UNIVERSIDAD LASALLISTA

BENAVENTE

ESCUELA DE
INGENIERÍA EN COMPUTACIÓN
Con estudios incorporados a la Universidad Nacional Autónoma de México

CLAVE: 8793-16

AMENAZAS A LA SEGURIDAD EN LAS REDES MÓVILES AD HOC

TESIS

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

Presenta:

RAMIRO ANTONIO BURGOS MORELOS

Asesor:

ING. ALEJANDRO GUZMÁN ZAZUETA

Celaya, Gto. Octubre 2011

Agradecimientos Personales

A DIOS por cuidarme y guiarme toda mi vida, permitirme terminar mi carrera y todas las gracias que he recibido.

A la Virgen de Guadalupe por sus intercesiones.

A mis Padres Ramiro y Laura por su invaluable guía, interminable apoyo y el amor que siempre me han dado.

A mi Hermana que siempre está a mi lado y que sus consejos siempre me han ayudado a salir adelante.

A mis amigos que me han ayudado a crecer como persona y siempre están apoyándome.

A mis maestros que me impulsaron a seguir adelante.

ÍNDICE

Introducción

Las redes móviles Ad hoc (MANET por sus siglas en inglés) es una colección de dispositivos de comunicación o nodos que desean comunicarse y/o compartir información sin la necesidad de una infraestructura fija. Los mismos nodos son los encargados de, dinámicamente, buscar y descubrir otros nodos para comunicarse. Y la tendencia, sobre todo en usos comerciales, es la de adoptar las redes Ad Hoc debido a las características especiales que conlleva este tipo de red, pero hay un reto muy grande para que estas redes proliferen el cual es la vulnerabilidad a los ataques de seguridad. Algunas de los retos presenten en las redes MANET son, la arquitectura de la red de pares (o P2P siglas en ingles comúnmente usadas), las limitaciones de recursos, la topología de una red dinámica etc. Ahora que las redes MANET se están popularizando por su capacidad de crear redes temporales sin la necesidad de infraestructura establecida o alguna administración central, los riesgos de seguridad deben de ser la primera preocupación. En esta tesis, identificare los riesgos de seguridad existentes que se presentan en las redes Ad Hoc, como reproducirlos, así como las medidas que se deben tomar para resolver estos problemas. Para esto me he informado acerca de los métodos de varios tipos de ataques así como su solución, además que he podido hacer comparativas para identificar las amenazas en las diferentes capas. En la creación de esta tesis me di cuenta de que un protocolo de enrutamiento totalmente seguro es algo difícil de establecer. No hay ningún algoritmo que proteja contra la mayoría de los ataques "comunes" como los hoyos de gusano, los ataques rápidos etc. En conclusión, me enfoque en encontrar soluciones como un mejor sistema de manejo de claves, sistemas basados en la confianza, y la seguridad de los datos en las diferentes capas. Aunque en realidad la verdadera solución de seguridad global es la prevención, detección y la respuesta rápida ante los problemas en las redes móviles Ad Hoc.

CAPÍTULO

I

INTRODUCCIÓN A LAS REDES DE COMPUTADORAS Y FINALIDAD DE LA TESIS

1.1.- Introducción a las redes

Una red de computadoras, también llamada red informática, es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que compartan información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc.

Una red de comunicaciones es, también, un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, cable de fibra óptica, etc.).

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI (Open System Interconnection) por la ISO, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

Una Intranet es una red privada donde la tecnología de Internet se usa como arquitectura elemental. Se trata de una red interna que se construye usando los protocolos TCP/IP para comunicación de Internet, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable.

El hardware fundamental no constituye por sí mismo una intranet; son imprescindibles los protocolos del software. La *Intranet* puede coexistir con otra tecnología de red de área local. En muchas compañías, los "sistemas patrimoniales" existentes que incluyen sistemas centrales, redes Novell, mini computadoras y varias bases de datos, están integrados en una intranet mediante una amplia variedad de herramientas.

Un ejemplo de aplicación práctica de una Intranet es el acceso a bases de datos patrimoniales mediante su interfaz de entrada común (CGI). Con el mismo propósito, la Intranet también puede utilizar aplicaciones codificadas en el lenguaje de programación Java para acceder a bases de datos patrimoniales.

La seguridad en una Intranet es complicada de implementar, ya que se trata de brindar seguridad tanto a usuarios externos como internos, que supuestamente deben tener permiso para usar los servicios de la red.

Una Intranet o una red interna se limita en alcance a una sola organización o entidad. Generalmente funciona a través de servicios de protocolo de comunicaciones como HTTP, FTP, SMTP, POP3 y otros de uso general.

En una Intranet se pueden tener los mismos servicios que en Internet, pero éstos sólo quedan disponibles para los usuarios de esa red privada, no para los usuarios en general.

1.2.- Clasificación de redes

1.2.1.- Clasificación de redes por alcance.

1.2.1.1.- Red de área personal (*PAN*)

PAN es una solución de red que aumenta nuestro ambiente personal de trabajo, seguridad. Se tiene una gran variedad de dispositivos disponibles (PDA, organizadores personales Webpads, computadores de mano, cámaras, etc.). Que envuelven a una persona dentro de la distancia que puede ser cubierta por la voz y proveen comunicaciones captables dentro del espacio personal y con el mundo exterior. Para los próximos dispositivos que trabajan en estas redes, PAN puede usar el medio inalámbrico, así como el campo magnético. En particular cuando se usa el medio inalámbrico, Se refiere a las PANs inalámbricas o WPAN. La WPAN forma una burbuja alrededor de la persona, que se le denomina espacio de operación personal (POS por sus siglas en inglés) Un concepto fundamental anterior a los sistemas WPAN, afirma que en algún momento dos dispositivos equipados con WPAN tienen cobertura dentro de aproximadamente 10 metros uno del otro (sus POSs se intersecan). Se forma entonces una posible conexión. Un dispositivo WPAN puede conectarse a un repetidor para acceder al internet o puede ser dinámicamente extendido para incluir el acceso a sensores y actuadores.

La tecnología inalámbrica WPAN es de corto-alance, en relación a la tecnología WLAN. Sin embargo WLAN y WPAN tienen situaciones complementarias:

WPAN enfatiza el bajo costo y el bajo consumo de potencia, usualmente permite una rápida transmisión y un máximo flujo de datos. WLAN enfatiza sobre una gran cantidad de datos y un amplio rango de cobertura que representa un gasto en los costos y el consumo de potencia. Este concepto es mostrado en la figura 1.1

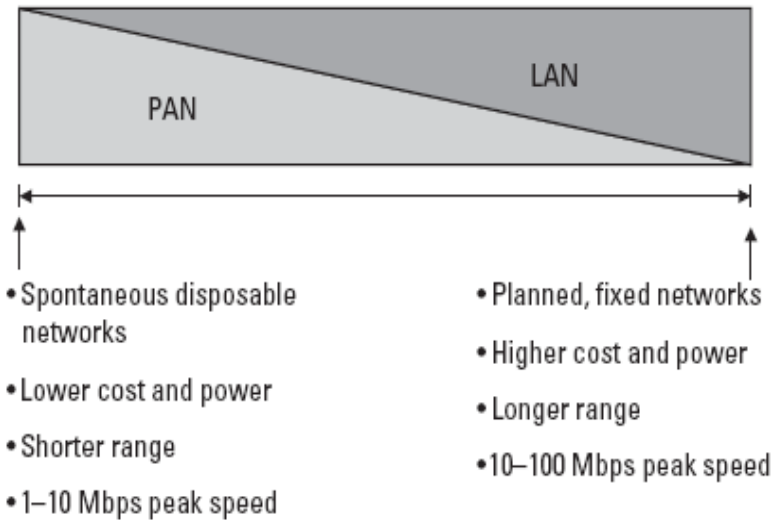


Figura 1.1 Posición complementarias de WLANS Y WPANs

1.2.1.2.- Red de área local (*LAN*)

Una red de área local, red local o LAN la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Las Redes de área local surgieron a partir de la revolución de la PC. Las LANs permitieron que usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos, y tener acceso a recursos compartidos de toda la Red, tales como Servidores de Archivos o de aplicaciones.

Con la aparición de NetWare surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. NetWare dominaba el campo de las LAN de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advanced Server y Windows for Workgroups.

1.2.1.3.- Red de área de campus (*CAN*)

Una red de área de campus (CAN) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Puede ser considerado como una red de área metropolitana que se aplica específicamente a un ambiente universitario. Por lo tanto, una red de área de campus es más grande que una red de área local, pero más pequeña que una red de área amplia.

En un CAN, los edificios de una universidad están conectados usando el mismo tipo de equipo y tecnologías de redes que se usarían en un LAN. Además, todos los componentes, incluyendo conmutadores, enrutadores, cableado, y otros, le pertenecen a la misma organización.

1.2.1.4.- Red de área metropolitana (*MAN*)

Es una red de alta velocidad que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como la red más grande del mundo una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

Las Redes MAN BUCLE, se basan en tecnologías Bonding, de forma que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario.

Además esta tecnología garantice SLAS´S del 99,999, gracias a que los enlaces están formados por múltiples pares de cobre y es materialmente imposible que 4, 8 ó 16 hilos se averíen de forma simultánea.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Este tipo de redes es una versión más grande que la LAN y que normalmente se basa en una tecnología similar a esta, La principal razón para distinguir una MAN con una categoría especial es que se ha adoptado un estándar para que funcione, que equivale a la norma IEEE.

Las redes MAN también se aplican en las organizaciones, en grupos de oficinas corporativas cercanas a una ciudad, estas no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Estas redes pueden ser públicas o privadas.

Las redes de área metropolitana, comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 km. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos.

1.2.1.5.- Red de área amplia (*WAN*)

Una red de área amplia se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continua.

Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro. A diferencia de las redes, la velocidad a la que circulan los datos por las redes WAN suele ser menor que la que se puede alcanzar en las redes LAN. Además, las redes LAN tienen carácter privado.

La infraestructura de redes WAN la componen, además de los nodos de conmutación, líneas de transmisión de grandes prestaciones, caracterizadas por sus grandes velocidades y ancho de banda en la mayoría de los casos.

Las líneas de transmisión (también llamadas "circuitos", "canales" o "troncales") mueven información entre los diferentes nodos que componen la red.

Los elementos de conmutación también son dispositivos de altas prestaciones, pues deben ser capaces de manejar la cantidad de tráfico que por ellos circula. De manera general, a estos dispositivos les llegan los datos por una línea de entrada, y este debe encargarse de escoger una línea de salida para reenviarlos. En la figura 1.2, se muestra un esquema general de los que podría ser la estructura de una WAN. En el mismo, cada host está conectada a una red LAN, que a su vez se conecta a uno de los nodos de conmutación de la red WAN. Este nodo debe encargarse de encaminar la información hacia el destino para la que está dirigida.

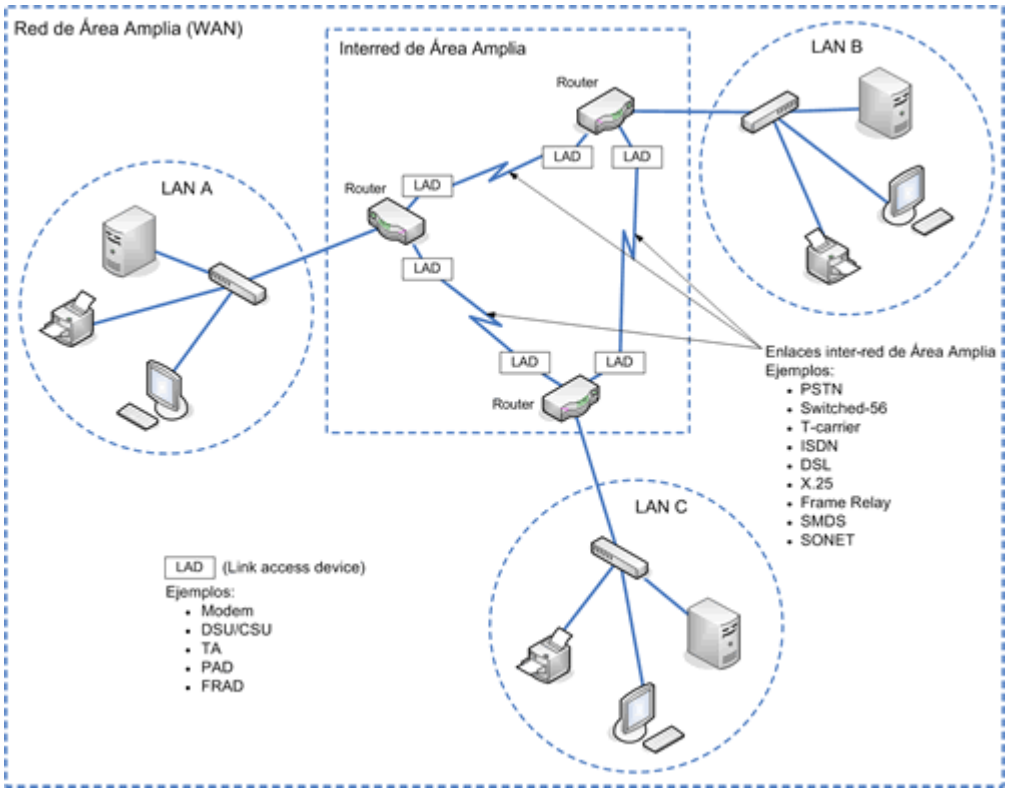


Figura 1.2 Estructura de una Red Área Amplia (WAN)

1.2.1.6.- Red de área de almacenamiento (*SAN*)

Una red de área de almacenamiento, SAN por sus siglas en inglés (*storage area network*), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA,SATA y SCSI. En otros métodos de almacenamiento, (como SMB o NFS), el servidor solicita un determinado fichero, por ejemplo "/home/usuario/test". En una SAN el servidor solicita "el bloque 6000 del disco 4". La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI.

Una SAN es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a LUNs. Un LUN (por sus siglas en inglés Logic Unit Number), o número de unidad lógica, es un disco virtual proporcionado por la SAN. El administrador del sistema tiene el mismo acceso y los derechos a la LUN como si fuera un disco directamente conectado a la misma. El administrador puede particionar y formatear el disco en cualquier medio que él elija.

Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Una red de canal de fibra es muy rápida y no está agobiada por el tráfico de la red LAN de la empresa. Sin embargo, es muy cara. También requieren conmutadores especiales de canal de fibra. iSCSI es una nueva tecnología que envía comandos SCSI sobre una red TCP / IP. Este método no es tan rápido como una red Fibre Channel, pero ahorra costos, ya que utiliza un hardware de red menos costoso.

Una de las diferencias y principales características de las SAN es que son construidas para minimizar el tiempo de respuesta del medio de transmisión. Además de que permite que múltiples servidores sean conectados al mismo grupo de discos o librerías de cintas, permitiendo que la utilización de los sistemas de almacenamiento y los respaldos sean óptimos.

Las SAN al ser construidas con fibra óptica heredan los beneficios de ésta, por ejemplo, las SAN pueden tener dispositivos con una separación de hasta 10 Km sin repetidores.

El rendimiento de cualquier sistema de cómputo dependerá de la velocidad de sus subsistemas, es por ello que las SAN han incrementado su velocidad de transferencia de información, desde 1 Gigabit, hasta actualmente 2 y 4 Gigabits por segundo.
Disponibilidad - Una de las ventajas de las SAN es que al tener mayor conectividad, permiten que los servidores y dispositivos de almacenamiento se conecten más de una vez a la SAN, de esta forma, se pueden tener *rutas* redundantes que a su vez incrementaran la tolerancia a fallos.

La seguridad en las SAN ha sido desde el principio un factor fundamental, desde su creación se notó la posibilidad de que un sistema accediera a un dispositivo que no le correspondiera o interfiriera con el flujo de información, es por ello que se ha implementado la tecnología de zonificación, la cual consiste en que un grupo de elementos se aíslen del resto para evitar estos problemas, la zonificación puede llevarse a cabo por hardware, software o ambas, siendo capaz de agrupar por puerto o por WWN (World Wide Name), una técnica adicional se implementa a nivel del dispositivo de almacenamiento que es la Presentación, consiste en hacer que una LUN (Logical Unit Number) sea accesible sólo por una lista predefinida de servidores o nodos (se implementa con los WWN) .

1.2.2.- Clasificación por método de conexión

Las redes de ordenadores se pueden clasificar de acuerdo a la tecnología de hardware y software que se utiliza para interconectar los dispositivos individuales en la red, como la fibra óptica, Ethernet, LAN inalámbrica, HomePNA, power line communication o G.hn.

Ethernet está definida por IEEE 802 y utiliza diferentes normas y medios que permiten la comunicación entre los dispositivos.

Con frecuencia los dispositivos desplegados incluyen concentradores, conmutadores, puentes o routers.

