DETECCIÓN DE INTRUSOS Y SEGURIDAD EN REDES MÓVILES AD-HOC

Carlos Felipe Téllez Castaño
Universidad Nacional de Colombia
Seminario de Investigación
cftellezc@unal.edu.co

ABSTRACT
Cuando hablamos de Redes Móviles Ad-Hoc, estamos hablando de una tecnología reciente que consiste en redes de topología dinámica inalámbrica, sin una estructura fija y que son muy útiles a la hora de comunicar diferentes estaciones o conocidos nodos de comunicación que interactúan, como enrutadores. Frente a esta descripción, nos encontramos con algunas características limitantes que hacen de las redes inalámbricas Ad-Hoc, muy vulnerables al acceso de intrusos y ataques que pueden dañar la integridad de la red. Características tales como la limitada capacidad de proceso en los nodos, un ancho de banda limitado y una interacción que requiere que cada nodo se involucre en la toma de decisiones de la red hacen de este tipo de redes un estudio exhaustivo de la misma. Este Estado del Arte hace referencia a la seguridad en este tipo de redes, involucrando las distintas técnicas de computación estudiadas hasta el momento para suplir esta necesidad, como lo son los sistemas de detección de intrusos (IDS), la seguridad en el enrutamiento y la autenticación de acceso a través de la administración de claves.

Categorías
Introducción a redes Ad-Hoc, Protocolos de enrutamiento, Seguridad en redes Ad-Hoc, Sistemas de detección de intrusiones, Seguridad de los protocolos de enrutamiento, Autenticación de acceso a través de la administración de claves.

Keywords
MANET, Seguridad Ad-Hoc, IDS, Agentes Móviles.

1. INTRODUCCIÓN
Una red móvil Ad-Hoc, también conocida como MANET (Mobile Ad-Hoc Network) consiste en un conjunto autónomo y espontáneo de Routers o Nodos móviles que se comunican entre sí a través de conexiones wireless, dónde no existe una infraestructura de red fija y la gestión se realiza de forma distribuida. Dichos nodos tienen libertad de movimiento, y su topología física cambia precipitadamente y de forma impredecible. Es así como los nodos hacen parte de la toma de decisiones, ejecutando las actividades propias del mantenimiento de la red y tomando parte en los algoritmos de enrutamiento y de seguridad.

El termino *Ad-Hoc*, aunque podría ser interpretado con connotaciones negativas tales como “improvisado” o “desorganizado”, en el contexto de las redes inalámbricas hace referencia a redes flexibles, en las cuales todos los nodos ofrecen servicios de enrutamiento para permitir la comunicación de nodos que no tienen conexión inalámbrica directa. Con relación a las redes cableadas, las redes *Ad-Hoc* presentan cambios de topología frecuentes e impredecibles debido a la movilidad de sus nodos. Estas características impiden la utilización de protocolos de enrutamiento desarrollados para redes cableadas y crean nuevos retos de investigación que permitan ofrecer soluciones de enrutamiento eficientes que superen problemas tales como topología dinámica, recursos de ancho de banda y batería limitada y seguridad reducida.

Los protocolos de enrutamiento desarrollados para redes cableadas no se adaptan al entorno altamente dinámico de las redes *Ad-Hoc*. Dichos protocolos hacen uso de mensajes de actualización de rutas periódicos que ofrecen una elevada sobrecarga incluso en redes con tráfico reducido. Esta metodología de diseño hace que en entornos dinámicos con cambios de topología frecuente dichas aproximaciones ofrezcan una sobrecarga excesiva.

Es aquí donde entramos al punto clave de este estado del arte, que es precisamente, la seguridad en las redes Ad-Hoc. A las limitaciones de estas redes móviles, que se convierten en una tecnología necesaria para la tendencia actual, se debe sumar el alto nivel de vulnerabilidad que se tiene con respecto a las intrusiones de nodos que no hacen parte de la red. La seguridad es un tema que se hace participe en este tipo de redes como tema de investigación, pues es necesario integrar a los distintos protocolos de enrutamiento, las técnicas necesarias para garantizar una red segura MANET.

