Seguridad en MANETs

Javier Echaiz Pablo M. Davicino* Jorge R. Ardenghi

Laboratorio de Investigación de Sistemas Distribuidos (LISiDi)
LISIDI es un miembro del IICyTI (Instituto de Investigación en Ciencia y Tecnología Informática).
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Av. Alem 1253 - (8000) Bahía Blanca - Argentina
Tel/Fax: (+54) 291-4595135/6
{je,pmd,jra}@cs.uns.edu.ar

Resumen

Las MANETs (*Mobile ad hoc networks*) pueden definirse como una gran colección de nodos móviles que conforman una red temporal pero sin la ayuda de ninguna infraestructura de red o *access point* central. Cada nodo participante de la red actúa al mismo tiempo como host y como router y debe por lo tanto reenviar paquetes para otros nodos. Las características de las MANETs incluyen: topología dinámica, movilidad de los nodos y capacidad de autoorganización.

Esta línea de investigación explorará la problemática de seguridad (todavía abierta) para el diseño y desarrollo de protocolos seguros aplicables a estos ambientes de comunicación distribuidos, abiertos e inalámbricos.

Palabras clave: seguridad, MANET, redes inalámbricas, redes de sensores.

Contexto

El trabajo objeto del presente artículo se desarrolla en el Laboratorio de Investigación en Sistemas Distribuidos (LISiDi) del Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur.

La línea de investigación presentada es parte del Proyecto "Computación Distribuida de Alto Rendimiento y Disponibilidad" (24/N024) dirigido por el Mg. Jorge Ardenghi y codirigido por el Dr. Javier Echaiz. Este proyecto se encuentra financiados por la Secretaria General de Ciencia y Tecnología de la Universidad Nacional del Sur, y se encuentra acreditados por la Universidad Nacional del Sur, Bahía Blanca.

*Becario CONICET.

Introducción

Las redes inalámbricas usuales, como por ejemplo las de telefonía celular, operan con la ayuda de un *access point* central que mantiene a los usuarios conectados al sistema. En estos sistemas los dispositivos se comunican por radio, compartiendo recursos e información, sin embargo la adaptabilidad de estos sistemas es limitada debido a la infraestructura fija que les da soporte. Los avances recientes en tecnología inalámbrica, como Bluetooth e IEEE 802.11 introdujeron un nuevo tipo de sistema inalámbrico conocido como *Mobile ad-hoc network* (MANET), el cual opera sin el empleo de un access point central y brinda a los nodos un mayor grado de flexibilidad (autoconfiguración y automantenimiento), portabilidad y movilidad que los sistemas tradicionales. En la Figura 1 se muestra un ejemplo de una MANET. Sin embargo, también presentan los siguientes inconvenientes:

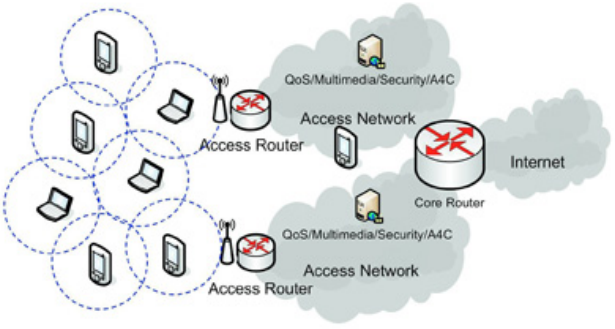

Figura 1: Ejemplo de una MANET

- Débiles en cuanto a seguridad (medio compartido, arquitectura abierta, topología dinámica).
- Restricciones de recursos, e.g. de CPU, de energía.

- Bajo ancho de banda y transferencias de datos lentas.

Los objetivos de seguridad de las MANETs no son distintos a los de cualquier sistema que requiera seguridad:

- Autenticación (autorización y gestión de claves).
- Integridad.
- Confidencialidad.
- No repudio.

Dentro de las características de las MANETs podemos incluir:

Terminal autónoma. Cada terminal móvil es un nodo autónomo, el cual funciona como host pero también como router. Por lo tanto los endpoints y los switches son indistinguibles.