La tecnología inalámbrica LAN está diseñada para conectar dispositivos sin necesidad de cables.

Estos dispositivos utilizan ondas de radio o las señales de infrarrojos como medio de transmisión.

La tecnología UIT-T G.hn utiliza el cableado existente en casa (cable coaxial, líneas telefónicas y líneas eléctricas) para crear una red de área local alta velocidad (hasta 1 Gigabit / s).

1.2.3.- Clasificación por relación

1.2.3.1.- Cliente / Servidor

Las redes Cliente/Servidor se usan en entornos LAN mayores, incluyendo colegios y universidades. En este enfoque de la conectividad, la red se compone de uno o más servidores especializados y varios clientes diferentes, los servidores están diseñados para proporcionar servicios centralizados y los clientes son los diferentes nodos en la red. En un entorno Cliente/Servidor, las PCs conectadas a la red puede llamarse clientes, nodos o estaciones de trabajo; existe poca diferencia técnica entre los tres términos en este tipo de red.

Muchos tipos diferentes de servidores se pueden usar en una red Cliente/Servidor. Estos servidores se agregan a la red conforme lo dictan las necesidades de ésta. Tipos comunes de servidores incluyen los siguientes:

Servidor de archivo. Esta computadora está dedicada a proporcionar almacena-miento y administración centralizados de archivos.

Servidor de impresión. Esta computadora está dedicada a proporcionar servicios de impresión centralizados.

Servidor de comunicaciones. Esta computadora está dedicada a proporcionar servicios de módem, fax y correo electrónico.

Servidor de base de datos. Esta computadora está dedicada a ejecutar un programa de base de datos centralizado.

Como mínimo, una red de este tipo tendrá un servidor de archivos, agregándose otros servicios conforme crezcan y desarrollen las necesidades de la empresa.

En muchas formas, el enfoque de Cliente/Servidor para la conectividad es un enfoque de arriba hacia abajo; los servidores proporcionan los servidores centralizados para la red entera. Aunque este enfoque es muy eficaz, tiene sus desventajas. Quizá la mayor desventaja es que si un servidor falla (por cualquier razón), la red entera falla en relación

con ese recurso. Por ejemplo, si un servidor de impresión no está disponible, no hay forma de imprimir a través de la red hasta de una impresora local, si hay una disponible). Debido a que es un asunto crítico mantener un funcionamiento la red, la mayor parte de los entornos que usan un enfoque Cliente/Servidor confían en una persona, o el jefe del departamento, se conoce como administrador de la red. Esta persona debe ser muy competente en lo relacionado con la conectividad y tener una compresión de la forma como lo relacionado con la conectividad y tener una compresión de la forma como encajan todas las piezas de la red. El administrador de la red- y los costos de una empresa que financia a esta persona- es la razón por la que el enfoque cliente/servidor se usa de manera compón sólo en redes grandes.

1.2.3.2.- Redes Par a par (peer to peer, punto a punto)

En un entorno de conectividad de punto a punto no hay servidores centralizados. En un lugar, cada nodo en la red proporciona servidores a los que pueden tener acceso otros nodos en la red. Por ejemplo, un nodo puede tener una impresora que pueden usar otros nodos, en tanto que un nodo diferente puede tener archivos de datos a disposición de otros usuarios de la red.

La conectividad de punto a punto se usa de manera tradicional para redes o grupos de trabajo menores. Por ejemplo un salón de clase, si no está conectado a una red mayor, puede usar el enfoque de red de punto. Este enfoque elimina varias de las desventajas inherentes en el enfoque Cliente/Servidor. Por ejemplo, si una de las computadoras en la red falla, no se desactiva la red completa. Por su puesto, los recursos compartidos por ese nodo no están disponibles, pero pueden usarse servicios alternativos por medio de otros nodos en la red. Además, de manera característica no es necesario un administrador de red porque cada persona que usa la red, por lo general mantiene su propia máquina y administra sus propios recursos compartidos.

1.3.- Topología de Red.

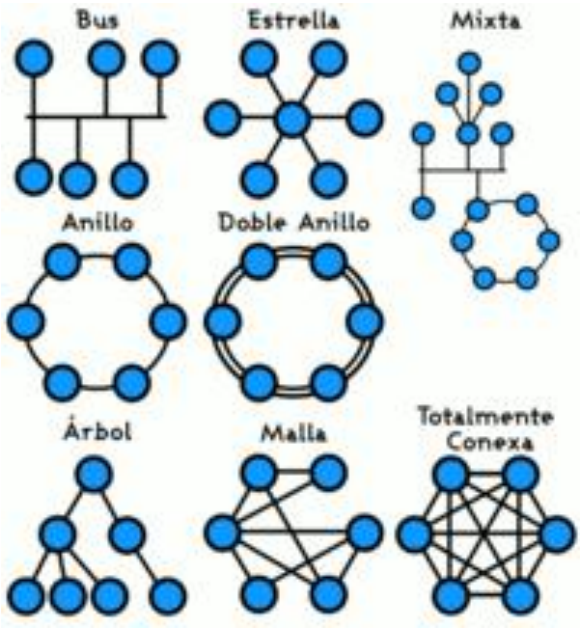


Figura 1.3 Topología de Red

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en cómo se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación.

1.3.1.- Topología en estrella.

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. Evidentemente, todas las tramas de información que circulen por la red deben pasar por el nodo principal, con lo cual un fallo en él provoca la caída de todo el sistema. Por otra parte, un fallo en un determinado cable sólo afecta al nodo asociado a él; si bien esta topología obliga a disponer de un cable propio para cada terminal adicional de la red. La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central.

Equipo como unidades de multiplexaje, concentradores y pares de cables solo reducen los requerimientos de cableado, sin eliminarlos y produce alguna economía para esta topología. Resulta económica la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que este requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

Los datos en estas redes fluyen del emisor hasta el concentrador. Este controla realiza todas las funciones de red además de actuar como amplificador de los datos. Esta configuración se suele utilizar con cables de par trenzado aunque también es posible llevarla a cabo con cable coaxial o fibra óptica.

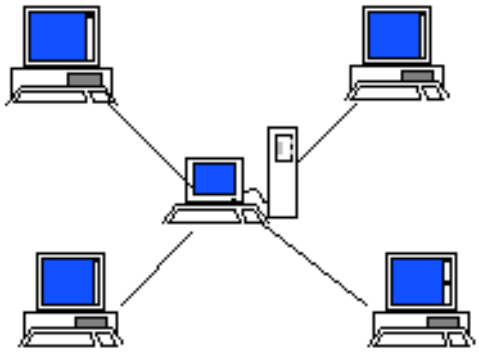


Figura 1.4: Topología en estrella

1.3.2.-Topología en bus

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizarla (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

Como ejemplo más conocido de esta topología, encontramos la red *Ethernet* de Xerox. El método de acceso utilizado es el *CSMA/CD*, método que gestiona el acceso al bus por parte de los terminales y que por medio de un algoritmo resuelve los conflictos causados

en las colisiones de información. Cuando un nodo desea iniciar una transmisión, debe en primer lugar escuchar el medio para saber si está ocupado, debiendo esperar en caso afirmativo hasta que quede libre. Si se llega a producir una colisión, las estaciones reiniciarán cada una su transmisión, pero transcurrido un tiempo aleatorio distinto para cada estación. Esta es una breve descripción del protocolo de acceso *CSMA/CD*, pues actualmente se encuentran implementadas cantidad de variantes de dicho método con sus respectivas peculiaridades. El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

Consiste en un cable con un terminador en cada extremo del que se "cuelgan" todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable. Este cable recibe el nombre de “Backbone Cable.”

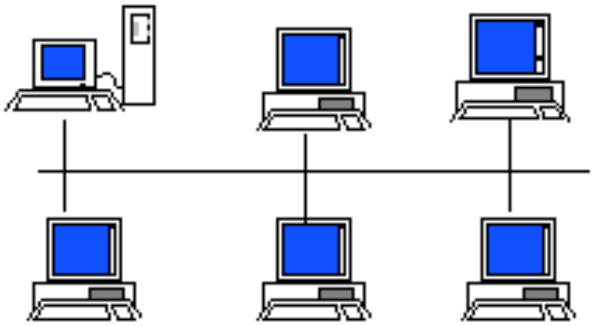


Figura 1.5: Topología bus

1.3.3.-Topología en anillo

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo está diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella. El anillo es fácilmente expandido para conectar más nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

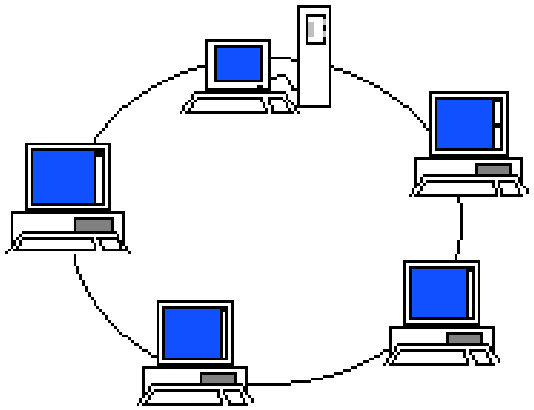


Figura 1.6: Topología en anillo

1.3.4.-Topología de Estrella cableada / Star-Wired Ring

Físicamente parece una topología estrella pero el tipo de concentrador utilizado, la MAU se encarga de interconectar internamente la red en forma de anillo.

Esta tipología es la que se utiliza en redes Token-Ring.

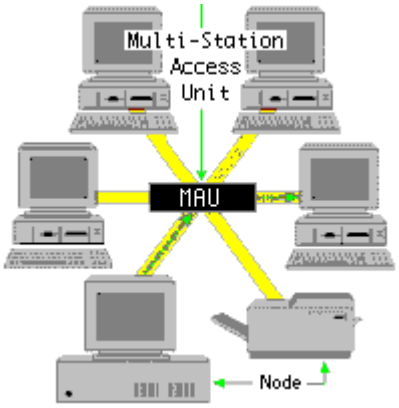


Figura 1.7. Topología de estrella cableada

1.3.5.-Topología de Árbol / Tree

La topología de árbol combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red.

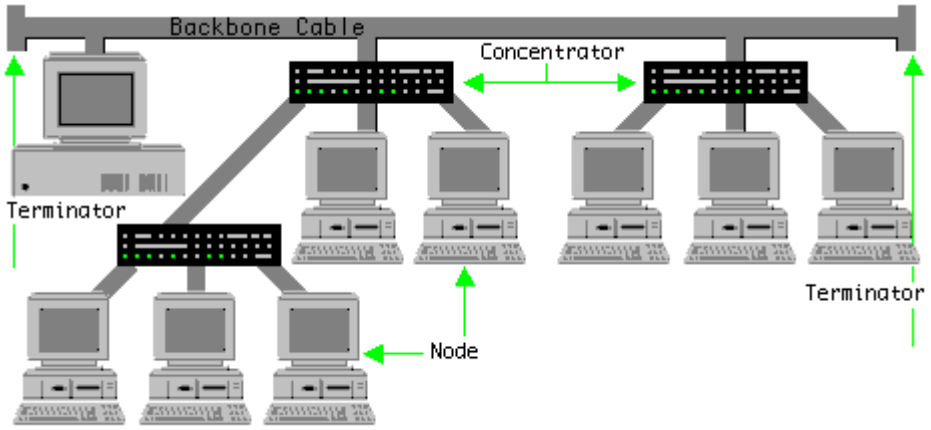


Figura 1.8: topología en árbol.

1.4.- Protocolos y Estándares

Estándar.- Es la especificación de red (o la serie de especificaciones) adoptada, e incluye guías y reglas que se refieren al tipo de componentes que deben usarse, a la manera de conectar los componentes, así como a los protocolos de comunicación que hay que utilizar.

ANSI (Instituto Nacional de Estándares Americanos).

IEEE (*Instituto de Ingenieros en Eléctrica y Electrónica)*

Protocolo.- Consiste en un conjunto de reglas que definen la forma en que deben de efectuarse las comunicaciones de las redes, incluyendo el formato, la temporización, la secuencia y la revisión y la corrección de errores.

Protocolo de comunicación.- Es el conjunto de reglas y convenciones establecidas *a priori* para el efecto de la comunicación entre el emisor y el receptor.

1.4.1.- Estándares de Redes LAN e Inalámbricas

El Comité 802, o proyecto 802, del Instituto de Ingenieros en Eléctrica y Electrónica (IEEE) han definido los siguientes estándares de redes de área local (LAN).

802.1 Definición Internacional de Redes. Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador puede tener una dirección única. Los vendedores de tarjetas de interface de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE. Cada vendedor es entonces responsable de crear una dirección única para cada uno de sus productos.

802.2 Control de Enlaces Lógicos. Define el protocolo de control de enlaces lógicos (LLC) del IEEE, el cual asegura que los datos sean transmitidos de forma confiable por medio del enlace de comunicación. La capa de Datos-Enlace en el protocolo OSI esta subdividida en las subcapas de Control de Acceso a Medios (MAC) y de Control de Enlaces Lógicos (LLC). En Puentes, estas dos capas sirven como un mecanismo de switcheo modular, como se muestra en la figura I-5. El protocolo LLC es derivado del protocolo de Alto nivel para Control de Datos-Enlaces (HDLC) y es similar en su operación. Nótese que el LLC provee las direcciones de Puntos de Acceso a Servicios (SAPs), mientras que la subcapa MAC provee la dirección física de red de un dispositivo. Las SAPs son específicamente las direcciones de una o más procesos de aplicaciones ejecutándose en una computadora o dispositivo de red.

802.3 Redes CSMA/CD (Ethernet).El estándar 802.3 del IEEE (ISO 8802-3), que define cómo opera el método de Acceso Múltiple con Detección de Colisiones (CSMA/CD) sobre varios medios. El estándar define la conexión de redes sobre cable coaxial, cable de par trenzado, y medios de fibra óptica. La tasa de transmisión original es de 10 Mbits/seg, pero nuevas implementaciones transmiten arriba de las 100 Mbits/seg calidades de datos en cables de par trenzado.

802.4 Redes Token Bus. El estándar token bus define esquemas de red de anchos de banda grandes, usados en la industria de manufactura. Se deriva del Protocolo de Automatización de Manufactura (MAP).La red implementa el método token-passing para una transmisión bus. Un token es pasado de una estación a la siguiente en la red y la estación puede transmitir manteniendo el token. Los tokens son pasados en orden lógico basado en la dirección del nodo, pero este orden puede no relacionar la posición física del nodo como se hace en una red token ring. El estándar no es ampliamente implementado en ambientes LAN.

802.5 Redes Token Ring. También llamado ANSI 802.1-1985, define los protocolos de acceso, cableado e interface para la LAN token ring. IBM hizo popular este estándar. Usa un método de acceso de paso de tokens y es físicamente conectada en topología estrella, pero lógicamente forma un anillo. Los nodos son conectados a una unidad de acceso central (concentrador) que repite las señales de una estación a la siguiente. Las unidades de acceso son conectadas para expandir la red, que amplía el anillo lógico. La Interface de Datos en Fibra Distribuida (FDDI) fue basada en el protocolo token ring 802.5, pero fue desarrollado por el Comité de Acreditación de Estándares (ASC) X3T9. Es compatible con la capa 802.2 de Control de Enlaces Lógicos y por consiguiente otros estándares de red 802.

802.6 Redes de área Metropolitana (MAN). Define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuida (DQDB). El bus dual provee tolerancia de fallos para mantener las conexiones si el bus se rompe. El estándar MAN está diseñado para proveer servicios de datos, voz y vídeo en un área metropolitana de aproximadamente 50 kilómetros a tasas de 1.5, 45, y 155 Mbits/seg. DQDB es el protocolo de acceso subyacente para el SMDS (Servicio de Datos de Multimegabit Switcheados), en el que muchos de los portadores públicos son ofrecidos como una manera de construir redes privadas en áreas metropolitanas. El DQDB es una red repetidora que switchea celdas de longitud fija de 53 bytes; por consiguiente, es compatible con el Ancho de Banda ISDN y el Modo de Transferencia Asíncrona (ATM). Las celdas son switcheables en la capa de Control de Enlaces Lógicos.

Los servicios de las MAN son Sin Conexión, Orientados a Conexión, y/o isócronas (vídeo en tiempo real). El bus tiene una cantidad de slots de longitud fija en el que son situados los datos para transmitir sobre el bus. Cualquier estación que necesite transmitir simplemente sitúa los datos en uno o más slots. Sin embargo, para servir datos isócronos, los slots en intervalos regulares son reservados para garantizar que los datos llegan a tiempo y en orden.

802.7 Grupo Asesor Técnico de Anchos de Banda. Este comité provee consejos técnicos a otros subcomités en técnicas sobre anchos de banda de redes.