En este Estado del Arte, primero se hará un reconocimiento breve a las distintas técnicas de enrutamiento que se trabajan sobre redes MANET, ya que es necesario tener en cuenta que cualquier tipo de técnica de detección de intrusos debe desempeñar su funcionalidad sobre un protocolo de enrutamiento que dirija el proceso de distribución de tareas de seguridad. Después se hará mención a la seguridad en general con redes MANET, teniendo en cuenta las metodologías usadas que son los sistemas de detección de intrusos, la seguridad de los protocolos de enrutamiento y los servicios de gestión de claves. Por ultimo se mencionan las conclusiones junto a las referencias.

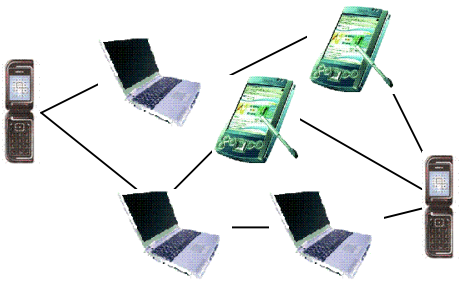

Figura 1: Red Ad-Hoc personal de dispositivos pequeños móviles

2. ENRUTAMIENTO

Los protocolos de enrutamiento en redes Ad-Hoc se pueden dividir en tres grupos: proactivos, reactivos y basados en cluster. Los protocolos proactivos son aquellos que mantienen una ruta hacia todos los nodos, aunque en ese momento no se utilicen. El caso de los protocolos reactivos intenta optimizar el uso de ancho de banda descubriendo la ruta hacia un destino sólo en el caso en que sea necesario enviar un paquete. Finalmente los protocolos basados en cluster son una mezcla de los dos tipos que hemos visto, y se basan en definir jerarquías entre los nodos de la red y mantener información sobre la topología local.

Un protocolo de enrutamiento con capacidades de Calidad del Servicio debería intentar establecer una ruta que satisficiese determinados requisitos de ancho de banda, retardo, jitter, etc. Sin embargo, la topología dinámica presente en redes Ad-Hoc hace que asegurar estos parámetros sea una tarea muy complicada. Inicialmente los protocolos reactivos serían más interesantes gracias a su menor uso de recursos de red (escasos en redes Ad-Hoc). Probablemente este sea uno de los campos donde menos trabajo se ha realizado, si bien existen ciertas iniciativas con un futuro prometedor.

Hace un par de años se estaban evaluando entre la comunidad investigadora cerca de 60 propuestas de enrutamiento diferentes. Sin embargo, hoy día solamente cuatro de estas propuestas han resistido la fuerte competencia. Estas propuestas son las siguientes: el protocolo “Ad-Hoc On Demand Distance Vector” (AODV), el protocolo “Dynamic Source Routing for Protocol Mobile Ad-Hoc Networks” (DSR), el protocolo “Optimized Link State Routing Protocol” (OLSR), y el protocolo “Topology Broadcast based on Reverse-Path Forwarding” (TBRPF). De estos cuatro, los protocolos AODV y OLSR han alcanzado el nivel de RFC (*Request for Comment*). AODV y DSR utilizan enrutamiento reactivo también conocido como enrutamiento bajo demanda, en el cual las rutas a utilizar para un determinado destino solamente se calculan cuando éstas son necesarias.

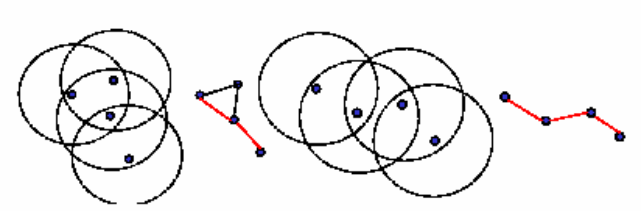

Figura 2: Enrutamiento AODV

Estos protocolos, intentan reducir así la sobrecarga generada por los mensajes de actualización de rutas periódicos. El principal inconveniente de los protocolos reactivos es el retardo inicial que introducen y que puede representar una seria limitación en aplicaciones interactivas que requieren asegurar determinada calidad de servicio (ej. audio y video interactivo). Por su parte, OLSR y TBRPF utilizan enrutamiento proactivo en los cuales todas las rutas a todos los posibles destinos se calculan a priori, y además, éstas se mantienen actualizadas en todo momento utilizando para ello mensajes de actualización periódicos. Estos protocolos introducen cierto nivel de sobrecarga, sin embargo, presenta la ventaja de poder seleccionar rutas válidas de forma prácticamente inmediata. Los protocolos anteriormente citados ofrecen soluciones de enrutamiento en el nivel de enlace.