Terminal liviana. Los nodos son dispositivos móviles con escasos recursos de hardware: CPU, memoria y almacenamiento de energía.

Operación distribuida. El control y la gestión de la red se encuentra distribuida entre los nodos participantes.

Ruteo multihop. Podemos tener MANETs de un único hop (conexión directa) o multihop, la primera es más sencilla en cuanto a estructura e implementación pero presenta menos funcionalidad y aplicabilidad que las de ruteo multihop.

Topología dinámica. Dado que los nodos son móviles, la red puede cambiar rápidamente y en forma no predecible y por lo tanto la conectividad entre nodos puede variar. Las MANETs deben adaptarse al dinamismo en las condiciones de tráfico, movilidad y propagación.

Aplicación

El aumento en el uso de dispositivos portables y el progreso en las comunicaciones inalámbricas constituyen dos factores que vuelven a las redes ad hoc muy populares en la actualidad. Su aplicabilidad incluye:

- Campo de batalla (uso militar).
- Redes de sensores inalámbricas (WSN).
- Ámbito comercial.
- Servicio médico.
- Trabajo colaborativo.
- Redes de área personal (PANs).

Ruteo

Comparado con el ruteo en redes cableadas tradicionales, el ruteo en redes móviles ad hoc encuentra desafíos adicionales. Existen numerosos protocolos de ruteo en la literatura para hacer frentes a las limitaciones que presentan estos ambientes ad hoc. El problema del ruteo en entornos de este tipo se encuentra agravado por las topologías rápidamente cambiantes, alto consumo de energía (baterías), bajo ancho de banda y frecuentes errores en las comunicaciones.

Línea de Investigación y Desarrollo

Los protocolos de ruteo actuales para redes ad hoc asumen que los nodos participantes actúan de buena fe y sin intención maliciosa de afectar la operación del protocolo. Sin embargo, la existencia de entidades maliciosas no puede negarse en ningún sistema, especialmente bajo redes ad hoc abiertas. En una red ad hoc la función de ruteo puede ser atacada tanto por nodos internos (terminales legítimas) como externos. Es posible emplear mecanismos criptográficos para minimizar el riesgo que traen aparejados los atacantes externos, por ejemplo mediante autenticación mutua de los nodos participantes. Sin embargo, los protocolos subyacentes también deben ser considerados, pues un atacante podría manipular un protocolo de una capa más baja para afectar un mecanismo de seguridad en una capa de más alto nivel. Los atacantes internos cuentan con la capacidad de acceder al enlace de comunicación y disparar, por ejemplo, falsos mensajes de información de ruteo, forzando decisiones de ruteo arbitrarias sobre sus pares.

Los nodos maliciosos pueden atacar a diferentes niveles (capas): física, enlace, red, y aplicación. A su vez, los ataques pueden clasifican en activos y pasivos; ejemplos del primero grupo son spoofing, fabricación, modificación, *denial of service* (DoS), y ejemplos de ataques pasivos incluyen *eavesdropping*, análisis de tráfico y monitoreo. Ejemplos de ataques en la capa de red son los ataques de ruteo, donde el atacante trata de corromper las tablas de ruteo de los nodos víctima (efecto remoto), o los ataques de *forwarding*, donde no son afectadas las tablas de ruteo sino que se modifica la entrega de

los paquetes (efecto local), también pueden explotarse vulnerabilidades en los protocolos, etc. Ataques en la capa enlace incluyen los ataques al mecanismo de gestión de claves, *denial of service*, etc. El escenario se vuelve aún más difícil si consideramos que los ataques podrían ser no intencionales, como por ejemplo un error de configuración.