802.8 Grupo Asesor Técnico de Fibra óptica. Provee consejo a otros subcomités en redes por fibra óptica como una alternativa a las redes basadas en cable de cobre. Los estándares propuestos están todavía bajo desarrollo.

802.9 Redes Integradas de Datos y Voz. El grupo de trabajo del IEEE 802.9 trabaja en la integración de tráfico de voz, datos y vídeo para las LAN 802 y Redes Digitales de Servicios Integrados (ISDNs). Los nodos definidos en la especificación incluyen teléfonos, computadoras y codificadores/decodificadores de vídeo (códec). La especificación ha sido llamada Datos y Voz Integrados (IVD). El servicio provee un flujo multiplexado que puede llevar canales de información de datos y voz conectando dos estaciones sobre un cable de cobre en par trenzado. Varios tipos de diferentes de canales son definidos, incluyendo full dúplex de 64 Kbits/seg sin switcheo, circuito switcheado, o canales de paquete switcheado.

802.10 Grupo Asesor Técnico de Seguridad en Redes. Este grupo está trabajando en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encriptamiento. Los estándares propuestos están todavía bajo desarrollo en este momento.

802.11 Redes Inalámbricas. Este comité está definiendo estándares para redes inalámbricas. Está trabajando en la estandarización de medios como el radio de espectro de expansión, radio de banda angosta, infrarrojo, y transmisión sobre líneas de energía. Dos enfoques para redes inalámbricas se han planeado. En el enfoque distribuido, cada estación de trabajo controla su acceso a la red. En el enfoque de punto de coordinación, un hub central enlazado a una red alámbrica controla la transmisión de estaciones de trabajo inalámbricas.

802.12 Prioridad de Demanda (100VG-ANYLAN). Este comité está definiendo el estándar Ethernet de 100 Mbits/seg. Con el método de acceso por Prioridad de Demanda propuesto por Hewlett Packard y otros vendedores. El cable especificado es un par trenzado de 4 alambres de cobre y el método de acceso por Prioridad de Demanda usa un hub central para controlar el acceso al cable. Hay prioridades disponibles para soportar envío en tiempo real de información multimedia.

1.4.2.- Protocolos de red

Podemos definir un protocolo como el conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática. Existen dos tipos de protocolos: protocolos de bajo nivel y protocolos de red.

Los protocolos de bajo nivel controlan la forma en que las señales se transmiten por el cable o medio físico. En la primera parte del curso se estudiaron los habitualmente utilizados en redes locales (Ethernet y Token Ring). Aquí nos centraremos en los protocolos de red.

Los protocolos de red organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel. Veamos algunos de ellos:

IPX/SPX: IPX (*Internetwork Packet Exchange*) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware.

Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino). Otro protocolo, el SPX (*Sequenced Packet eXchange*), actúa sobre IPX para asegurar la entrega de los paquetes.

NetBIOS: NetBIOS (*Network Basic Input/Output System*) es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN. Desarrollado originalmente para las redes de ordenadores personales IBM, fue adoptado posteriormente por Microsoft. NetBIOS se usa en redes con topologías Ethernet y token ring.

No permite por sí mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos (por ejemplo, el TCP).
NetBIOS puede actuar como protocolo orientado a conexión o no (en sus modos respectivos *sesión* y *datagrama*).

En el modo sesión dos ordenadores establecen una conexión para establecer una conversación entre los mismos, mientras que en el modo datagrama cada mensaje se envía independientemente.

Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

NetBEUI: *NetBIOS Extended User Interface* o *Interfaz de Usuario para NetBIOS* es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos.

También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para Trabajo en Grupo.

Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos (por ejemplo, IPX o TCP/IP).

Un método usual es instalar tanto NetBEUI como TCP/IP en cada estación de trabajo y configurar el servidor para usar NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

AppleTalk: Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo. Existen tres variantes de este protocolo:

LocalTalk: La comunicación se realiza a través de los puertos serie de las estaciones. La velocidad de transmisión es pequeña pero sirve por ejemplo para compartir impresoras.

Ethertalk: Es la versión para Ethernet. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos.

Tokentalk: Es la versión de Appletalk para redes Tokenring.

TCP/IP: Es realmente un conjunto de protocolos, donde los más conocidos son TCP (*Transmission Control Protocol* o protocolo de control de transmisión) e IP (*Internet Protocol* o protocolo Internet).

1.4.3.- Estándares IEEE 802

802.1	Interfaec de Alto Nivel
802.2	Control de Enlaec Lógico
802.3	CSMA/CD
802.4	Token-Passing Bus
802.5	Token-Passing Ring
802.6	Redes de Área Metropolitana
802.7	Grupo de Consejo Técnico de Broadband
802.8	Grupo de Consejo Técnico de Fibra Óptica
802.9	Redes de Voz y Datos Integrados
802.10	Seguridad en Redes
802.11	LAN's sin cables

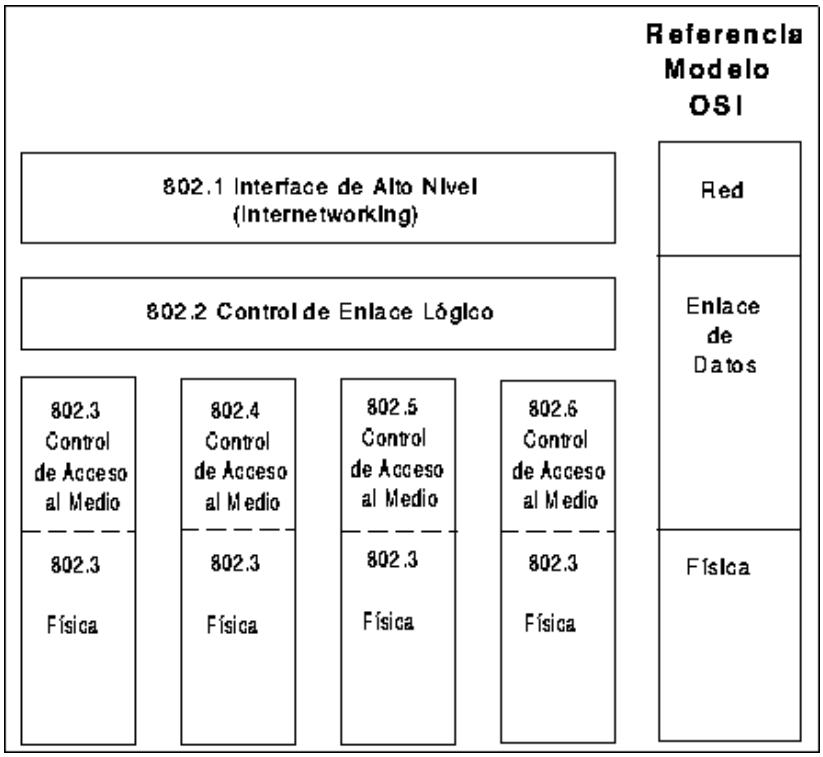
El comité 802 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE 802) fue formado al principio de los 80's para desarrollar estándares para las tecnologías emergentes, de manera que el equipo de redes de diferentes fabricantes pudiera trabajar junto e integrarse sin problemas.

En el año de 1982 se publicó un borrador de los estándares para redes CSMA/CS y Token Bus. En 1983 se publicó el estándar 802.3 que describe una red baseband CSMA/CD similar a Ethernet. Desde entonces se le han hecho algunos anexos dependiendo del tipo de medio físico que se utilice. Estos anexos incluyen redes como:

- 10BASE-2. Red baseband operando en cable coaxial delgado a 10 Mbps.
- 1BASE-5. Red baseband operando en cable trenzado a 1 Mbps.
- 10BASE-T. Red baseband operando en cable trenzado a 10 Mbps.
- 10BROAD-36. Red broadband operando en cable coaxial grueso a 10Mbps.

El siguiente estándar publicado fue el 802.4 que describe una red con token-passing bus, orientada a transmisiones tanto broadband como baseband.

El tercer estándar fue el 802.5, se basó en las especificaciones de la red IBM de Token-ring. Este define una red token-ring en cable trenzado cubierto con transmisión de datos de 1 a 4 Mbps. Se le han hecho mejoras al estándar para incluir entre otras cosas una tasa de operación de 16 Mbps.



1.5.- Componentes básicos de las redes

1.5.1.- Computadora

La mayoría de los componentes de una red media son los computadoras individuales, también denominados host; generalmente son sitios de trabajo (incluyendo computadoras personales) o servidores.

1.5.2.-Tarjetas de red

Para lograr el enlace entre las computadoras y los medios de transmisión (cables de red o medios físicos para redes alámbricas e infrarrojos o radiofrecuencias para redes inalámbricas), es necesaria la intervención de una tarjeta de red o NIC (Network Card Interface) con la cual se puedan enviar y recibir paquetes de datos desde y hacia otras computadoras, empleando un protocolo para su comunicación y convirtiendo esos datos a un formato que pueda ser transmitido por el medio (bits 0's/1's). Cabe señalar que a cada tarjeta de red le es asignado un identificador único por su fabricante, conocido como dirección MAC *(Media Access Control)*, que consta de 48 bits (6 bytes). Dicho identificador permite direccionar el tráfico de datos de la red del emisor al receptor adecuado.

El trabajo del adaptador de red es el de convertir las señales eléctricas que viajan por el cable (ej.: red Ethernet) o las ondas de radio (ej.: red Wifi) en una señal que pueda interpretar la computadora.

Estos adaptadores son unas tarjetas PCI que se conectan en las ranuras de expansión de la computadora. En el caso de computadoras portátiles, estas tarjetas vienen en formato PCMCIA. En algunas computadoras modernas, tanto de sobremesa como portátiles, estas tarjetas ya vienen integradas en la placa base.

Adaptador de red es el nombre genérico que reciben los dispositivos encargados de realizar dicha conversión. Esto significa que estos adaptadores pueden ser tanto

Ethernet, como Wireless, así como de otros tipos como fibra óptica, coaxial, etc. También las velocidades disponibles varían según el tipo de adaptador; éstas pueden ser, en Ethernet, de 10, 100 ó 1000 Mbps, y en los inalámbricos de 11 ó 55 Mbps.

1.6- Tipos de servidores

En las siguientes listas hay algunos tipos comunes de servidores y sus propósitos.

- Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.
- Servidor de impresiones: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.
- Servidor de correo: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con *e-mail* para los clientes de la red.
- Servidor de fax: almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
- Servidor de la telefonía: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o Internet; p. ej., la entrada excesiva del IP de la voz (VoIP), etc.
- Servidor proxy: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., *prefetching* y depositar documentos u otros datos que se soliciten muy frecuentemente). También *sirve* seguridad; esto es, tiene un Firewall (cortafuegos). Permite administrar el acceso a Internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios web.

- Servidor del acceso remoto (RAS): controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.
- Servidor de uso: realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza el interfaz operador o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.
- Servidor web: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos normalmente como contenido), y distribuye este contenido a clientes que la piden en la red.
- Servidor de reserva: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada *clustering*.
- Impresoras: muchas impresoras son capaces de actuar como parte de una red de Computadoras sin ningún otro dispositivo, tal como un *"print server"*, actuando como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión de ser terminado
- Terminal: muchas redes utilizan este tipo de equipo en lugar de puestos de trabajo para la entrada de datos. En estos sólo se exhiben datos o se introducen. Este tipo de terminales, trabajan unido a un servidor, que es quien realmente procesa los datos y envía pantallas de datos a los terminales.
- Otros dispositivos: hay muchos otros tipos de dispositivos que se puedan utilizar para construir una red, muchos de los cuales requieren una comprensión de conceptos más avanzados del establecimiento de una red de la computadora antes de que puedan ser entendidos fácilmente (ej., los cubos, las rebajadoras, los

puentes, los interruptores, los cortafuegos del hardware, etc.). En las redes caseras y móviles, que conectan la electrónica de consumo, los dispositivos, tales como consolas videojuegos, están llegando a ser cada vez más comunes.

- Servidor de Autenticación: Es el encargado de verificar que un usuario pueda conectarse a la red en cualquier punto de acceso, ya sea inalámbrico o por cable, basándose en el estándar 802.1x y puede ser un servidor de tipo *RADIUS*.
- Servidor DNS: Este tipo de servidores resuelven nombres de dominio sin necesidad de conocer su dirección IP.

1.7.- Construcción de una red de computadoras

1.7.1.- Una red simple

Una red de computadoras sencilla se puede construir de dos computadoras, agregando un adaptador de la red (controlador de interfaz de red (NIC)) a cada computadora y conectándolos mediante un cable especial llamado "cable cruzado" (el cual es un cable de red con algunos cables invertidos, para evitar el uso de un *router* o *switch*). Este tipo de red es útil para transferir información entre dos computadoras que normalmente no se conectan entre sí por una conexión de red permanente o para usos caseros básicos del establecimiento de red.

Alternativamente, una red entre dos computadoras se puede establecer sin aparato dedicado adicional, usando una conexión estándar, tal como el puerto serial RS-232 en ambos computadoras, conectándolos entre sí vía un cable especial cruzado nulo del módem.

En este tipo de red solo es necesario configurar una dirección IP, pues no existe un servidor que les asigne IP automáticamente.

En el caso de querer conectar más de dos computadoras, o con vista a una posible ampliación de la red, es necesario el uso de un concentrador que se encargará de repartir la señal y el ancho de banda disponible entre los equipos conectados a él.

Simplemente le llega el paquete de datos al concentrador, el cual lo reenvía a todos los equipos conectados a él; el equipo destinatario del paquete lo recoge, mientras que los demás simplemente lo descartan.

Esto afecta negativamente al rendimiento de la red, ya que solo se puede enviar un paquete a la vez, por lo que mientras ese paquete se encuentra en circulación ningún otro paquete.

1.7.2.-Redes prácticas

Las redes prácticas constan generalmente de más de dos computadoras interconectados y generalmente requieren dispositivos especiales además del controlador de interfaz de red con el cual cada computadora se debe equipar. Ejemplos de algunos de estos dispositivos especiales son: los concentradores (hubs), multiplexores (switches) y enrutadores (routers).

Las características más importantes que se utilizan para describir una red son: velocidad, seguridad, disponibilidad, escalabilidad y confiabilidad. La consideración de estas características permite dimensionar de manera adecuada una red de computadoras solucionando las necesidades de los usuarios.

- Velocidad: Es una medida de la rapidez con que los datos son transmitidos sobre la red.
- Seguridad: Indica el grado de seguridad de la red incluyendo los datos que son transmitidos por ella.
- Disponibilidad: Es una medida de la probabilidad de que la red va a estar disponible para su uso.
- Escalabilidad: Indica la capacidad de la red de permitir más usuarios y requerimientos de transmisión de datos.
- Confiabilidad: Es una medida de la probabilidad de falla.

1.8.- Resumen Tipos de redes

- Red pública: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.
- Red privada: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.
- Red de área Personal (PAN): (Personal Área Network) es una red de computadoras usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación intrapersonal), o para conectar con una red de alto nivel e Internet (un up link). Las redes personales del área se pueden conectar con cables con los buses de la computadora tales como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.
- Red de área local (LAN): una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización. Nota: Para los propósitos administrativos, las LANs grandes se dividen generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de computadoras que comparten un sistema común de recursos dentro de una LAN.
- Red de área local virtual (VLAN): Una Virtual LAN o comúnmente conocida como VLAN, es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden

alcanzar a los otros por medio de broadcast (dominio de broadcast) en la capa de enlace de datos, a pesar de su diversa localización física. Con esto, se pueden lógicamente agrupar computadoras para que la localización de la red ya no sea tan asociada y restringida a la localización física de cada computadora, como sucede con una LAN, otorgando además seguridad, flexibilidad y ahorro de recursos. Para lograrlo, se ha establecido la especificación IEEE 802.1Q como un estándar diseñado para dar dirección al problema de cómo separar redes físicamente muy largas en partes pequeñas, así como proveer un alto nivel de seguridad entre segmentos de redes internas teniendo la libertad de administrarlas sin importar su ubicación física.

- Red del área del campus (CAN): Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.
- Red de área metropolitana (MAN): una red que conecta las redes de un área (dos o más redes locales juntas) pero que no se extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Los enrutadores (routers) múltiples, los interruptores (switch) y los cubos están conectados para crear una MAN.
- Red de área amplia (WAN): es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de enlace de datos, y la capa de red.
- Red de área de almacenamiento (SAN): Es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología de fibra ó iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos de almacenamiento que la conforman.
- Red irregular: Es un sistema de cables y buses que se conectan a través de un módem, y que da como resultado la conexión de una o más computadoras. Esta

red es parecida a la mixta, solo que no sigue los parámetros presentados en ella. Muchos de estos casos son muy usados en la mayoría de las redes.

- Centralizado: Un WAN centralizado consiste en una computadora central que esté conectada con las terminales nodos y/u otros tipos de dispositivos del Terminal.
- Distribuido: Un WAN distribuido consiste en dos o más computadoras en diversas localizaciones y puede también incluir conexiones a los terminales nodos y a otros tipos de dispositivos del Terminal.