3. SEGURIDAD

Hablar de seguridad en redes Ad-Hoc, es hablar de un gran desafío en la investigación de la ciencia de la computación, ya que involucra el surgimiento y aplicación de modelos y técnicas que sean capaces de sustentar la vulnerabilidad al acceso de este tipo de redes con topología dinámica. Para poder determinar cuales son esos modelos computacionales, se debe tener en cuenta en primera medida, cuales serian los requisitos que deberían cumplir este tipo de técnicas computacionales de fortalecimiento de seguridad en las redes Ad-Hoc. Al igual que las redes cableadas, las redes MANET deben cumplir con los criterios de integridad, autenticación, no repudiación y disponibilidad.

No obstante, esto resultaría un poco más sencillo, si no se tuvieran en cuenta las particularidades habituales de una red Móvil Ad-Hoc de topología variable, conexiones con anchos de banda escasos y de capacidad inestable, limitaciones de energía, capacidad de procesamiento en los nodos y vulnerabilidad a los ataques provenientes de las intrusiones. Esto sin mencionar, que lo más optimo sería plantear una solución General en términos de seguridad donde todos las limitaciones de este tipo de redes móviles, no afecten la integridad de la red, y se convierta en un tipo de comunicación seguro y confiable, y no tener en cuenta muchas particularidades siendo suplidas en forma independiente.

Es por eso, que ha este punto y sólo en la actualidad, sería una locura (tal vez en un futuro muy cercano no lo sea), hablar de un estándar de seguridad que cubra cualquier desempeño en redes MANET, teniendo en cuenta que redes MANET no sólo son las redes personales de dispositivos móviles pequeños, como PDA’s, Portátiles,

Celulares, etc., sino que también hacen parte las redes satelitales, militares, de medios de transporte, y de gran escala en comunicaciones, donde las exigencias (junto al presupuesto financiero a invertir) son mucho mayores.

Cuando se hace referencia a un estándar, se menciona un desarrollo de protocolos o modelos computacionales que sean aplicables en cualquier tipo de red Ad-Hoc, pero en este caso es necesario tener en cuenta el entorno y la estructura de la red para determinar sus posibles aplicaciones y combatir cualquier tipo de ataque, intrusión o disrupción. Sin embargo, los requerimientos de seguridad para cualquier estructura Ad-Hoc, deberían ser compartidos, pues las exigencias, aunque no son las misas, deben conllevar aspectos que se deben cumplir para garantizar la seguridad en redes dinámicas. En la investigación [1] se ha encontrado que esos aspectos son: Los Sistemas de Detección de Intrusos (IDS), La seguridad en los protocolos de enrutamiento y la autenticación de acceso a través de la administración de claves.

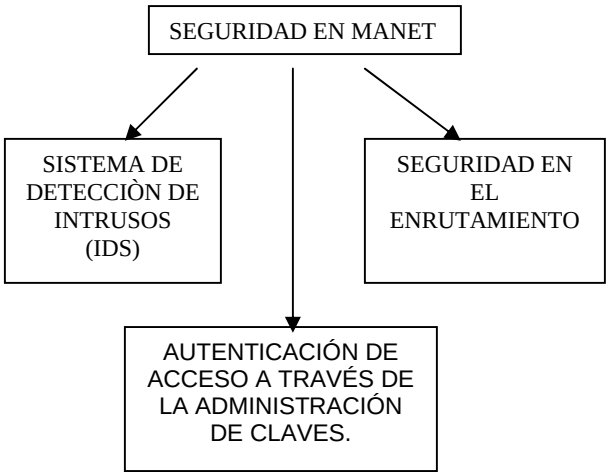

Figura 3: Modelos computacionales usados para la seguridad en redes MANET.