Existen varias propuestas de protocolos de ruteo seguro para MANETs, e.g. los de ruteo proactivos DSDV, TBRPF, WRP, OLSR y los de ruteo reactivo DSR, TORA, ADOV. Los de ruteo proactivo emplean estrategias clásicas de ruteo, como por ejemplo el monitoreo del estado del enlace y el cómputo de vectores de distancia; además llevan registro de las rutas hacia todos los posibles destinos y actualizan periódicamente los cambios de estado de los enlaces, de esta forma si bien las demoras son mínimas, como contrapartida debe almacenarse mucha información de control. En cambio, los protocolos de ruteo reactivo, descubren por demanda las rutas hacia los nodos destino, ahorrando ancho de banda pero experimentando mayores demoras. Además de la clasificación entre sistemas de ruteo proactivo y reactivo, los protocolos de ruteo seguro también pueden clasificarse según sus mecanismos criptográficos subyacentes: simétricos (e.g. SEAD y SRP), asimétricos (e.g. ARAN y SAR) o híbridos (e.g. SAODV).

Es claro que el ruteo es una función esencial de las redes ad hoc y por lo tanto los mecanismos de seguridad no deben dificultar su operación. Además deben tenerse en cuenta las asunciones y los requerimientos de cada aplicación, por ello es importante satisfacer las correspondientes restricciones de seguridad pero al mismo tiempo tener en cuenta que se debe minimizar el *overhead* para que el sistema siga siendo viable.

Resultados y Objetivos

Esta línea de I+D espera conseguir resultados que tiendan a solucionar los problemas de seguridad actuales en las MANETs. Para ello se espera desarrollar un nuevo protocolo de seguridad bajo las siguientes restricciones:

Liviano. Si bien es fundamental que sea seguro también debe tener bajo overhead para evitar pérdidas significativas de performance.

Multicapa. Es importante contemplar soluciones multicapas para lograr una solución de seguridad completa.

Distribuido y con ruteo multihop. Sin nodos 'especiales' (arquitectura peer-to-peer pura), el ruteo multihop maximiza la aplicabilidad y flexibilidad del sistema.

Asunción de nodos egoístas. El sistema debe garantizar un mecanismo de incentivos que favorezca la cooperación entre nodos. En este ítem también consideraremos grupos de nodos y el concepto de confianza.

Ruteo reactivo. El ruteo se efectúa por demanda, i.e. las rutas hacia los destinos se conocen sólo por demanda, con lo cual si bien se agregan delays también se minimiza el consumo de ancho de banda.

Tolerante a fallas/intrusiones. Soportar operación ante la ocurrencia de fallas e intrusiones originadas en nodos participantes aumenta el nivel de seguridad del sistema.

Sistema de detección de intrusos (IDS). Monitorear nodos vecinos y rutas en busca de comportamientos anómalos. La naturaleza inherentemente dinámica de las MANET vuelve este ítem desafiante.

Se espera entonces poder desarrollar un protocolo capaz de proveer ruteo y forwarding seguros, que mediante mecanismos criptográficos abiertos y probados provea primitivas de autenticación seguras. Además debe ser capaz de llevar la tolerancia a fallas tan lejos como sea posible, no sólo debe poder minimizar/mitigar ataques sino también soportar fallas, errores de configuración y sobrecargas en la red. Para ello deberemos complementar los mecanismos criptográficos con redundancia de conectividad y de ruteo (a nivel de sistema y de protocolo). Las soluciones proactivas por si mismas no pueden ser capaces de eliminar ataques mediante mecanismos seguros en la capa enlace y de red, es por ello que proponemos la inclusión de tecnología de IDS como segunda línea de defensa, asumiendo que tanto las aplicaciones como el comportamiento de los usuarios es observable y que por ello es posible poder diferenciar entre actividades normales e intrusiones.

Es claro que el desarrollo de un protocolo de seguridad para MANETs que incluya estos objetivos en forma simultánea es muy ambicioso, sin embargo se vuelve factible debido a la existencia de componentes de hardware cada vez más potentes, lo que permite soluciones más complejas y efectivas.

Los objetivos de esta línea incluyen el diseño de subsistemas de seguridad que cumplan con las necesidades planteadas y sean potencialmente adaptables a distintas necesidades de las MANETs. Inicialmente se espera lograr una validación exitosa de nuestra propuesta mediante simulación.

