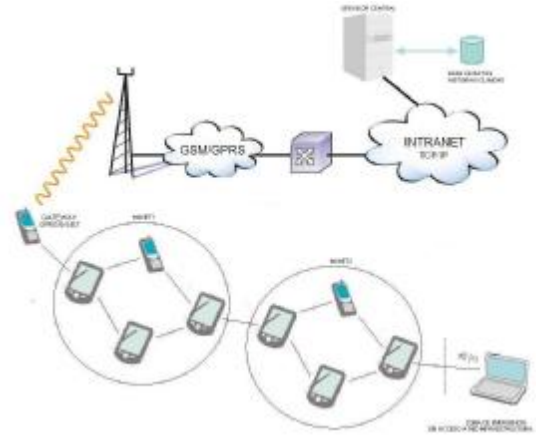

Figura 1

El nodo móvil que inicialmente se encontraba conectado a la intranet mediante una WLAN se desplazo a un área donde no existe cobertura de señal, entonces debe reconfigurarse a si mismo en modo ad hoc y vincularse a una MANET que le permita llegar a un nodo con acceso a la red GPRS y luego a la intranet.

Debido a la criticidad y sensibilidad de la información que se almacena en la base de datos de historias clínicas, es necesario utilizar protocolos de seguridad en la capa de transporte que permitan garantizar una comunicación segura (confidencialidad, integridad, autenticación, no repudio y disponibilidad) entre un nodo fijo de la intranet (servidor) y un nodo móvil (cliente).

La tabla 1 muestra ejemplos de protocolos seguros que pueden ser utilizados por las aplicaciones en cada tecnología de red involucrada en el caso de estudio. Si alguno de los protocolos de la tabla es utilizado en una tecnología de red para la cual no fue diseñado, puede no funcionar correctamente y degradar considerablemente la performance general de toda la red. Para solucionar este inconveniente aparecen dos opciones, la primera es utilizar gateways de seguridad que realicen la conversión y/o adaptación de los protocolos (Ej: Gateway GPRS/MANET) y la segunda es una solución end to end entre el servidor de base de datos y el nodo remoto.

Intranet TCP/IP	TLS (rfc 5246) y una infraestructura de clave pública (PKI) centralizada con autoridad de certificación centralizada (X.509 – rfc 2459).
GSM/GPRS	WTLS (rfc 2636) y una infraestructura de clave pública (PKI) centralizada con autoridad de certificación centralizada (X.509 – rfc 2459).
MANETs	Infraestructura de claves distribuida basada en un modelo de confianza PGP (“web of trust” - rfc 4880) con autoridad de certificación (CA) distribuida.

Tabla 1

Debido a la naturaleza dinámica de las MANETs no podemos asegurar a priori cual de las dos opciones se adapta mejor al escenario planteado, por esta razón se hace necesario estudiar y comparar las diferentes alternativas, para determinar cual es la más conveniente.

2. LINEAS DE INVESTIGACION y DESARROLLO

Los principales ejes temáticos, que abarca la investigación de este proyecto, son los siguientes:

- Redes móviles ad-hoc.
- Seguridad en redes móviles ad-hoc.
- Protocolos seguros a nivel transporte en redes TCP/IP, GSM/UMTS y MANET.
- Sistemas distribuidos de gestión de claves asimétricas.
- Autoridades de certificación distribuidas.

3. RESULTADOS Y OBJETIVOS

Los objetivos de este proyecto de investigación, son los siguientes:

- Presentar una propuesta de comunicaciones seguras en la capa de transporte para redes móviles ad-hoc.

- Presentar alternativas para integración de comunicaciones seguras a nivel transporte

entre redes de infraestructura y redes móviles ad-hoc.

- Realizar una comparación de las alternativas presentadas en diferentes escenarios de comunicación.

El trabajo resultante va generar un aporte para el desarrollo de aplicaciones seguras sobre redes móviles ad hoc, sirviendo de base para futuras implementaciones.

4. FORMACION DE RECURSOS HUMANOS

La estructura del equipo de investigación es de 5 (cinco) miembros incluidos el Director y un Asesor.
Uno de sus miembros se encuentra realizando el trabajo de tesis de postgrado denominado: "Caso de estudio de comunicaciones seguras sobre redes móviles Ad Hoc", para la obtención del Magister en Redes de Datos de la Universidad Nacional de La Plata.
Otro de los miembros se encuentra desarrollando su Seminario de Sistemas titulado "Sistema móvil para emergencias médicas" en la Licenciatura en Análisis de Sistemas de la Universidad Nacional de Salta.

5. REFERENCIAS

[1] AD HOC NETWORKING. Charles E. Perkins. Ed. Addison-Wesley. Edición 2008. ISBN: 9780321579072

[2] SECURITY AND QUALITY OF SERVICE IN AD HOC WIRELESS NETWORKS. Amitabh Mishra. Ed. Cambridge University Press. Edición 2008. ISBN: 978-0-511-38813-2

[3] SECURITY FOR WIRELESS AD HOC NETWORKS. Farooq Anjum and Petros Mouchtaris. Ed John Wiley & Sons. Edición 2007. ISBN: 978-0-471-75688-0

[4] SECURITY IN AD-HOC NETWORKS. AK Bayya, S Gupte, YK Shukla, A Garikapati. Computer Science Department University of Kentucky

[5] Tesis doctoral: SECURITY PROTOCOLS FOR MOBILE AD HOC NEWORKS. Carlton R. Davis. McGill University - Montreal.