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
El Abstract.

Categorías
Introducción a redes Ad-Hoc, Protocolos de acceso al medio, Protocolos de enrutamiento (unicast), Protocolos de enrutamiento (multicast), Seguridad en redes Ad-Hoc, QoS en redes Ad-Hoc, Interconexión a redes fijas.

Keywords
MANET, QoS, IDS.

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 todas las estaciones ofrecen servicios de enrutamiento para permitir la comunicación de estaciones que no tienen conexión inalámbrica directa. En relación a las redes cableadas, las redes *Ad-Hoc* presentan cambios de topología frecuentes e impredecibles debido a la movilidad de sus estaciones. 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 artículo 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 correr 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.

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 QoS 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. 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

Los requisitos de seguridad en una red móvil Ad-Hoc son los mismos que los existentes en redes tradicionales, y se enumeran a continuación: confidencialidad, integridad, autenticación, no repudiación y disponibilidad. Sin embargo, las características generales de una MANET de topología dinámica, enlaces de ancho de banda limitado y capacidad variable, limitaciones de energía y capacidad de procesamiento en los nodos y seguridad física limitada, hacen del cumplimiento de los requisitos anteriores un problema mucho más complejo de abordar, mostrando la dificultad de diseñar una solución general en términos de seguridad sobre un escenario móvil Ad-Hoc.

La política de seguridad a aplicar en un entorno Ad-Hoc dependerá, en gran medida, de la aplicación y del escenario concreto para los que se realiza el despliegue de la red. Las propuestas de seguridad se centran en aspectos concretos del problema. Se pueden identificar tres aspectos clave que deberán ser cubiertos por cualquier política de seguridad en redes ad-hoc: sistemas de detección de intrusiones (IDS), seguridad de los protocolos de enrutamiento y servicios de gestión de claves.

3.1 Sistemas de detección de intrusiones

Las técnicas de prevención, tales como el cifrado y la autenticación, son necesarias como primera línea de defensa en una MANET. Sin embargo, una red *wireless* ad-hoc presenta vulnerabilidades inherentes que no son fácilmente previsibles. La detección de intrusiones permite establecer una segunda línea de defensa, y puede ser necesaria en beneficio del requisito de disponibilidad.

En [1] los autores proponen una arquitectura distribuida y cooperativa para la detección de intrusiones que utiliza un modelo de detección de anomalías. En el sistema propuesto, cada nodo de la red ejecuta un agente IDS que monitoriza las actividades locales al nodo. Si el IDS detecta una intrusión a partir de las trazas locales inicia un procedimiento de respuesta. Si detecta una anomalía, pero no tiene una evidencia concluyente de que se esté produciendo un ataque, puede iniciar un proceso cooperativo con sus nodos vecinos, de modo que puedan determinar finalmente si la intrusión ha tenido o no lugar. Los autores proponen además una estructura multicapa, en la que la detección se realiza a diferentes niveles en la torre de protocolos.

En [2] se propone un IDS distribuido basado en tecnología de agentes móviles. Un agente móvil es una entidad software autónoma poco pesada y dinámicamente actualizable que atraviesa la red y se ejecuta sobre ciertos nodos. Los autores indican que la tecnología de agentes es especialmente apropiada en el caso de MANETs, dónde los recursos en forma de ancho de banda en los enlaces y de capacidad en los nodos pueden ser limitados. Se propone una arquitectura no monolítica en la que las diferentes funciones a realizar por el IDS se distribuyen entre diferentes tipos de agentes, de modo que, finalmente, la carga introducida por el IDS se distribuye de forma eficiente entre los nodos de la red.

En cualquier caso, el empleo de técnicas de detección dependerá siempre de las características de la aplicación y del escenario concreto sobre el que dicha aplicación se ejecuta. Dada la sobrecarga que pueden introducir estos mecanismos, en términos de transmisión sobre el medio *wíreless* y de procesamiento y almacenamiento en los nodos, su uso puede resultar justificable únicamente en aplicaciones con fuertes requisitos de seguridad y en las que los dispositivos involucrados dispongan de la suficiente capacidad y autonomía como para que la ejecución de un sistema de detección no imponga una limitación no tolerable sobre las prestaciones ofrecidas al usuario final. Por otro lado, los modelos de detección tradicionales no son directamente aplicables en este nuevo escenario. Las grandes diferencias existentes con respecto a las redes convencionales deberán ser tenidas en cuenta por cualquier IDS aplicable en MANETs.

3.1.1 Los Agentes móviles

3.1.2 Sistemas Cooperativos

3.1.3 Computación y seguridad Ubicua

3.2 Seguridad de los protocolos de enrutamiento

Los nodos en una MANET actúan como *routers*, participando en el protocolo de enrutamiento para descubrir y mantener rutas a otros nodos de la red. Así, mientras que en las redes tradicionales 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 [3] 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 (disrupción). 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.

3.3 Servicios de gestión de claves

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] V. Kärpijoki. "Security in Ad-Hoc networks".