Red interna Dos o más redes o segmentos de la red conectados con los dispositivos que funcionan en la capa 3 (la capa de la "red") del modelo de la referencia básica de la OSI, tal como un router. Nota: Cualquier interconexión entre las redes del público, privadas, comerciales, industriales, o gubernamentales se puede también definir como red interna.

Estas redes pueden comunicarse al exterior utilizando NAT.

Internet Una red interna específica, está basada en una interconexión mundial de las redes gubernamentales, académicas, públicas, y privadas basadas sobre el Advanced Research Projects Agency Network (ARPANET) desarrollado por WARRA del departamento de la defensa de los EE.UU. también al World Wide Web (WWW) y designando el "Internet" con una "I" mayúscula para distinguirlo de otros internetworks genéricos.

Intranet y extranet Una red interna que se limitan en alcance a una sola organización o entidad y que utilicen el TCP/IP Protocol Suite, el HTTP, el FTP, y los otros protocolos y software de red de uso general en el Internet. Nota: Intranets se puede también categorizar como el LAN, CAN, MAN, WAN.

Una configuración común de una LAN es una intranet. Los servidores web intranet difieren de los servidores web públicos en que estos últimos no tienen acceso a la infraestructura de una empresa sin los permisos y las contraseñas adecuadas. En una Intranet, los servidores web están instalados en la red y la tecnología de navegador se

utiliza como frontal común para acceder a información de tipo financiero o datos basados en texto o gráficos almacenados en esos servidores.

Una Extranet es una Intranet parcialmente accesible para los foráneos autorizados. Mientras que una Intranet reside dentro de un firewall y es accesible solo para las personas que son miembros de la misma empresa u organización, una Extranet proporciona varios niveles de accesibilidad a los foráneos. Puede acceder a una Extranet sólo si dispone de un nombre de usuario y contraseña válidos y de acuerdo a esta información, se decide que partes de la Intranet puede ver. Las Extranets ayudan a extender el alcance de las aplicaciones y los servicios basados en Intranet, asegurando el acceso a empresas y usuarios externos.

Las Extranets enlazan clientes, proveedores, socios o comunidades de interés a una intranet corporativa sobre una infraestructura compartida utilizando conexiones dedicadas.

1.9.- Resumen Clasificación de las redes de computadoras

Por capa de red Clasificar según la capa de red en la cual funcionan según algunos modelos de la referencia básica que se consideren ser estándares en la industria tal como el modelo OSI de siete capas y el modelo del TCP/IP de cinco capas.

Por la escala Las redes de computadoras se pueden clasificar según la escala o el grado del alcance de la red, por ejemplo como red personal del área (PAN), la red de área local (LAN), red del área del campus (CAN), red de área metropolitana (MAN), o la red de área amplia (WAN).

Por método de la conexión Las redes de computadoras se pueden clasificar según la tecnología que se utiliza para conectar los dispositivos individuales en la red tal como HomePNA, línea comunicación, Ethernet, o LAN sin hilos de energía.

Por la relación funcional Las redes de computadores se pueden clasificar según las relaciones funcionales que existen entre los elementos de la red, servidor activo por ejemplo del establecimiento de una red, de cliente y arquitecturas del Par-a-par (workgroup). También, las redes de computadoras son utilizadas para enviar datos a partir del uno a otro por el hardrive.

Por topología de la red Define como están conectadas computadoras, impresoras, dispositivos de red y otros dispositivos. En otras palabras, una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

Las topologías son las siguientes: bus, anillo o doble anillo, estrella, estrella extendida, jerárquica y malla.

Por los servicios proporcionados Las redes de computadoras se pueden clasificar según los servicios que proporcionan, por ejemplo redes del almacén, granjas del servidor, redes del control de proceso, red de valor añadido, red sin hilos de la comunidad, etc.

Por protocolo Las redes de computadoras se pueden clasificar según el protocolo de comunicaciones que se está utilizando en la red. Ver los artículos sobre la lista de los apilados del protocolo de red y la lista de los protocolos de red.

1.10.-Finalidad de la Tesis

En esta tesis, me enfoqué en las amenazas de seguridad y algunos problemas en las redes móviles Ad Hoc. Los problemas de seguridad van a ser analizados desde las capas individuales (sobre todo en la capa de aplicación, capa de transporte, capa de red, capa de enlace y la capa física. De esta manera me es más sencillo explicar con claridad los diferentes escenarios en cada capa. Las soluciones de los problemas de seguridad también son expuestas. En esta tesis trato de proveer un entendimiento de la mayoría de los problemas a los que se enfrentan las redes Ad Hoc en materia de seguridad. En general trate de responder las siguientes preguntas:

- ¿Cuáles son las vulnerabilidades en materia de seguridad en las redes móviles Ad Hoc?, ¿Qué capas son las más vulnerables a los ataques?
- ¿Qué servicios de seguridad, tales como, confidencialidad, integridad y autentificación pueden ser implementados en las redes móviles Ad Hoc? ¿Qué es lo que se requiere?
- ¿Cuáles son las contramedidas para los ataques? ¿Cómo está asegurado el sistema entero?
- ¿Cuáles son los riesgos futuros?

1.11.-Organización de la Tesis

Esta tesis está organizada de la siguiente manera:

Capítulo I.- Introducción a las redes de computadoras y finalidad de la tesis.

Capítulo II.- Redes Ad Hoc características y vulnerabilidades.

Capítulo III.- Exploits de seguridad y tipos de ataques en las redes Ad Hoc.

Capítulo IV.- Amenazas de Seguridad.

Capítulo V.-. Soluciones o contramedidas.

Conclusiones.

Las siguientes tablas [15] [16] son un resumen de los ataques y su solución

Tabla 1.1 Ataques de seguridad en las capas de las redes móviles Ad Hoc

Capa	Ataques
Capa de Aplicación	Repudio, Corrupción de la información
Capa de Transporte	Secuestro de Sesión, Inundación SYN
Capa de Red	Hoyo de gusano, agujero negro, Bizantino, Flooding, consumir recursos, Ataques de descubrimiento
Capa de enlace de datos	Análisis del tráfico, monitoreo, debilidades WEP
Capa Física	Jamming, intercepciones, escuchas

Tabla 1.2 Soluciones de seguridad para las rede móviles Ad Hoc

Capa	Soluciones
Capa de Aplicación	Detección y prevención de virus, gusanos, códigos maliciosos, y abusos de las aplicaciones
Capa de Transporte	Autentificación y aseguramiento de los puntos de comunicación P2P mediante la encriptación de datos
Capa de Red	Proteger los protocolos de enrutamiento y envió de la red Ad Hoc
Capa de enlace de datos	Proteger los protocolos de las MAC inalámbricas y proporcionar soporte a las capas de enlace
Capa Física	Prevenir el jamming de la señal y las ataques DoS

1.12 Mi investigación

La seguridad debe de tomarse en consideración a la hora de diseñar la red. En mi investigación, identifique los riesgos de seguridad en cada capa y sus posibles soluciones. En la siguiente tabla se puede apreciar los posibles ataques y su posible solución.

Tabla 1.3 Riesgos de seguridad y Soluciones o Contramedidas

Capa	Ataques	Soluciones
Capa de Aplicación	Ataques de falta de cooperación, Ataques de código malicioso (virus, gusanos, spyware,	Aplicar mecanismos de cooperación (Confianza, CORE (Cooperation Enforcement Based on

	Troyanos)	Reputation)), Firewalls, Identificaciones, etc.
Capa de Transporte	Secuestro de la sesión, Inundación SYN, ataques de tormenta TCP/ACK etc.	Autentificar y asegurar las comunicaciones P2P, usando criptografía (SSL,TLS,SET,PCT)
Capa de Red	Ataques a los protocolos de enrutamiento, envenenamiento del cache, desbordamiento de tabla, hoyos de gusano, agujeros negros, Bizantino, Flooding, consumo de recursos, personificación, ataques de descubrimiento etc.	Autentificación segura y mecanismos para verificar la integridad de los mensajes y así prevenir su modificación, protocolos de enrutamientos seguros (IPsec,ESP,SAR, ARAN) para prevenir los agujeros negros, Packet Leashes, Mecanismos SECTOR para los ataques de gusano
Capa de enlace de datos	Análisis de tráfico, monitoreo, disrupción MAC, debilidades WEP	Desafortunadamente no hay un mecanismo efectivo para prevenir el análisis y monitoreo de señales, asegurar las capas de enlace con protocolos como LLSP, usar WPA
Capa Física	Jamming, intercepciones, escucha	Usar mecanismo de espectro amplio FHSS,DSSS etc.

CAPÍTULO

II

REDES AD HOC CARACTERÍSTICAS Y VULNERABILIDADES.

2.1.- Introducción

Una red Ad Hoc es una colección de nodos inalámbricos y móviles que conforman una red temporal sin la necesidad de una administración centralizada. En una red así, a veces es necesario que un nodo enliste a otros anfitriones (Host es el termino comúnmente utilizado) para que re direccione los paquetes de datos para otros dispositivos móviles que no estén en rango de transmisión con los demás. Cada nodo opera, no solamente como anfitrión, sino como un router que retransmite los datos de otros nodos que no estén en rango de transmisión. Cada nodo tiene un protocolo de enrutamiento que le permite descubrir rutas Multihop (término acuñado por Cisco) en la red hacia otro dispositivo. Las redes móviles Ad Hoc también son conocidas como redes sin infraestructura (infrastructureless networking), ya que los nodos móviles en la red dinámicamente establecen enrutamiento entre sí para formar su propia red sobre la marcha [2].

Una diferencia esencial entre las redes Ehernet y las inalámbricas es que estas últimas se construyen en un *medio compartido*. Se parecen más a los viejos concentradores de red que a los conmutadores modernos, en ellas cada computadora conectada a la red puede "ver" el tráfico de todos los otros usuarios. Para monitorear todo el tráfico de la red en un punto de acceso, uno puede simplemente sintonizar el canal que se está utilizando, colocar la tarjeta de red en el modo de monitoreo, y registrar cada paquete. Estos datos pueden ser de mucho valor para alguien que los escucha a escondidas (incluyendo datos como el correo electrónico, datos de voz o registros de conversaciones en línea). Esto también puede proveer contraseñas y otros datos de gran valor, posibilitando que la red se vea comprometida en el futuro. Como veremos más adelante en este capítulo, este problema puede mitigarse con el uso de la encriptación.

Otro problema serio de las redes inalámbricas es que los usuarios son relativamente *anónimos*. Todos los dispositivos inalámbricos incluyen una dirección MAC única, la cual es asignada por el fabricante, pero esas direcciones a menudo pueden ser modificadas con ciertos programas. Aun teniendo la dirección MAC, puede ser muy difícil identificar donde está localizado físicamente un usuario inalámbrico. Los efectos

del eco, las antenas de gran ganancia, y una amplia variedad de características de los transmisores de radio, pueden hacer que sea imposible determinar si un usuario malintencionado está en el cuarto de al lado o en un lujar muy alejado.

Si bien el espectro sin licenciamiento implica grandes ahorros económicos para el usuario, por otro lado tiene el desafortunado efecto colateral de que los ataques de *denegación del servicio* (*DoS* por su sigla en inglés) son extremadamente simples. Simplemente con encender un punto de acceso.

De alta potencia, un teléfono inalámbrico, un transmisor de video, o cualquier otro dispositivo de 2.4 GHz, una persona con malas intenciones puede causar problemas significativos a la red. Muchos dispositivos de red son vulnerables también a otras formas de ataques de denegación del servicio, tales como una avalancha de des asociaciones (disassociation flooding) y el desborde de las tablas ARP.

2.2.-QoS o Calidad de Servicio

Son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.

2.3.-Problemas en redes de datos conmutados

Muchas cosas le ocurren a los paquetes desde su origen al destino, resultando los siguientes problemas vistos desde el punto de vista del transmisor y receptor:

2.3.1.-Paquetes sueltos

Los ruteadores pueden fallar en liberar algunos paquetes si ellos llegan cuando los buffers ya están llenos. Algunos, ninguno o todos los paquetes pueden quedar sueltos dependiendo del estado de la red, y es imposible determinar que pasará de antemano. La aplicación del receptor puede preguntar por la información que será retransmitida posiblemente causando largos retardos a lo largo de la transmisión.

2.3.2.-Retardos

Puede ocurrir que los paquetes tomen un largo período en alcanzar su destino, debido a que pueden permanecer en largas colas o tomen una ruta menos directa para prevenir la congestión de la red. En algunos casos, los retardos excesivos pueden inutilizar aplicaciones tales como VoIP o juegos en línea.

2.2.3.-Jitter

Los paquetes del transmisor pueden llegar a su destino con diferentes retardos. Un retardo de un paquete varía impredeciblemente con su posición en las colas de los ruteadores a lo largo del camino entre el transmisor y el destino. Esta variación en retardo se conoce como jitter y puede afectar seriamente la calidad del flujo de audio y/o video.

2.3.4.-Entrega de paquetes fuera de orden

Cuando un conjunto de paquetes relacionados entre sí son encaminados a Internet, los paquetes pueden tomar diferentes rutas, resultando en diferentes retardos. Esto ocasiona que los paquetes lleguen en diferente orden de cómo fueron enviados. Este problema requiere un protocolo que pueda arreglar los paquetes fuera de orden a un estado isócrono una vez que ellos lleguen a su destino. Esto es especialmente importante para flujos de datos de video. y VoIP donde la calidad es dramáticamente afectada tanto por latencia y pérdida de sincronía.

2.3.5.-Errores

A veces, los paquetes son mal dirigidos, combinados entre sí o corrompidos cuando se encaminan. El receptor tiene que detectarlos y justo cuando el paquete es liberado, pregunta al transmisor para repetirlo así mismo.

2.4.-QoS en ATM

Una de las grandes ventajas de ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) respecto de técnicas como el Frame Relay y Fast Ethernet es que admite niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo o que garantizarán un ancho de banda específico para un servicio. Esto es posible marcando los paquetes que provengan de una dirección IP determinada de los nodos conectados a un gateway (como por ejemplo la IP de un teléfono IP, según la puerta del router, etc.). Además, en los servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

Una red IP está basada en el envío de paquetes de datos. Estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama ToS (Type of Service), en realidad pensada para llevar banderas o marcas. Lo que se puede hacer para darle prioridad a un paquete sobre el resto es marcar una de esas banderas (flags, en inglés).

Para ello, el equipo que genera el paquete, por ejemplo una puerta de enlace (gateway, en inglés) de voz sobre IP, coloca una de esas banderas en un estado determinado. Los dispositivos por donde pasa ese paquete después de ser transmitido deben tener la capacidad para poder discriminar los paquetes para darle prioridad sobre los que no fueron marcados o los que se marcaron con una prioridad menor a los anteriores. De esta manera podemos generar prioridades altas a paquetes que requieren una cierta calidad de envío, como por ejemplo la voz o el vídeo en tiempo real, y menores al resto.

2.5.-QoS en escenarios inalámbricos

El entorno inalámbrico es muy hostil para medidas de Calidad de Servicio debido a su variabilidad con el tiempo, ya que puede mostrar una calidad nula en un cierto instante de tiempo. Esto implica que satisfacer la QoS resulta imposible para el 100% de los casos, lo que representa un serio desafío para la implementación de restricciones de máximo retardo y máxima varianza en el retardo (jitter) en sistemas inalámbricos.

Los sistemas de comunicaciones ya estandarizados con restricciones QoS de retardo y jitter en entornos inalámbricos (por ejemplo en GSM y UMTS) sólo pueden garantizar los requisitos para un porcentaje (<100%) de los casos. Esto implica una caída del servicio (Outage o downtime en inglés), generando los cortes de llamadas y/o los mensajes de "red ocupada". Por otro lado, algunas aplicaciones de datos (por ejemplo, WiFi) no requieren de restricciones de máximo retardo y jitter, por lo que su transmisión sólo necesita de calidad media.

2.6.-Soluciones para la calidad de servicio

El concepto de QoS ha sido definido dentro del proyecto europeo Medea+PlaNetS, proporcionando un término común para la evaluación de las prestaciones de las comunicaciones en red, donde coexisten aplicaciones sin requisitos de retardo con otras aplicaciones con estrictas restricciones de máximo retardo y jitter. Dentro de PlaNetS, cuatro diferentes clases de aplicaciones han sido definidas, donde cada clase se distingue por sus propios valores de máximo retardo y jitter.

Conversación: caracterizada por la más alta prioridad y los requerimientos de menor retardo y jitter.

Streaming: flujo de vídeo o voz.

Servicios interactivos.

Aplicaciones secundarias: la más baja prioridad y mayor permisividad de retardo y jitter.