Formación de Recursos Humanos

Este trabajo corresponde a una de las principales líneas de investigación del Laboratorio de Investigación en Sistemas Distribuidos (LISiDi) de la Universidad Nacional del Sur. La misma será objeto de estudio de diversas tesinas de grado de las carreras de Ingeniería en Sistemas de Computación y Licenciatura en Ciencias de la Computación, ambas dictadas por el Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur y posiblemente se extienda a varios trabajos de postgrado (actualmente forma parte del trabajo de una tesis de Magíster).

A su vez, el LISiDi cuenta con recursos propios, sobre los cuales se despliegan los distintos componentes que permiten trabajar con los sistemas objetos de este estudio. Si bien es posible trabajar en cuestiones de seguridad distribuida sin la necesidad de contar con sistemas distribuidos de gran escala (que se encuentren dispersos geográficamente) es cierto que para validar los modelos propuestos es interesante que los entornos sean efectivamente distribuidos, permitiendo probar los sistemas bajo diferentes dominios organizativos, diferentes CAs (con cadenas de certificación no triviales), atravesando firewalls, etc. Para ello se trabajará en forma colaborativa con otras Universidades, especialmente con el LIDI de la Facultad de Informática de la Universidad Nacional de La Plata, junto con quienes se ha trabajado exitosamente en cuestiones de computación grid.

A continuación se mencionan los cursos de pregrado relacionados con la línea de investigación presentada, dictados por los integrantes del grupo de investigación:

- Seguridad en Sistemas. Materia obligatoria para los estudiantes de la carrera de Ingeniería en Sistemas de Computación, y optativa para los de Licenciatura en Ciencias de la Computación, Universidad Nacional del Sur.
- Sistemas Operativos. Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas de Computación, Universidad Nacional del Sur.
- Sistemas Distribuidos. Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas de Computación, Universidad Nacional del Sur.
- Sistemas Operativos y Distribuidos. Materia obligatoria para los estudiantes de la carrera Licenciatura en Ciencias de la Computación, Universidad Nacional del Sur.
- Paradigmas de Computación Paralela y Distribuida. Materia optativa para los estudiantes de las carreras Licenciatura en Ciencias de la Computación e Ingeniería en Sistemas de Computación, Universidad Nacional del Sur.
- Sistemas Distribuidos I. Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas, Facultad de Ingeniería, Universidad Nacional de la Pampa. Esta materia actualmente se dicta por docentes de la propia Facultad de la UNLPam.
- Sistemas Distribuidos II. Materia obligatoria para los estudiantes de la carrera Ingeniería en Sistemas, Facultad de Ingeniería, Universidad Nacional de la Pampa. Esta materia actualmente se dicta por docentes de la propia Facultad de la UNLPam.

Asimismo se han dictado cursos de posgrado relacionados con Seguridad de la Información y Sistemas Distribuidos (especialmente referidos al paradigma grid y peer-to-peer) en varias Universidades Nacionales.

Referencias

[1] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam. Addressing security concerns of data exchange in aodv protocol, 2006.

[2] Todd R. Andel and Alec Yasinsac. Surveying security analysis techniques in MANET routing protocols. *IEEE Communications Surveys and Tutorials*, 9:70–84, 2007.

[3] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru, and Herbert Rubens. ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. *ACM Trans. Inf. Syst. Secur.*, 10:6:1–6:35, January 2008.

[4] Mike Burmester and Breno de Medeiros. On the Security of Route Discovery in MANETs. *IEEE Transactions on Mobile Computing*, 2008.

[5] L. Buttyán and Ta Vinh Thong. Formal verification of secure ad-hoc network routing protocols using deductive model-checking. In *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, pages 1 –6, oct. 2010.

[6] Vee Liem Chee and Wei Chuen Yau. Security analysis of tora routing protocol. In *Proceedings of the 2007 international conference on Computational science and Its applications - Volume Part II*, ICCSA'07, pages 975–986, Berlin, Heidelberg, 2007. Springer-Verlag.

[7] Chee-Yee Chong and S.P. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, Aug. 2003.