3.1 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Un intruso, en una red Ad-Hoc, consiste en un nodo (dispositivo móvil, medio de transporte, satélite, etc.) que irrumpe en una red privada, a la que no pertenece, y accede a los datos y a la información que circula en dicha red. Su ingreso ilícito a la red, no es garantía de una fácil detección, teniendo en cuenta que se adquiere un acceso inalámbrico que constantemente cambia de topología. Además, una posible detección no es indemnidad para la red, pues es necesario después de detectar al intruso, eliminar su comunicación dentro de la red y excluirlo por completo de la red para evitar una nueva intrusión en futuras ocasiones.

En cuanto a las técnicas de Detección de Intrusos podemos nombrar, algunos modelos computacionales que ya hacen parte de este novedoso tema como lo es la seguridad en las redes Ad-Hoc. Existen propuestas de arquitecturas distribuidas y cooperativas para la detección de intrusos usando modelos de detección de anomalías y comportamientos incongruentes. Anomalías tales como incoherencias en la tabla de enrutamiento de un nodo, el flujo de desvío de información por causa de mensajes de difusión que capturan las direcciones físicas MAC de los nodos pertenecientes a la red por parte del nodo intruso, y la disrupción, se convierten en características que hacen pensar a un IDS de la red, que un nodo con tales comportamientos sea un nodo intruso. Es por eso que en [2] se habla de un sistema propuesto, donde cada uno de los nodos de la MANET ejecuta un agente simple IDS que supervisa de forma constante las actividades locales al nodo. De acuerdo a las características de las anomalías se puede llegar a pensar en la existencia de un intruso, (Tarea que realiza el agente IDS del nodo correspondiente). Si el IDS detecta una intrusión a partir de los parámetros establecidos locales para el nodo, se ejecuta una operación de contradicción al intruso. En medio de este proceso puede suceder que a pesar de la anomalía detectada, el IDS no tenga la certeza definitiva de que exista propiamente una intrusión, de esta manera se inicia un proceso conjunto con los enrutadores o nodos que se encuentren más cercanos al nodo que detecto la anomalía, pero que no tiene la certeza de la intrusión; así con esta operación conjunta se pretende decidir si finalmente existe o no un ataque. Cuando se llega a la detección definitiva en la red se elimina la intrusión reiniciando la comunicación entre los nodos que si hacen parte de la red.

En este enfoque se pretende también incentivar a una búsqueda más avanzada de la intrusión, dando una estructura llamada “estructura multicapa”, para realizar la detección del ataque, en las capas de los protocolos que hacen parte de la red.

Es precisamente en este tipo de enfoques de agentes sencillos aplicados a cada uno de los nodos para detección de anomalías y por consiguiente, realizar un rastreo a una posible intrusión, aparece un nuevo enfoque inspirado del anterior llamado: “Detección de Intrusos usando Agentes Móviles”. En este modelo computacional, muy pertinente para topologías dinámicas, lo que se pretende es implementar un Sistema de Detección de Intrusos cimentado en técnicas computacionales con agentes móviles que se adaptan al medio, aún cuando este varía su estructura con el tiempo, y realizar una percepción de acuerdo a las posibles anomalías que presentan la presencia de un intruso. Básicamente podemos hablar de un agente móvil como una entidad software, muy sencilla de implementar, con comportamiento inteligente y que se adapta a su entorno dinámicamente viajando por la red MANET y ejecutándose sobre ciertos nodos.

Esto se encuentra con más detalle en [3] donde se propone una arquitectura distribuida y colaborativa en donde se asignan funciones de detección a diferentes tipos de agentes. Así, de esta forma se obtiene una carga de funcionalidades entre agentes viajando por los diferentes nodos.

Estas son las técnicas propuestas hasta el momento que reúnen las opciones útiles para realizar detección de intrusos en redes Ad-Hoc. Al final, siempre tendría que pensarse en implementar este tipo de modelos de detección de intrusos tendiendo en cuenta la ubicación de los nodos, y la necesidad que cobija esa red, esto sin olvidar que los dispositivos involucrados dispongan de la suficiente capacidad y autonomía como para que la ejecución de un sistema de detección no atribuya una limitación no resistible sobre las prestaciones ofrecidas al usuario final.