Los beneficios de la solución PlaNetS se resumen en:

La posibilidad de pre-calcular el máximo retardo y jitter de la comunicación; y para cada una de las clases de aplicaciones.

La solución propuesta es implementada con un simple scheduler que conoce la longitud de las colas de paquetes.

La conformidad de los nodos de la comunicación es fácilmente comprobable.

Una mayor QoS, tanto para el sistema como para el usuario final.

La posibilidad de obtener esquemas prácticos de control de acceso (Connection Admission Control, (CAC), en inglés).

QoS o Calidad de Servicio (*Quality of Service*, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

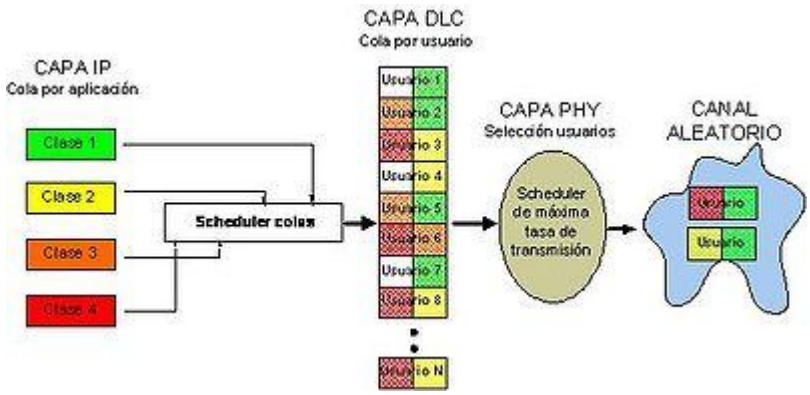


Figura 2.1: Las cuatro diferentes clases de servicios en Medea+ PlaNetS

2.7.-Calidad de servicio utilizando UPnP

UPnP es una tecnología desarrollada por el UPnP Forum que permite a los dispositivos en una red formar comunidades y compartir servicios. Cada dispositivo se ve como colección de uno o más dispositivos y servicios empotrados no necesitando establecer ninguna conexión preliminar o persistente para comunicarse con otro dispositivo. Existe un punto de control que descubre los dispositivos y sincroniza su interacción. Esta tecnología se usa sobre todo en el entorno multimedia, pudiéndola utilizar en dispositivos comerciales como la XBOX 360 (compartir archivos multimedia entre la videoconsola y el ordenador), la generación de móviles N de Nokia, etc.

Dentro del UPnP Forum se trabaja en la especificación de arquitecturas de calidad de servicio, y considerando la calidad de servicio local, es decir dentro de la red local. La segunda versión de la especificación de la arquitectura de calidad de servicio UPnP se ha publicado, donde la especificación no define ningún tipo de dispositivo, sino un framework de UPnP QoS formado básicamente por tres distintos servicios. Estos servicios, por lo tanto, van a ser ofrecidos por otros dispositivos UPnP. Los tres servicios son:

1. QosDevice
2. QosPolicyHolder
3. QosManager

La relación entre estos servicios puede verse en la figura 2.2 en la que se muestra un diagrama con la arquitectura UPnP QoS.

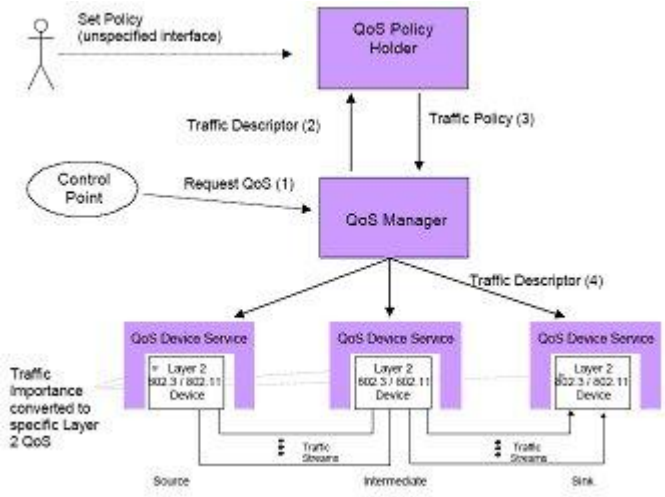


Figura 2.2: la arquitectura UPnP QoS.

En la figura se aprecia que un punto de control es el que inicia la comunicación (por ejemplo, puede ser un punto de control multimedia). Este punto de control tiene información del contenido a transmitir, origen y destino de la transmisión, así como de la especificación del tráfico. Con esta información, accede al gestor de QoS (QosManager), que a su vez actúa como punto de control para la arquitectura QoS. El QosManager consulta al QosPolicyHolder para establecer las políticas para el tráfico (básicamente para establecer la prioridad de ese flujo de tráfico).

El QosManager calcula además los puntos intermedios en la ruta desde el origen al destino del flujo, y con la información de la política, configura los QosDevices que hay en dicha ruta. En función de los dispositivos QosDevices, o bien ellos mismos o bien la pasarela pueden realizar control de admisión de flujos.

Estas interacciones entre los distintos componentes de la arquitectura se reflejan en la figura 2.3.

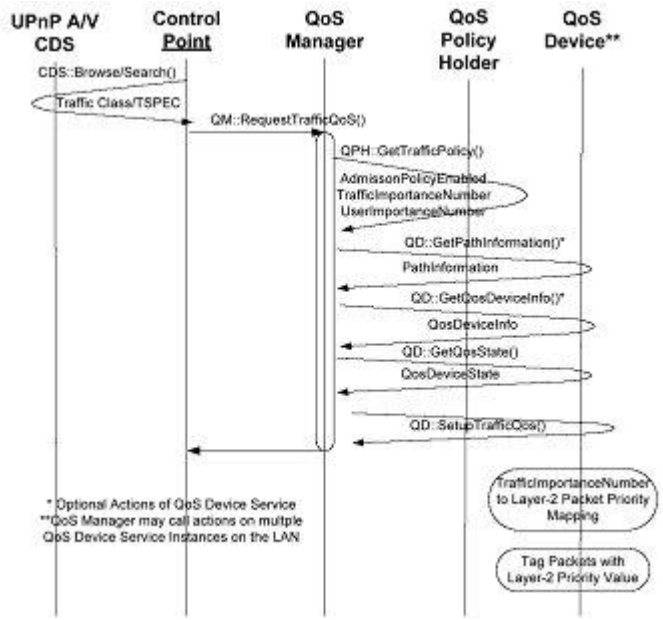


Figura 2.3: las interacciones de la arquitectura.

2.8.-Vulnerabilidades de las Redes Inalámbricas

Les presento varias categorías de personas que pueden causar problemas a una red inalámbrica:

- Usuarios involuntarios. Como la mayoría de las redes inalámbricas están instaladas en áreas muy pobladas, es común que los usuarios de computadoras portátiles se asocien accidentalmente a la red equivocada. La mayoría de los clientes va a elegir cualquier red disponible si la de su preferencia no lo está. Los usuarios pueden hacer uso de esta red como lo hacen habitualmente, ignorando completamente que pueden estar transmitiendo datos importantes en la red de alguien más. Las personas malintencionadas pueden aprovechar esta situación instalando puntos de acceso en lugares estratégicos, para intentar atacar usuarios desprevenidos y capturar sus datos. El primer paso para evitar este problema es educar a sus usuarios, y subrayar la importancia de conectarse solamente a redes conocidas y de confianza. Muchos clientes inalámbricos pueden configurarse para conectarse solamente a redes confiables, o para pedir permiso antes de incorporarse a una nueva red. Como veremos más adelante en este capítulo los usuarios pueden conectarse de forma segura a redes públicas abiertas utilizando una encriptación fuerte.

- War drivers. El fenómeno de los "war drivers" (buscadores de redes) basa su nombre en la famosa película sobre piratas informáticos de 1983, "Juegos de Guerra" (War Games). Ellos están interesados en encontrar la ubicación física de las redes inalámbricas. En general se mueven por la ciudad equipados con una computadora portátil, un GPS, y una antena omnidireccional, registrando el nombre y la ubicación de cada red que localizan. Luego se combinan esos registros con los de otros buscadores de redes transformándose en mapas gráficos describiendo las "huellas" inalámbricas de una ciudad. La amplia mayoría de los buscadores de redes no representa una amenaza directa a la red, pero los datos que recolectan pueden ser de interés para aquellos que se dedican a atacar redes. Por ejemplo, un punto de acceso desprotegido detectado de esta manera, puede

estar ubicado en un edificio importante, como una oficina de gobierno o de una empresa. Una persona con malas intenciones puede utilizar esta información para acceder a esa red ilegalmente. La instalación de ese AP nunca debió haber sucedido en primer lugar, pero los buscadores de redes hacen más urgente la solución de este problema. Como veremos más adelante en este capítulo, los buscadores de redes que utilizan el famoso programa NetStumbler pueden ser detectados con otros programas como el Kismet.

- Puntos de acceso deshonestos. Hay dos clases generales de puntos de acceso deshonestos: aquellos instalados incorrectamente por usuarios legítimos, y los instalados por gente malintencionada que piensa en recolectar datos o dañar la red. En el caso más sencillo, un usuario legítimo de la red, puede querer una mejor cobertura inalámbrica en su oficina, o puede que encuentre demasiado difíciles de cumplir las restricciones de seguridad de la red inalámbrica corporativa. Al instalar un punto de acceso sin autorización, el usuario abre la red desde el interior de la misma a los ataques potenciales. Si bien existe la posibilidad de rastrear a través de la red puntos de acceso no autorizados, es muy importante tener una política clara que los prohíba. Puede que sea muy difícil lidiar con la segunda clase. Al instalar un AP de gran potencia que utilice el mismo ESSID de la red, una persona puede engañar a la gente para que use este equipo y registrar o manipular todos los datos que pasan por él. Repetimos, si sus usuarios están entrenados para usar una fuerte encriptación, este problema se va a deducir de forma significativa.

- Escuchas Subrepticias. Este es un problema muy difícil de manejar en las redes inalámbricas. Utilizando una herramienta de monitoreo pasiva (como Kismet), un fisgón puede registrar todos los datos de la red desde lejos sin que ni siquiera se note su presencia. Los datos encriptados pobremente simplemente pueden registrarse y luego descifrarse, mientras que los datos sin encriptación se pueden leer fácilmente en tiempo real.

2.9.- Trasfondo

En nuestros días las redes móviles Ad Hoc es uno de los recientes campos de la informática que han recibido mucha atención debido a su capacidad de auto-configuración y auto-mantenimiento [16]. En las primeras investigaciones se trabaja asumiendo que el ambiente era amistoso y cooperativo, por lo que se enfocaron en solucionar problemas como los canales de acceso inalámbricos y el enrutamiento multihop, con esos problemas bajo control la seguridad se ha vuelto el foco de atención para proveer protección en ambientes potencialmente hostiles. Estudios recientes indican que la redes móviles inalámbricas Ad Hoc presentan una mayor inseguridad en comparación con las redes alámbricas e inalámbricas comunes.

Aunque las redes móviles Ad Hoc tienen muchas ventajas sobre las tradicionales redes alámbricas, presentan algunos problemas únicos. En primera, las redes móviles Ad hoc presentan problemas en las comunicaciones seguras. Por ejemplo los recursos limitados de los nodos en las redes Ad Hoc limitan las medidas criptográficas usadas para los mensajes seguros. Por lo que es son susceptibles a ataques que van desde a la escucha pasiva a la personificación activa, respuesta a los mensajes o alteración de ellos. Segundo, los nodos móviles sin la protección adecuada son fáciles de comprometer. Un atacante puede escuchar, modificar e intentar enmascarar todo el tráfico en los canales de comunicación inalámbrica como si fuera un nodo auténtico en la red. Tercero, la configuración estática como solución de seguridad puede no ser la más adecuada para la topología dinámica. Varios ataques como la Negación del servicio (DoS por sus siglas en inglés) pueden ser fácilmente iniciados e inundar la red con mensajes de enrutamiento falsos por medio de un nodo malicioso que provea de información de actualización incorrecta pretendiendo ser una cambio en el enrutamiento de la información legítimo. Finalmente, la falta de cooperación y la capacidad limitada son una constante en lo las redes móviles inalámbricas Ad hoc lo que se traduce en una dificultad para distinguir anomalía alguna. En general las redes móviles Ad Hoc son particularmente vulnerables debido a sus características como ser un medio abierto, topología dinámica, la ausencia de centrales de autentificación, cooperación distribuida y las capacidades limitadas.

2.10.- Estudios Relacionados.

Actualmente se están realizando investigaciones en los problemas y soluciones de seguridad en las redes móviles Ad Hoc. Zhou y Haas and propuesto usar criptografía del umbral para proveer seguridad en la red [18]. Hubauz et al. Definieron un método que está diseñado para asegurar la participación equitativa entre miembros de un grupo Ad Hoc, lo que le permite a cado noto expedir certificados [3]. Kong, et al. [8] propuso un protocolo seguro basado en compartición secreta; desafortunadamente, este protocolo está basado en asumpciones incorrectas, como que cada nodo no puede ser personificar la dirección MAC de múltiples nodos. Yi et al, también diseñó un cuadro general por enrutamiento seguro en las Ad Hoc [17]. Deng, et al. Se ha centrado en el problema del enrutamiento inseguro en la redes móviles Ad Hoc y ha descrito una solución al problema del "Agujero negro" [2]. Sanzgirim, et al. Propuso el protocolo de enrutamiento seguro ARAN el cual está basado en certificado y que ha probado detener todos los ataques identificados [14]. Yang, et al. Identificó los problemas de seguridad relacionados con la conectividad multihop, discutió los problemas para el diseño de seguridad, y revisó el estado del arte de las propuestas de seguridad que protegen las operaciones de entrega de paquetes en los canales inalámbricos multihop de las redes móviles ad hoc (en las capas de enlace y red) [16]. En esta tesis, me enfoque más que nada en los problemas de seguridad en la capa de enlace y la capa de red.

CAPÍTULO

III

EXPLOITS DE SEGURIDAD Y TIPOS DE ATAQUES EN LAS REDES AD HOC.

3.1.-Servicios de Seguridad

El propósito de las soluciones de seguridad para las redes móviles Ad Hoc es proveer servicios de seguridad como autentificación, confidencialidad, integridad, anti-repudiación, anonimidad y disponibilidad para los usuarios móviles. Para asegurar estos, las soluciones de seguridad deben de proveer protección completa. Se debe de tener en cuenta que no hay un mecanismo que por sí solo provea seguridad total para las redes móviles Ad Hoc. Los servicios de seguridad más comunes son:

3.1.1.-Disponibilidad

La disponibilidad está ligada con la defensa de los recursos. Una variedad de ataques pueden desencadenar en una pérdida o reducción de disponibilidad. Algunos de esos ataques pueden ser detenidos con medidas como la autentificación y la encriptación mientras que otros ataques necesitan algún tipo de acción para recuperar o prevenir una pérdida de disponibilidad de algunos de los elementos o servicios de un sistema distribuido. La disponibilidad asegura la supervivencia de los servicios de red aunque esta esté bajo ataque. Por ejemplo, en las capas de control de acceso al medio, el atacante podría usar jamming para interferir con la comunicación en un canal físico mientras que en la capa de red esto podría interrumpir el protocolo de enrutamiento y la continuidad de los servicios de red. En niveles superiores, un adversario podría tirar servicios de nivel superior como el servicio de administración de llaves y los servicios de autentificación [18].

3.1.2.-Confidencialidad

La confidencialidad asegurar que la información solo pueda ser leída o accesada por receptor autorizado. Básicamente, protege la información de ataques pasivos. La transmisión de información importante requiere confidencialidad. Revelar esta información a receptores no autorizados puede tener consecuencias graves. El enrutamiento y reenvió de información también debe permanecer confidencial para que el atacante no pueda poseer más blancos a atacar. Con respecto a mostrar el contenido del mensaje, diferentes niveles de protección pueden ser identificados.

3.1.3.-Integridad

La integridad garantiza que los usuarios autorizados son los únicos con permisos para modificar la información o los mensajes. A si mismo asegura que la información transmitida no pueda ser corrompida. Tal como con la confidencialidad, la integridad aplica para el flujo de datos. Pero lo mejor de la integridad es la completa protección del flujo de datos. Una conexión orientada a la integridad del servicio, una que se encargue del flujo de datos, asume que todos los mensajes fueron recibidos, sin duplicación, inserciones, modificaciones, reordenamiento o reproducciones. La destrucción de la información también está protegida por los servicios de integridad ya que. Además de que soluciona los problemas de modificación del flujo de información y de negación del servicio.

3.1.4.-Autentificación

La autentificación se asegura de que el acceso y el abasto de datos sea hecho solamente por los usuarios autorizados, es una preocupación asegurar que la comunicación sea autentica. En el caso de un mensaje, como una alerta o una señal de alarma, la función de la autentificación es asegurarse de que el que recibe la señal la reciba del emisor que dice ser. Sin la autentificación, un invasor se puede enmascarar como un nodo. Y así ganar acceso, sin estar autorizado, a información sensible o servicios de seguridad e interferir con la operación de otros nodos [18].