[8] Vinu V Das, editor. *Simulation Based Routing Protocols Evaluation for IEEE 802.15.4 enabled Wireless Sensor Networks*, volume 2 of *3*, 1133 Broadway,Suite 706,New York,NY10010,USA, july 2011. Institute of Doctors Engineers and scientist(IDES), The Association of Copmuter Electronics and Electrical Engineers.

[9] Hongmei Deng, Wei Li, and D.P. Agrawal. Routing security in wireless ad hoc networks. *Communications Magazine, IEEE*, 40(10):70 – 75, October 2002.

[10] D. Dhillon, T.S. Randhawa, M. Wang, and L. Lamont. Implementing a fully distributed certificate authority in an OLSR MANET. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, volume 2, pages 682 – 688 Vol.2, march 2004.

[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.*, 11(1-2):21–38, January 2005.

[12] Jean-Pierre Hubaux, Levente Buttyán, and Srdjan Capkun. The quest for security in mobile ad hoc networks. In *MobiHoc*, pages 146–155, 2001.

[13] Nurul Md. Huda, Shigeki Yamada, and Eiji Kamioka. Routing cost versus network stability in manet. In Pascal Lorenz and Petre Dini, editors, *ICN (2)*, volume 3421 of *Lecture Notes in Computer Science*, pages 218–225. Springer, 2005.

[14] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. *Wireless Communications, IEEE*, 14(5):85 –91, October 2007.

[15] Zhi Li and Yu-Kwong Kwok. A new multipath routing approach to enhancing tcp security in ad hoc wireless networks. In *ICPP Workshops*, pages 372–379. IEEE Computer Society, 2005.

[16] Wenjing Lou, Wei Liu, Yanchao Zhang, and Yuguang Fang. Spread: Improving network security by multipath routing in mobile ad hoc networks. *Wireless Networks*, 15(3):279–294, 2009.

[17] Jeongseo Park, Jinsoo Cho, and Taekeun Park. The impact of disjoint multiple paths on sctp in the connected manet for emergency situations. *IEICE Transactions*, 95-B(3):1011–1014, 2012.

[18] Vincent D. Park and M. Scott Corson. A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing. In *In proceedings of IEEE International Symposium on Systems and Communications. IEEE Computer*, pages 592–598. Society Press, 1998.

[19] K Sanzgiri, B Dahill, B N Levine, C Shields, and E M Belding-Royer. A secure routing protocol for ad hoc networks. *10th IEEE International Conference on Network Protocols 2002 Proceedings*, 02(UM-CS-2002-032):78–87, 2002.

[20] Nadir Shah, Depei Qian, and Rui Wang. Manet adaptive structured p2p overlay. *Peer-to-Peer Networking and Applications*, 5(2):143–160, 2012.

[21] M. K. Soni, P.K. Suri, and Parul Tomar. Article: A comparative study for secure routing in manet. *International Journal of Computer Applications*, 4(5):17–22, July 2010. Published By Foundation of Computer Science.

[22] Frank Stajano and Ross J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Security Protocols Workshop*, pages 172–194, 1999.

[23] Xiaoxin Wu and David K. Y. Yau. Mitigating denial-of-service attacks in manet by incentive-based packet filtering: A game-theoretic approach. In *SecureComm*, pages 310–319. IEEE, 2007.

[24] Li Yang, Alma Cemerlic, and Xiaohui Cui. A dirichlet reputation system in reliable routing of wireless ad hoc network. *Security and Communication Networks*, 3(2-3):250–260, 2010.

[25] Shushan Zhao, A. Aggarwal, Shuping Liu, and Huapeng Wu. A Secure Routing Protocol in Proactive Security Approach for Mobile Ad-Hoc Networks. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pages 2627 –2632, April 2008.

[26] Gergely Ãcs, Levente ButtyÃ¡n, and IstvÃ¡n Vajda. Provable security of on-demand distance vector routing in wireless ad hoc networks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *ESAS*, volume 3813 of *Lecture Notes in Computer Science*, pages 113–127. Springer, 2005.