3.2 SEGURIDAD EN EL ENRUTAMIENTO

En una red Ad-Hoc, los nodos proceden como routers, haciendo parte de los distintos protocolos de enrutamiento para revelar y conservar rutas a otros nodos de la red. Mientras que en las redes cableadas los routers son administrados por operadores de confianza, esto deja de ser cierto en redes wíreless Ad-Hoc, en las que se espera que cada nodo que llega a la red participe en la toma de decisiones. En general, el objetivo de un algoritmo de enrutamiento es establecer una ruta adecuada entre cada par de nodos. Si el resultado de este algoritmo es manipulado, el funcionamiento normal de la MANET puede verse seriamente afectado, actuando en contra del requisito de disponibilidad. Por este motivo la seguridad en el enrutamiento tiene un gran peso sobre la seguridad del sistema.

Además, se identifican los principales ataques contra los mecanismos de enrutamiento ad-hoc, clasificándolos en pasivos y activos. En [4] los ataques activos se clasifican a su vez en externos e internos. Los ataques externos son realizados por nodos que no pertenecen a la red. Estos ataques incluyen la inyección de información errónea de enrutamiento, reenvío de información de enrutamiento antigua y distorsión de la información de enrutamiento intercambiada entre los nodos de la red. Las medidas de prevención, tales como el cifrado y la autenticación, pueden establecer la defensa contra este tipo de ataques. Los ataques internos proceden de nodos comprometidos pertenecientes red. Esta es una amenaza de mayor gravedad, y los IDS pueden jugar un papel fundamental en la detección de este tipo de ataques.

En [5] se indican un conjunto de técnicas para diseñar algoritmos de enrutamiento ad-hoc resistentes a intrusiones (TIARA). Estas técnicas son independientes del algoritmo de enrutamiento, si bien para su implementación los algoritmos de enrutamiento ad-hoc deben ser modificados.

En [6] se propone un esquema que permite construir redes ad-hoc resistentes a intrusiones. El enfoque se basa en extender las capacidades de los algoritmos de enrutamiento ad-hoc existentes sin tener por ello que modificar dichos algoritmos. Esta propuesta utiliza mecanismos TIARA.

En [7] se propone un algoritmo de enrutamiento seguro, SRP, que proporciona información de conectividad correcta, actualizada y autenticada a cada par de nodos que desean establecer una comunicación segura. Para ello, el único requisito es la existencia de una asociación de seguridad entre el nodo que inicia la comunicación y el nodo destino.

En [8] se describe otro protocolo de enrutamiento seguro, SEAD, basado en parte en el protocolo de enrutamiento ad-hoc Destination- Sequenced Distance-Vector (DSDV). Los autores indican que SEAD es robusto ante múltiples ataques no coordinados que provocan un estado erróneo en la información de enrutamiento de cualquier nodo de la red.

En [9] se propone un algoritmo de enrutamiento seguro bajo demanda, ARIADNE, basado en el uso de criptografía simétrica de elevada eficiencia.

3.3 AUTENTICACIÓN DE ACCESO A TRAVÈS DE LA ADMINISTRACIÓN DE CLAVES

El empleo de técnicas de cifrado y de firmas digitales como mecanismos de prevención requiere el uso de claves criptográficas, que serán utilizadas por las partes comunicantes. El servicio de gestión de claves asiste a los nodos en el proceso de comunicación, permitiendo establecer relaciones de confianza entre las entidades que se comunican. Con frecuencia, este servicio es proporcionado por un tercero de confianza, en el que confían todos los nodos de la red. Típicamente, en el caso de sistemas criptográficos de clave pública, el tercero de confianza suele ser una autoridad de certificación

(AC).

En [10] se propone un esquema threshold (K,N), que permite distribuir las funciones de la AC entre un subconjunto de nodos de una red con N nodos. El sistema contiene tres tipos de nodos: clientes, servidores y combinadores. Los nodos cliente son los usuarios del servicio de gestión de claves. Los nodos servidores y combinadores, conjuntamente, proporcionan la funcionalidad de la AC. Cada nodo servidor mantiene una clave que le permite generar certificados parciales. Los nodos combinadores, que son también servidores, combinan certificados parciales para formar un certificado válido. Cuando el cliente desea renovar su certificado, solicita la renovación al menos a K nodos servidores. Si la solicitud es tramitada, cada nodo servidor genera un nuevo certificado parcial. Los certificados parciales son enviados a un combinador, que genera un certificado válido para el cliente. Los certificados de todos los clientes son almacenados por los nodos servidores, de modo que éstos actúan también como repositorios de claves.