3.1.5.-Anti-repudiación

La anti repudiación previene que, tanto el emisor como el receptor, nieguen transmitir/recibir un mensaje, y de esta manera el receptor pueden comprobar que el mensaje proviene de la fuente que dice ser. Por otra parte, después de enviar el mensaje, el emisor puede comprobar que el mensaje fue recibido por el receptor que dice ser. La anti-repudiación es útil para detectar y aislar nodos problemáticos. Cuando el nodo A recibe un mensaje erróneo desde el nodo B, la anti-repudiación permite al nodo A proveer información para comprobar que el nodo B está comprometido.

3.1.6.-Escalabilidad

La escalabilidad no está relacionada directamente con la seguridad pero es un problema muy importante que tiene un gran impacto en los servicios de seguridad. Una red Ad Hoc puede consistir en cientos de nodos. Los mecanismos de seguridad deben de ser escalables para poder manejar una red tan grande [18]. De otro modo, el nuevo nodo en la red podría estar vulnerable a un ataque y así ser usado para ganar acceso no autorizado al sistema. Es extremadamente sencillo hacer un ataque mediante un nodo comprometido en una red.

3.2.- Tipos de ataques.

Las redes móviles Ad hoc actuales permiten diferentes tipos de ataques. Aunque muchos de estas vulnerabilidades también existen en las redes alámbricas pero que son fácilmente solucionables mediante infraestructura en estas redes. Actualmente las redes móviles Ad Hoc son básicamente vulnerables a dos tipos de ataques: Los ataques activos y los ataques pasivos. Un ataque activo es un ataque en el que un nodo tiene que actuar para producir la amenaza. Un ataque pasivo se produce gracias a la falta de cooperación, a veces producidos por la necesidad de ahorrar energía. Los nodos que realizan ataques activos con el propósito de dañar otros nodos mediante pausar la red son considerados maliciosos mientras que los nodos que realizan ataques pasivos con el propósito de ahorrar energía para sus comunicaciones son considerados como egoístas. En este capítulo he clasificado los ataques como de modificación, personificación, fabricación, hoyos de gusanos y falta de cooperación.

3.2.1.-Ataques usando modificación

Los ataques de modificación es un tipo de ataque que cuando un usuario no autorizado obtiene acceso y además manipula un activo. Por ejemplo un código maliciosos puede re direccionar el tráfico de red y conducir un ataque de negación de servicio modificando mensajes de campo o reenviando mensajes de enrutamiento con valores falsos. En la figura 5.1, M es un nodo maliciosos que puede evitar el tráfico a X continuamente diciéndole a B una ruta más corta a X que la ruta a X que promueve C [14]. De esta manera los nodos maliciosos fácilmente pueden crear una negación del servicio (DoS) simplemente alterando los campos de los protocolos. Estos ataques comprometen la integridad del enrutamiento. Mediante modificaciones, un atacante puede causar fallas en el tráfico de red, re direccionándolo a un destino diferente o dándole una ruta más larga para llegar a destino causando un retraso innecesario.

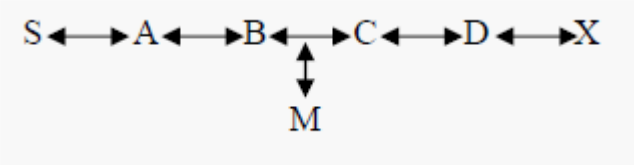


Figura 3.1. Red Ad Hoc con un nodo malicioso

En la figura 3.2 se asume que existe un camino más corto entre S y X, además C y X no se pueden oír el uno al otro, y que los nodos B y C no se pueden escuchar el uno al otro, y que M en un nodo maliciosos intentando una negación del servicio (DoS). Supuestamente S desea comunicarse con X y que S no tiene en su cache la ruta a X. S transmite un paquete de datos a X con su ruta S → A→ B→M→C→D→X contenido en el header. Cuando M recibe el paquete, puede alterar la ruta en el Header, como por ejemplo borrando D de la ruta. Por lo que cuando C recibe el paquete alterado trata de comunicarse con X y como X no puede escuchar a C, la transmisión es infructuosa.

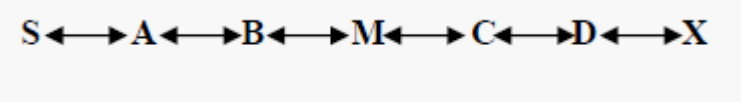


Figura 5.2 una red Ad hoc con DoS

3.2.2.-Ataques usando personificación

Mientras que no haya autentificación de los paquetes de datos en las redes Ad Hoc, un nodo malicioso podría lanzar muchos ataques a la red enmascarándose como otro nodo, por ejemplo suplantación. La suplantación ocurre cuando un nodo malicioso enmascara su identidad en la red (alterando su MAC o su dirección IP en algún paquete de salida) y altera en objetivo en la topología de la red a la que un nodo podría acceder. Por ejemplo, un ataque de suplantación permite formar loops en el enrutamiento de paquetes que a su vez podría dividir la red, En la figura se muestra este escenario.

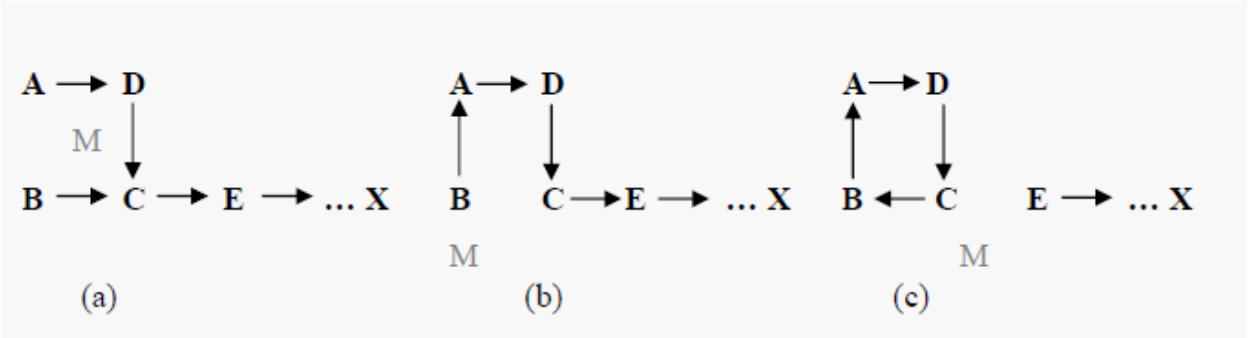


Figura 3.3 una secuencia de evento formando loops mediante paquetes falsos.

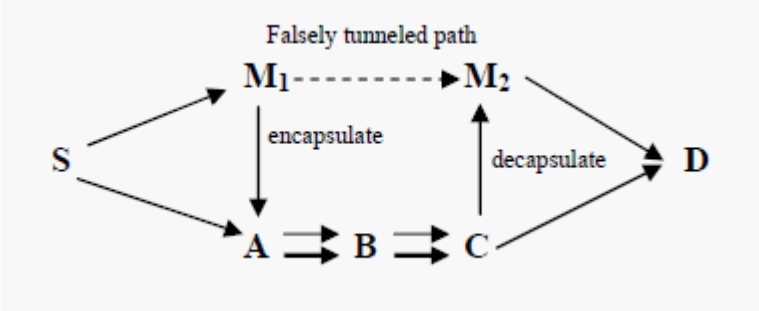
En la figura 3.3(a) existe un camino entre 5 nodos. A puede escuchar a B y D, B puede escuchar A y C, D puede escuchar A y C, y C puede escuchar B, D y E. M puede escuchar A,B,C y D mientras que E puede escuchar C y el próximo nodo en la ruta hacia X. Un nodo malicioso M cambia su dirección MAC para igualar a A, y se mueve cerca de B y fuera del rango de A. Manda un mensaje a B que contiene un numero se saltó hacia X que es menor que el que fue enviado por C, por ejemplo cero. Ahora B cambia su ruta hacia su destino hacia X para ir a través de A como se muestra en la figura 5.3. (b). De nuevo M cambia su dirección MAC para igualar a la de B, se mueve cerca de C y fuera de rango de B. Entonces manda su mensaje a C con la información de que la ruta a través de B contiene un numero de saltos menor que mediante E. C cambiar su ruta hacia B lo cual forma un loop tal y como se muestra en la figura 5.3(c). Por lo que X no puede ser alcanzada por ninguno de los cuatro nodos en la red.

3.2.3.-Ataques mediante fabricación

Fabricación es un ataque en el cual una parte no autorizada no solo gana acceso sino que también inserta objetos falsificados en el sistema. En las redes móviles Ad Hoc, la fabricación es usada para referirse a los ataques realizados mediante generar mensajes falsos de enrutamiento. Este tipo de ataques pueden ser muy difíciles de verificar ya que contienen una construcción valida, especialmente en el caso de mensajes de error fabricados que dicen que un vecino no puede ser contactado [11]. Considerando la figura 5.1 Supuestamente el nodo S tiene la ruta hacia X mediante los nodos A, B, y D. un nodo malicioso M puede lanzar un ataque de negación del servicio contra X mandando continuos mensajes de error a B y suplantar el nodo C, indicando que un enlace roto entre los nodos C y X. b recibe el mensaje de error falsificado pensando que viene de C. B borra de su tabla de enrutamiento a X y reenvía el mensaje a A, quien a su vez borra su tabla de enrutamiento. Si M escucha y transmite mensajes de error de enrutamiento falsos cada que una ruta es establecida desde S hacia X, M puede prevenir la comunicación entre S y X [14].

3.2.4.-Ataques de hoyos de gusano

Los ataques de hoyo de gusano son también conocidos como ataques de tunneling. Un ataque de tunneling es donde dos o más nodos pueden colaborar para encapsular e intercambiar mensajes entre ellos mediante rutas de datos existentes. Este exploit le da la oportunidad a un nodo o a múltiples nodos para corto circuitar el flujo normal de mensajes creando un vértice virtual en la red que es controlado mediante dos atacantes coludidos. En la figura 5.4 M1 y M2 son dos nodos maliciosos que encapsulan paquetes de datos y falsifican en tamaño de la ruta.



Supuestamente el nodo S desea formar una ruta hacia D e inicia el descubrimiento de la ruta. Cuando M1 recibe un RREQ de S, M1 encapsula el RREQ y lo "tunelea" hacia M2, mediante una ruta de datos existentes en este caso {m1→A→B→C→M2}. Cuando m2 recibe el RREQ encapsulado y lo dirige hacia D como si solo hubiera viajado {S→M1→M2→D}. Ni M1 y M2 actualizan el encabezado del paquete. Después de descubrir la ruta, el destinatario descubre dos rutas desde S con longitudes diferentes; una de 5 y la otra de 4. Si M2 "tunelea" el RREP de regreso a M1, S asumirá falsamente que la ruta hacia D vía M1 es mejor que la ruta hacia D vía A. Esto significa que el tunneling puede prevenir que nodos honestos puedan actualizar la métrica usada para medir la distancia entre los diferentes caminos.

3.2.5.-Falta de cooperación

Las redes móviles Ad Hoc se fían de la cooperación entre todos los nodos participante. Entre más nodo cooperen para transferir el trafico la red móvil Ad Hoc se vuelve más poderos. Pero uno de las malas conductas que se pueden presentar en los nodos es el egoísmo, esto es que quiera preservar sus propios recursos mientras que usa los servicios de otros y consume sus recursos. Esto pone en peligro el correcto funcionamiento de la red, al no participar en la operación o al no reenviar los paquetes. Este tipo de ataques se conoce como agujero negro y es descrito una sección posterior.

3.2.- Resumen

En este capítulo los servicios de seguridad fueron explicados brevemente. Aunque hay muchos otros servicios de seguridad sobre los cuales escribir. Por ejemplo el control de acceso que el que se encarga de limitar y controlar el acceso al sistema y sus aplicaciones mediante los vínculos de comunicación. Otro punto importante es que siembre habrá que balancear los servicios de seguridad y mantener un buen intercambio entre ellos para proveer un buen sistema de seguridad para las redes móviles Ad Hoc.

La seguridad de las redes Ad Hoc depende ampliamente de las seguridades de los protocolos de enrutamiento, la tecnología de transmisión y los sistemas de comunicación usados por los nodos participantes. En este capítulo, mostré los ataques más comunes a las redes móviles Ad Hoc. El resto de la tesis describe las amenazas en cada capa de la pila de protocolos y muestra las soluciones a esos ataques.

CAPÍTULO IV

AMENAZAS DE SEGURIDAD

4.1.- Amenazas de seguridad en la capa física

La seguridad en la capa física es importante para asegurar las redes móviles Ad Hoc ya que muchos ataques se producen en esta capa. La capa física se debe de adaptar a los rápidos cambios en las características de los enlaces. El ataque más común en la capa física en las redes móviles Ad Hoc es la escucha, interferencia, negación del servicio y jamming. Las señales más comunes de radio en las redes móviles Ad Hoc es fácil de atascar o interceptar. Por otra parte un atacante puede desestabilizar físicamente una red inalámbrica. Un atacante con suficiente poder de transmisión y conocimiento de diferentes mecanismos de las capas de control puede ganar acceso al medio inalámbrico. En este capítulo describiré los tipos de ataque escucha, interferencia y jamming.

4.1.1.-Escucha

La escucha es la lectura de mensajes u conversaciones por receptores no elegidos. Los nodos en la red móvil Ad Hoc comparten un medio inalámbrico y las comunicaciones usan es espectro RF y por su naturaleza de transmisión puede ser fácilmente interceptado mediante receptores sintonizados en la frecuencia correcta. Como resultado los mensajes transmitidos pueden ser escuchados así como mensajes falsos pueden ser inyectados en la red.

4.1.2.- Interferencia y Jamming

Jamming y la interferencia de las señales de radio pueden causar que una transmisión se pierda o se corrompa. Un transmisor lo suficientemente poderoso puede generar una señal que sea los suficientemente fuerte para opacar la señal del objetivo e interrumpir las comunicaciones. Pulsos y ruido aleatorio son los tipos más comunes de Jamming [15].

4.1.3-Resumen

La topología es altamente dinámica ya que los nodos frecuentemente dejan o se unen a la red, y se mueven en la red a voluntad. De nuevo los canales de comunicación en las redes móviles Ad Hoc se basan en un ancho de banda estrecho y es compartido entre múltiples entidades de red. Este canal está sujeto a interferencias y errores exhibiendo características volátiles en términos de ancho de banda y retrasos. El atacante podría tomar provecho de esas características.

4.2.- Amenazas de seguridad en la capa de sesión

Las redes móviles Ad Hoc son una arquitectura de red abierta multipunto P2P en la cual los protocolos de la capa de sesión mantienen una conexión de un salto entre sus vecinos cercanos. Muchos ataques pueden ser lanzados en la capa de sesión interrumpiendo la cooperación entre los protocolos de esta capa. Los protocolos de los medios de acceso de control (MAC) inalámbricos tienen que coordinar la transmisión de los nodos comunes de comunicación o los medios de transmisión. El protocolo IEEE 802.11 MAC usa mecanismos de resolución de contenido distribuido que están basados en dos diferentes funciones de coordinación. Una es la función de coordinación distribuida (DCF por sus siglas en ingles) el cual es un protocolo de acceso completamente distribuido y el otro es el protocolo de acceso centralizado llamo Función de punto coordinado (PCF por sus siglas en ingles. Para resolver el contenido de un canal entre múltiple anfitriones inalámbricos, DCF usa un mecanismo transportador intuitivo de múltiple acceso con evasión de colisiones o CSMA/CA.

4.2.1.- Amenazas en IEEE 802.11 MAC

El IEEE 802.11 MAC es vulnerable a los ataques de negación de servicio. Para lanzar un ataque DoS el ataque puede explotar el esquema binario del "exponential backoff". Por ejemplo, el atacante puede corromper los frames fácilmente agregando algunos bits o ignorando la transmisión saliente. Entre los nodos participantes, el esquema binario exponencial favorece al último ganador lo que resulta en el efecto captura. El efecto captura significa que los nodos con carga pesada tienen a monopolizar el canal enviando datos continuamente, por lo que vecinos con cargas ligeras tienden a mantenerse a la espera indefinidamente. Los nodos maliciosos pueden tomar ventaja de la vulnerabilidad del efecto captura. Y esto podría causar una reacción en cadena en los niveles superiores de los protocolos usando el esquema de espera, tal como el sistema de gestión TCP de Windows [15].

Otra vulnerabilidad a los ataques DoS está expuesta en el IEEE 802.11 MAC a través del vector de asignación de red (NAV por sus siglas en inglés) transportador de campo

en el RTS/CST (Ready to send/Clear to send) frames. Durante el saludo RTS/CTS, un pequeño frame RTS incluyendo el tiempo necesario para completar el CTS, datos y frames ACK es enviado por el emisor. Todos los vecinos del emisor y del receptor actualizas su campo NAV de acuerdo con el tiempo que escucharon para la duración de la transmisión. El atacante en el vecindario local también es consciente de la duración de las transmisiones salientes y él/ella pueden transmitir algunos bits en este periodo para inducir un error de bits en el frame de la capa de sesión de la víctima mediante interferencia inalámbrica [16].

4.2.2.- Amenazas en IEEE 802.11 WEP

El primer estándar en el esquema de seguridad provisto por IEEE 802.11 es la privacidad equivalente a la alámbrica (WEP por sus siglas en ingles). Básicamente fue diseñada para proveer seguridad para las redes inalámbricas (WLAN). Pero sufre de muchos problemas de diseño y algunas debilidades en el cifrado RC4 usado en WEP. Es bien conocido que WEP es vulnerable a los ataques de privacidad del mensaje e integridad del mensaje y a los ataques de recuperación de llaves cifradas probabilísticamente Algunas de las vulnerabilidades de WEP son:

- La administración de las llaves no está especificado en el protocolo WEP.
- La inicialización de vector usada en WEP está en un campo de 24 bits el cual es enviado en limpio y es parte de RC4 es sensible a ataques de recuperación de llaves cifradas probabilísticamente o comúnmente conocido como un ataque analítico.
- La combinación del uso de un algoritmo integrado no criptográfico, CRC 32 con el flujo entusiasta es un riesgo de seguridad y puede causar ataques de privacidad de mensaje e integridad de mensaje.

4.2.3.-Resumen

La mayoría de los ataques de capa de sesión en las redes móviles Ad Hoc son evitados usando los protocolos más nuevos o bien proponiendo algún protocolo que detenga estas amenazas. Por ejemplo WPA, RSN/AES-CCMP (el cual es un nuevo protocolo que está siendo desarrollado para mejorar la criptografía e incrementar la seguridad). En la actualidad los ataques usando el campo NAV del frame RTS/CTS permanecen sin solución, y es bastante difícil saber cómo detener los ataques DoS que consumen recursos en las redes móviles Ad Hoc.

4.3.- Amenazas de seguridad en las capas de red

En las redes móviles Ad Hoc. Los nodos también funcionan como routers que descubren y mantienen rutas hacia otros nodos en la red. Estableciendo una ruta óptima y eficiente entre los diferentes nodos comunicándose es la primera preocupación en los protocolos de erutación de las redes móviles Ad Hoc. Cualquier ataque en el la fase de enrutamiento interrumpe la comunicación general y la red entera puede quedar paralizada. Por lo que la seguridad en la capa de red juego un importante rol en la seguridad de la red.

4.3.1.- Protocolos de enrutamiento

Un número de protocolos de enrutamiento han sido desarrollados en las redes móviles Ad Hoc. El principal objetivo es proveer comunicación secura y remover los defectos en los protocolos existentes. Pueden ser clasificadas en las siguientes categorías.

4.3.1.1.- Manejo de tablas

En el protocolo de enrutamiento del manejo de tablas, un esquema proactivo es usado. Esto significa que ellos mantienen una información de enrutamiento actualizada constantemente desde cada nodo hasta todos los nodos en una red. Una o más tablas son usadas para almacenar la información de enrutamiento, cambios en la topología de red, etc. para mantener un ambiente de red consistente. Algunos ejemplo comunes son DBF (el sistema distribuido de protocolos de enrutamiento Bellman-Ford) DSDC (Protocolo de enrutamiento altamente dinámico con vector de destino-secuenciado), OLSR (Protocolo de enrutamiento del estado de enlace optimizado) etc.

4.3.1.2.- A petición

Una fuente iniciando un protocolo de enrutamiento a petición (reactivo) es diferente al protocolo de enrutamiento por manejo de tablas. Este crea rutas solo cuando la fuente lo requiere. El protocolo encuentra la ruta a petición inundando la red con paquetes de petición de ruta. Algunos ejemplos de protocolos a petición son: ACOR (Control de admisión habilitado a petición de enrutamiento), DSR (enrutamiento fuente dinámico) etc.

4.3.1.3.- Otros protocolos de enrutamiento

Hay otros dos tipos de protocolos de enrutamiento llamados hibrido y jerárquico. El protocolo de enrutamiento hibrido es una combinación de esquemas proactivos y reactivos. El protocolo jerárquico contiene estrategias de enrutamiento escalables y establece una jerarquía que es seguida en la misma forma que un camino de hormigas. HSLS (protocolo de enrutamiento del estado del enlace de visión turbia) y ZRP (protocolo de enrutamiento de zona) son protocolos híbridos mientras que DDR (algoritmos de enrutamiento distribuido dinámico), HSR (Enrutamiento de estado jerárquico), OORP (protocolo de enrutamiento OrderOne) son ejemplos de protocolos jerárquicos. Otro protocolo usando en las redes móviles Ad Hoc también conocido como protocolo de enrutamiento geográfico. Enrutamiento geográfico se refiere a un conjunto de técnicas para enrutar paquetes de datos en la comunicación de red. ALARM (Enrutamiento asistido de locación adaptativa), GPSR (enrutamiento sin estado perimetral ambiciosos) son protocolos geográficos.

4.3.2.-Ataques a la Capa de red

Un número de ataques en la capa de red han sido identificados y estudiados en estudios de seguridad. Un atacante puede absorber tráfico de red. Inyectándose a sí mismo en el camino entre la fuente y el destino y así controlar el flujo del tráfico de red. Por ejemplo. Como se muestra en la figura 4.1. (a) Y (b), un nodo malicioso M puede inyectarse en el camino del enrutamiento entre el emisor S y el receptor R.

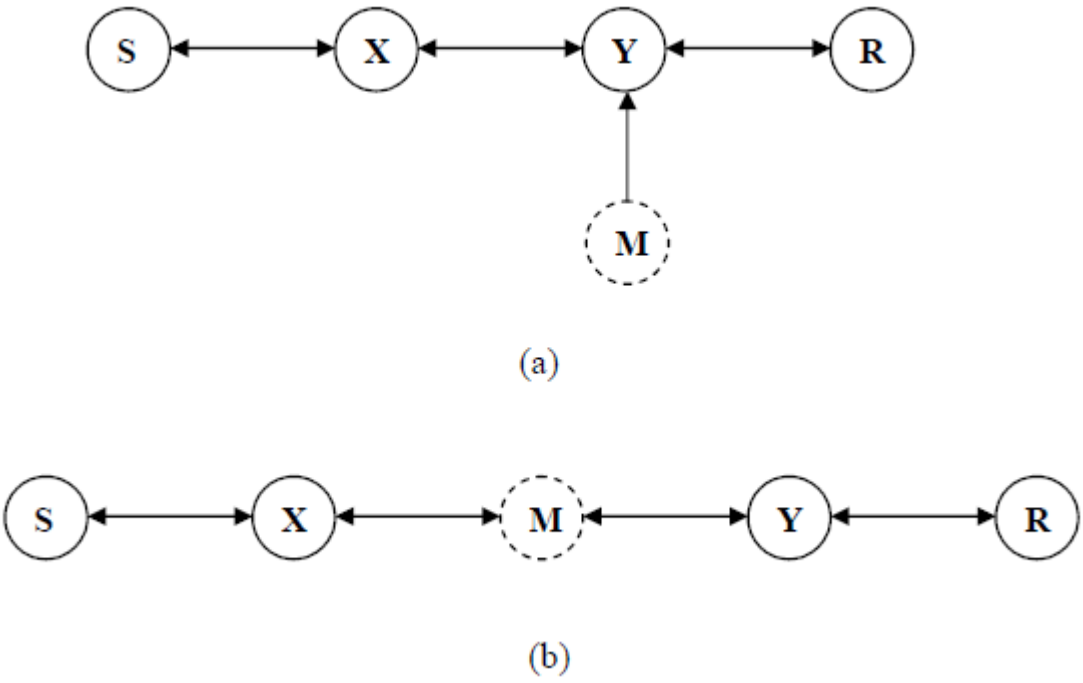


Figura 4.1: Ataque de enrutamiento

Las vulnerabilidades en la capa de red caen en dos categorías: ataques de enrutamiento y ataques de reenvió de paquetes [16]. La familia de ataques de enrutamiento se refiere a cualquier acción de anunciar actualizaciones de enrutamiento, que no siguen las especificaciones de los protocolos de enrutamiento. Las formas de actuar de los ataques específicos están relacionados con los protocolos de enrutamiento de las redes móviles Ad Hoc.

4.3.2.1.- Ataque de desbordamiento de las tablas de enrutamiento

Este ataque básicamente sucede debido a protocolos de enrutamiento proactivos, los cuales actualizan la información de enrutamiento constantemente. Para lanzar un ataque de desbordamiento de las tablas de enrutamiento, el atacante intenta crear rutas que hacia nodos que no existen a los nodos autorizados presentes en la red. Él o ella pueden simplemente enviar excesivos anuncios de ruta para desbordar las tablas de enrutamiento del sistema objetivo. La finalidad es tener suficientes rutas de tal manera que la creación de nuevas rutas es imposible o la implementación de un protocolo de enrutamiento sobrecargado.

4.3.2.2.- Ataque de envenenamiento del cache de enrutamiento

El envenenamiento del cache de enrutamiento usa en su favor el promiscuo modo de actualización de la tabla de enrutamiento. Esto ocurre cuando la información guardad en las tablas de enrutamiento es o borrada o alterada o inyectada con información falsa. Suponiendo que el nodo malicioso M quiere envenenar las rutas hacia el nodo X, M podría transmitir paquetes falsos con la ruta hacia X vía M, por lo que los nodos vecinos que escuchan ese paquete agreguen esa ruta a sus caches [15].

4.3.2.3.-Ataques a un protocolo de enrutamiento particular

Hay muchos ataques en las redes móviles Ad Hoc que tienen como objetivo un protocolo de enrutamiento particular. Esto es debido al desarrollo de servicios de enrutamiento que no consideraron los problemas de seguridad. La mayoría de las investigaciones reciente sufren de ese problema. En esta parte del capítulo describiré acerca de los riesgos de seguridad, ventajas y desventajas de algunos de los protocolos de enrutamiento más comunes.

4.3.2.3.1.-AODV

El algoritmo de enrutamiento Vector de distancia a petición Ad Hoc (AODV) es un algoritmo reactivo que en ruta datos a través de redes inalámbricas. La ventaja de AODC es que es simple, requiere menos memoria y no crea trafico extra para comunicaciones a lo largo de enlaces existentes. En AODV el atacante puede anuncias una ruta con una distancia menor a la distancia original o anuncia una actualización de enrutamiento con una secuencia larda de números e invalidar todas las actualización de otros nodos.

4.3.2.3.2.-DSR

El protocolo de enrutamiento de fuente dinámica (DSR) es similar a AODV en que también forma rutas a petición. Pero la mayor diferencia es que usa enrutamiento fuente en lugar de confiar en la tabla de enrutamiento en cada nodo intermedio. También provee una funcionalidad que permite que los paquetes puedan ser reenviados en una base salto pro salto. En DSR. Es posible modificar la fuente de la ruta listada en los paquetes RREQ o RREP por el atacante. Borrando un nodo de la lista, cambiando el orden o agregando un nuevo nodo a la lista son los posibles riesgos en DSR.

4.3.2.3.4 ARIADNE

ARIADNE es un protocolo de enrutamiento seguro a petición Ad Hoc basado en DSR que implementa una altamente eficiente criptografía simétrica. Este provee autentificación punto a punto de mensajes de enrutamiento usando un mensaje de autentificación código (MAC) y una llave compartida entre dos nodos comunicándose. Aunque ARIADNE no está libre de un flood de paquetes RREQ y ataques de envenenamiento de cache, si es inmune a los hoyos de gusano y a los ataques rafageantes.

4.3.2.3.5.-SEAD

SEAD fue construido en base de la versión protocolo DSDV-SQ del protocolo DSDV (destinación del vector de distancia secuencial). Este se encarga de los atacantes que modifican la información de enrutamiento y también con los ataques de reproducción y hace uso de las cadenas one-way hash en lugar de implementar costosas operaciones de criptografía asimétricas. Dos diferentes aproximaciones son usadas para la autentificación de mensajes para detener a los atacantes. SEAD no es inmune a los ataques de gusano.

4.3.2.4.-Otros ataques avanzados

En investigaciones reciente ataques más sofisticados han sido identificados en las redes móviles Ad Hoc. Algunos protocolos también mejoraron sus servicios y algunos otros protocolos se han propuesto sobrepasar los ataques. Aun así es un área de interés para la seguridad personal. Como sea, el agujero negreo, bizantino, agujero de gusano, ataques relampagueantes son ejemplos típicos y son descritos a continuación.

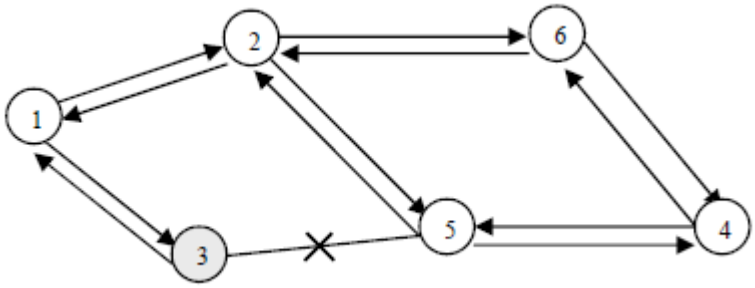
4.3.2.4.1.-Ataque de agujero de gusano

Un ataque de agujero de gusano también es conocido como un ataque de tunneling. Un atacante crea un túnel y usas encapsulación y des encapsulación para crear rutas falsas entre dos nodos maliciosos. En el capítulo 3.4 describí los agujeros de gusano.

4.3.2.4.2.-Ataques de agujeros negros

Los ataques de agujeros negros son ataques ejecutados en dos pasos. En el primer paso, el nodo malicioso explota un protocolo de enrutamiento móvil Ad Hoc como por ejemplo AODV, para anunciarse proclamando tener una ruta valida a el nodo de destino, aunque la ruta sea falsa, con la intención de interceptar paquetes. En el segundo paso, el atacante toma el paquete y nunca lo reenvía. En una forma avanzada el atacante suprime o modifica los paquetes originados en algunos nodos, mientras que deja los datos de otros nodos sin cambio. De esta manera, el atacante falsifica los nodos vecinos que monitorean los paquetes salientes en la figura 4.2 el nodo 1 quiere enviar un paquete de datos al nodo 4 e inicia el proceso para descubrir la ruta. Asumimos que el nodo 3 es un nodo malicioso que dice tener la ruta hacia el destino cada que recibe un paquete RREQ, e inmediatamente manda la respuesta al nodo 1. si la respuesta del nodo 3 llega primero al nodo 1 entonces en nodo 1 piensa que el descubrimiento de la ruta está completo, ignora cualquier otro mensaje de respuesta y empieza a enviar paquetes de datos.

Como resultado todos los paquetes que pasen por el nodo malicioso se pierden.



[2]

Figura 4.2 El problema del agujero negro

4.3.2.4.3.- Ataques bizantinos

El ataque bizantino puede ser lanzado por un solo nodo malicioso o un grupo de nodos que trabajan en cooperación. Un nodo intermedio comprometido trabaja solo o es parte de un grupo de nodos comprometidos que se coluden para formar un ataque. El nodo comprometido puede crear loops de enrutamiento, reenviar paquetes por la ruta larga en lugar de la óptima, y podría destruir paquetes. Este ataque degrada el performance del enrutamiento y también interrumpe los servicios de enrutamiento.

4.3.2.4.4.-Ataque relampagueante

En el ataque del agujero de gusano, dos atacantes coludidos forman un túnel para falsificar la ruta original. Si por suerte el camino de transmisión es lo bastante rápido (por ejemplo un canal dedicado) entonces los paquetes "tuneleados" pueden propagarse más rápidamente que aquellos que se van por una ruta multi saltos normal, y esto resulta en un ataque relampagueante. Básicamente es otra forma de DoS que puede ser lanzada contra los protocolos de enrutamiento de las redes móviles Ad Hoc propuestas a petición tales como ARAN y ARIADNE [5].

4.3.2.4.5.-Ataques de consumo de recursos

La energía es un componente crítico en las redes móviles Ad Hoc. Los dispositivos dependientes de una batería trataran de conservar la energía transmitiendo solamente cuando sea absolutamente necesario [2]. El objetivo del ataque de consumo de recursos es mandar un número excesivo de peticiones de descubrimiento de ruta o paquetes innecesarios a la víctima para que se consuma su batería. Un atacante o nodo comprometido que pueda interrumpir las funciones normales de las redes móviles Ad Hoc. Este ataque también es conocido como ataque de privación de sueño.