En [11] se propone un esquema threshold (K, N) similar al anterior, sólo que ahora las funciones de la AC se distribuyen entre todos los nodos de la red, y no entre un subconjunto de nodos servidores especializados.

En [12] se propone una solución similar a PGP, donde los certificados son generados por los usuarios, sin necesidad de una AC. Cada nodo almacena un conjunto reducido de certificados correspondientes a las claves públicas de nodos que considera válidas.

Cuando dos nodos desean autenticar la clave pública del otro, lo hacen en base a los certificados que mantienen mediante un protocolo Shortcut Hunter, propuesto por los autores, basado en el fenómeno pequeño mundo.

En [13] se propone un servicio de gestión de claves basado en criptografía simétrica. Los nodos de la red comparten una clave secreta de grupo, que se utiliza para tareas de autenticación y para generar claves de cifrado. La clave de grupo no expira, mientras que las claves de cifrado se actualizan en periodos regulares. Este esquema es adecuado en redes con nodos de capacidad limitada, en los que la criptografía pública resulta excesivamente pesada.

En [14] y [15] se proponen esquemas para el acuerdo de claves entre nodos de redes ad-hoc localizadas sobre escenarios concretos.

Las propuestas anteriores permiten establecer un servicio de gestión de claves en un entorno ad-hoc. Sin embargo, la implementación final de estos servicios dependerá en gran medida de la capacidad de los nodos de la red, que en una MANET puede ser limitada. El desarrollo de propuestas que tengan en cuenta estas limitaciones puede ser una de las líneas de trabajo futuras en este apartado.

4. REFERENCIAS

[1] Y. Zhang, W. Lee. "Intrusion detection in wireless ad-hoc networks". Mobile Computing and Networking, 275-283, 2000.

[2] O. Kachirski, R. Guha. “Intrusion detection using mobile agents in wireless ad hoc networks“. Proceedings of the IEEE Workshop on Knowledge Media Networking, 153 -158, 2002.

[3] J. Lundberg. "Routing security in ad hoc networks".

[4] V. Kärpijoki. "Security in ad hoc networks".

[5] R. Ramanujan, A. Ahamad; J. Bonney, R. Hagelstrom, K. Thurber. “Techniques for intrusion-resistant ad hoc routing algorithms

(TIARA)”. Proceedings of IEEE Military Communications Conference (MILCOM'00), vol.2, Los Angeles, CA, USA, 22-25, 2000.

[6] R. Ramanujan, S. Kudige, S. Takkella, T. Nguyen, F. Adelstein. “Intrusion-resistant ad hoc wireless networks”. MILCOM 2002. Proceedings , vol 2 , 890 -894, 2002.

[7] P. Papadimitratos, Z. J. Haas. “Secure routing for mobile ad hoc networks”. Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation (CNDS),

2002.

[8] Y-C. Hu, D. B. Johnson, A. Perrig. “Secure efficient distance vector routing in mobile wireless ad hoc networks”. Proceedings of the

4th IEEE Workshop on Mobile Computing

Systems and Applications (WMCSA), 2002.

[9] Y-C. Hu, A. Perrig, D. B. Johnson. “Ariadne: a secure on-demand routing protocol for ad hoc networks”. Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom), 2002.

[10] L. Zhou, Z. J. Haas. “Securing ad hoc networks”. IEEE Networks, vol. 13, issue 6,

1999.

[11] H. Luo, S. Lu. “Ubiquitous and robust authentication services for ad hoc wireless networks”. Technical Report 200030, UCLA Computer Science Department, 2000.

[12] J-P. Hubaux, L. Buttyán, S. Capkun. “The quest for security in mobile ad hoc networks”. ACM,

2001.

[13] D. Balfanz, D. K. Smetters, P. Stewart, H. Chi Wong. “Talking to strangers: authentication in ad-hoc wireless networks”. Internet Society, Conference Proceeding of NDSS Conference

2002.

[14] N. Asokan, P. Ginzboorg. “Key agreement in ad hoc networks”. Computer Communications, vol. 23, 2000.

[15] Jiangchuan Liu, Kazem Sohraby, Qian Zhang, Bo Li, and Wenwu Zhu, “Resource Discovery in Mobile Ad Hoc Networks”