4.3.2.4.6.-Ataques de descubrimiento de posición

Los ataques de descubrimiento de posición es parte de los ataques de descubrimiento de información. El nodo malicioso filtra información que contiene la recopilación de la posición de la estructura de la red y usa la información para ataques futuros. Este recopila la información de la localización de los nodos, el mapa de la ruta y sabe cuáles nodos están situados en el objetivo de la ruta. El análisis del tráfico es uno de los problemas que no están resueltos en los ataques contra las redes móviles Ad hoc.

4.3.3.- Resumen

La capa de red de las redes móviles Ad Hoc es la que mayor inmunidad a los ataques tiene, en comparación con las otras capas. Un bien seguro algoritmo de enrutamiento puede prevenir las vulnerabilidades presentadas en este capítulo. Aunque no hay algoritmo alguno que cubra todas las vulnerabilidades. Los diferentes algoritmos deberían de usarse en cooperación con cada uno de los demás.

4.4.-Amenazas de seguridad en la capa de transporte

Los problema de seguridad relacionados a la capa de transporte son la autentificación, asegurar comunicaciones end-to-end mediante encriptación de datos, retrasos, perdida de paquetes, etc. Los protocolos de la capa de transporte en las redes móviles Ad Hoc provee conexiones end-to-end, una confiable entrega de paquetes, control de flujo, gestión de congestión y limpiar las conexiones end-to-end. Como el protocolo TCP en el modelo de internet, los nodos en las redes móviles Ad-Hoc son vulnerables a la inundación SYN y a los ataques de secuestro de sesión. Durante el capítulo los problemas de la capa de transporte serán discutidos.

4.4.1.-Ataques de inundación SYN

La inundación SYN es un tipo de ataque de negación del servicio (DoS) el cual se produce al crear un gran número de conexiones TCp a medio abrir con el nodo objetivo. Las conexiones TCP entre dos nodos comunicándose son establecidas mediante un saludo de tres vías. En la figura 4.3 el emisor envía un mensaje SYN al receptor con un ISN (Numero de secuencia inicial) generado aleatoriamente.

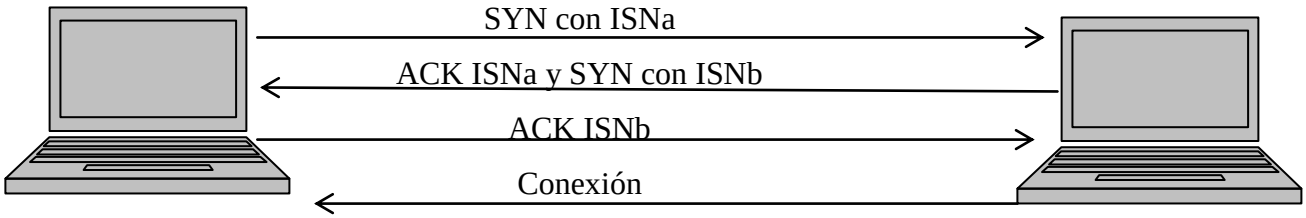


Figura 4.3: Saludo TCP de tres vías

El receptor genera otro mensaje ISN y lo envía con un mensaje SYN que incluye la confirmación de la recepción (ACK) del mensaje SYN. El emisor envía confirmación al receptor. Esta vía de conexión es establecida entre dos nodos comunicándose usando el saludo de tres vías TCP.

Durante un ataque de inundación SYN, un nodo malicioso envía una gran cantidad de paquetes SYN al objetivo, Suplanta la dirección de regreso en el mensaje SYN. Cuando la computadora objetivo recibe los paquetes SYN, y envía los paquetes ACK-SYN al emisor y espera por el paquete ACK. El nodo victima guarda todos los paquetes SYN en una pequeña tabla y espera por el ACK del saludo de tres vías. Esas peticiones de conexión pendientes podrían desbordar el buffer de la tabla del nodo víctima y hacer que el sistema no esté disponible por un largo tiempo.

4.4.2.- Secuestro de sesión

El secuestro de sesión es un error crítico que da al nodo malicioso la oportunidad de comportarte como un sistema autorizado. Todas las comunicaciones son autentificadas solamente durante la configuración de inicio de sesión. El atacante podría tomar ventaja de esto e intentar un secuestro de sesión. Para empezar él/ella suplanta la dirección IP de la víctima y determina la secuencia correcta de números. Después de eso ejecuta un ataque de negación del servicio (Dos) a la víctima. Como resultado, el objetivo se queda no disponible por algún tiempo. El atacante entonces continúa la sesión con otros sistemas con un sistema autorizado.

4.4.3.- Tormenta TCP ACK

Una tormenta TCP ACK es muy simple. Para empezar el ataque, el atacante lanza un secuestro de sesión TCP. Después el atacante envía datos de sesión inyectados, figura 4.4 un nodo A confirma la recepción con un paquete ACK al nodo B. El nodo B es confundido con el paquete conteniendo una secuencia de datos no esperada por lo que trata de re sincronizar la sesión TCP con el nodo A enviando un paquete ACK que contiene la secuencia de números esperada, entonces en nodo A continúa repitiendo el envió del paquete ACK incorrecto produciendo una tormenta TCP ACK [15].

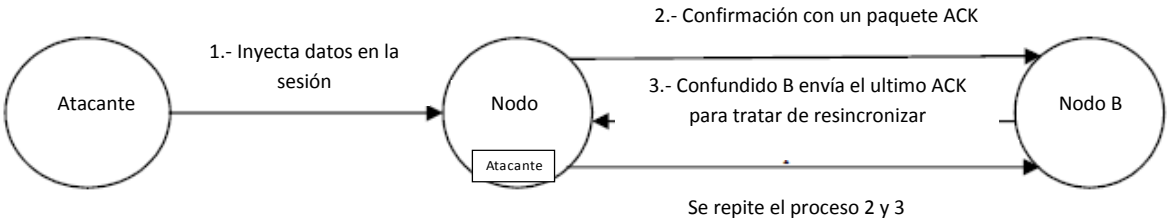


Figura 4.4: Tormenta TCP ACK

4.4.4.- Resumen

Las redes móviles Ad Hoc tienen un alto porcentaje de error en la canales comparados con las redes alámbrico. Esto es debido a que el protocolo TCP no tiene ningún mecanismo para distinguir la causa de la perdida, por ejemplo cuando fue causada por la congestión, algún error o por algún ataque. Por otro lado, el protocolo UDP tampoco es inmune al secuestro de sesión. Es lo mismo que pasa en UDP que con el TCP, con la excepción de que el/la atacante no se tiene que preocupar de la sobrecarga de manejar la secuencia de número y de otro mecanismo TCP ya que el protocolo UDP es un protocolo connectionless.

4.5.- Amenazas de seguridad en la capa de aplicación

Las aplicaciones necesitan ser diseñados para manejar frecuentes conexiones y desconexiones con aplicaciones punto así como una amplia variedad de característica de retraso y perdida de paquetes [13]. Justo como otras capas, la capa de aplicación es vulnerable (y bastante atractiva) para los atacantes. Porque esta capa contiene información del usuario que suportan muchos protocolos, tales como SMTP, HTTP, TELNET, FTP etc. los cuales tienen muchas vulnerabilidades y puntos de acceso para los atacantes. Los principales taques son ataques de código maliciosos y ataques de repudiación.

4.5.1.- Ataques de código malicioso

Los códigos maliciosos (virus, gusanos, spyware, troyanos) atacan tanto el sistema operativo como las aplicaciones de usuario que cusan que el sistema y la red sufran de una reducción de velocidad o en algunos casos dejen de funcionar. Un atacante puede producir estos tipos de ataques en las redes móviles Ad Hoc y buscar por la información deseada [15].

4.5.2.-Ataques de repudiación

Las soluciones que se podrían tomar para resolver los ataques de autentificación y de anti-repudiación en la capa de red no son suficientes, porque la repudiación resulta en una negación de la participación en la comunicación. Un ejemplo de un ataque de repudiación en un sistema comercial: una persona egoísta se niega a realizar una operación en una compra con tarjeta de crédito o retrasar la transacción en línea [15].

4.5.3.- Resumen

Un problema fundamental en las redes móviles Ad Hoc es la seguridad end-to-end. Las redes heterogéneas pueden sufrir de una variedad de riesgos de seguridad que podrían incrementar la latencia en la entrega de paquetes, incrementar la pérdida de paquetes etc. El principal problema de seguridad relacionado a la capa de aplicación es la detección y prevención de virus, gusanos, códigos maliciosos y abusos de la aplicación.

CAPÍTULO V

Soluciones o contramedidas

La seguridad en unos de las principales preocupación en las redes móviles Ad Hoc para poder proveer una comunicación entre las partes comunicándose. Es esencial para las funciones básicas de la red, enrutamiento y reenvió de paquetes. La operación de la red puede ser fácilmente puesta en juego, si las soluciones o contramedidas no está integradas en las funciones básicas de la red en los primeros pasos del diseño de la red [11]. Aunque hay muchos mecanismos de seguridad han sido desarrollados para contrarrestar ataques maliciosos. Hay dos mecanismos que son ampliamente usados para proteger a las redes móviles Ad Hoc de los ataques.

- Mecanismos preventivos: En los mecanismos preventivos la autentificación, control de acceso, encriptación y las firmas digitales son la primera línea de defensa. Algunos módulos de seguridad, como Tokens, Tarjetas inteligentes que son accesibles mediante un PIN, Passphrasesy verificaciones biométricas.
- Mecanismos reactivos: En los mecanismos reactivos se usan esquemas como el sistema de detección de intrusos (IDS), mecanismos de cooperación forzada etc. En la redes móviles Ad Hoc. Los sistemas de detección de intrusiones son usados para detectar malfuncionamientos o anomalías. La cooperación forzada (Confianza, CORE, Tokens) reducen los comportamientos egoístas de los nodos.

5.1.-Soluciones o contramedidas a los ataques en la capa física

La capa física en las redes móviles ad Hoc es vulnerable al jamming de señal, DoS y algunos ataques pasivos. Usar dos tecnologías de espectro esparcido ensanchado pueden ser usadas para dificultar la detección o el atascamiento de la señal. La tecnología de espectro ensanchado cambia la frecuencia aleatoriamente o crea un espectro más amplio lo que dificulta capturar la señal a personas ajenas. El FHSS (espectro ensanchado por salto de frecuencia) hace que la señal sea inentendible por periodos creando ruido para los escuchas. DSSS (Espectro ensanchado por frecuencia directa) representa cada bit de la señal original con múltiples bits en la señal transmitida a través de un código Barker de 11 bits. FHSS y DSSS proveen dificultades para el usuario malicioso que esté intentando interceptar la señal de radio. Para poder captura y liberar el contenido de la señal de transmisión el atacante debe de conocer la frecuencia de la banda, el código de difusión y las técnicas de modulación, y aunque esto es muy efectivo también tiene un problema. Esos mecanismos son seguros solamente cuando el patrón de datos o el código de difusión son desconocidos para el escucha [15].

5.2.-Soluciones o contramedidas en los ataques de capa de enlace

Los problemas de seguridad que están más relacionados a la capa de enlace son proteger el protocolo inalámbrico MAC y proveer soporte a la seguridad en la capa de enlace. Una de las vulnerabilidades en la capa de enlace es el esquema exponential backoff. Recientes extensiones de seguridad propuestas al protocolo 802.11 puestas en [10] donde el esquema original backoff del 802.11 es ligeramente modificado de tal manera que el contador backoff en el emisor es proporcionado por el receptor en lugar de usar un tiempo arbitrario. Los problemas del consumo de recursos (usando campos NAV) es aún un desafío y algunas soluciones se han propuesto, por ejemplo ERA-802.11 [12]). Finalmente el fallo más conocido en la capa de enlace es la debilidad WEP. Afortunadamente el protocolo 802.11.i/WPA [7] han solucionados los problemas WEP y algunas soluciones se están siendo desarrolladas tal como el protocolo RSN/AES-CCMP que proveen una mayor seguridad inalámbrico.

5.3.-Soluciones en los ataques de la capa de red

La capa de red la más vulnerable de todas la capas en las redes móviles Ad Hoc. Una variedad de riesgos de seguridad son impuestos en esta capa. El uso de protocolos de enrutamiento seguros provee la primera línea de defensa. Los ataques activos como modificar los mensajes de enrutamiento pueden ser prevenidos atraves de mecanismo de integridad de mensajes. Por ejemplo firmas digitales, mensajes de autentificación de código (MAC), hashed MAC (HMAC), cadena de una vía HMAC etc. Usar una métrica física inalterable e independiente, como un retraso o la localización geográfica, pueden ser usadas para detectar ataques de agujero de gusano. Por ejemplo, leashes packets son usados para combatir estos ataques [6]. IPSec es el protocolo comúnmente usado en la capa de red y el internet que se podría usar en las redes móviles Ad Hoc para proveer cierto nivel de confidencialidad. El protocolo de enrutamiento seguro denominada ARAN protege de varios ataques, como modificación del número de secuencia, modificación del número de saltos, modificación de la fuente de la ruta, suplantación, fabricación de la fuente de la ruta, etc. [14]. La investigación hecha por Deng [2], et al presenta una solución para detener los ataques de agujero negro. Esta solución es deshabilitar la habilidad de un nodo intermedio para responder un mensaje, y así todos los mensajes de respuesta deben de ser respondidos solo por el nodo de destino.

5.4.-Soluciones o contramedidas para los ataques de la capa de transporte

Una manera de proveer confidencialidad en los mensajes en la capa de transporte son comunicaciones P2P o end-to-end atraves de encriptación de datos. A través del protocolo TCP es la forma de conexión primaria que provee una conexión confiable en el internet, y no encaja totalmente en las redes móviles Ad Hoc. TCP feedfack (TCP-F) [4], Notificación de fallo explicito (TCP-ELFN) [4], protocolos de transmisión Ad Hoc (ATCP) [4] y los protocolos de transporte Ad Hoc (ATP) han sido desarrollados para cubrir los problemas de seguridad relacionados a la redes móviles Ad Hoc. Secure Socket Layer (SSL) [9], Transport Layer Security (TLS)[9] Y Private Communications Transport (PCT) [9] fueron diseñados sobre la base de la criptografía de llaves públicas para proveer comunicaciones seguras. TLS/SSL provee protección ante ataques enmascarados, ataques de rollback, y ataques de respuesta.

5.5.-Soluciones o contramedidas para los ataques en la capa de aplicación

Virus, gusanos, spyware, troyanos son los problemas comunes en la capa de aplicación en cualquier red. Los Firewall proveen de protección contra algunos de esos ataques. Por ejemplo, puede proveer control de acceso, autentificación de usuario, filtros de paquetes entrantes y salientes, filtros de red, servicios de cuenta etc. El software Spyware puede detectar spyware y programas maliciosos en el sistema. Solamente usar un Firewall no es suficiente porque en ciertas situaciones el atacante puede penetrar el Firewall y hacer un ataque. El Sistema de detección de intrusos (IDS) es efectivo para prevenir ciertos ataques como el tratar de ganar acceso no autorizado a algún servicio, pretendiendo ser un usuario legítimo. La capa de Aplicación también detecta ataques DoS más rápidamente que las capas inferiores.

5.6.-Resumen

En este capítulo describí las soluciones o contramedidas en los ataques sufridos en las diferentes capas. Aun así hay algunos ataque que son multi capas, las soluciones a este tipo de ataques necesitas ser implementadas en las diferentes capas. Por ejemplo, antenas direccionales [1] son en la capa de medios para defenderse contra ataques de agujero de gusano mientras que packet lashes [6] son usados para las defensas en la capa de red.

CONCLUSIONES

Las redes móviles Ad Hoc tienen la habilidad de configurar redes al vuelo en ambientes hostiles donde no es posible (o económicamente inviable) desplegar una estructura de red tradicional. Aunque las redes Ad Hoc tienen un gran potencial, aunque muchos retos por solucionar. La seguridad es una característica primordial para la implementación de una red móvil Ad Hoc. En esta tesis, mostré un resumen de los problemas y soluciones a los riesgos de seguridad en las redes móviles Ad Hoc. La primera pregunta en esta investigación fue ¿Cuáles son las vulnerabilidades en materia de seguridad en las redes móviles Ad Hoc?, ¿Qué capas son las más vulnerables a los ataques?, durante mi investigación presente varios ataques relacionados a diferentes capas y descubrí que la capa de red es la más vulnerable más que nada por la información contenida en ella. Esta aislación de los ataques en las diferentes capas hizo que fuera más fácil de entender los ataques en las redes móviles Ad Hoc.

La segunda pregunta fue ¿Qué servicios de seguridad, tales como, confidencialidad, integridad y autentificación pueden ser implementados en las redes móviles Ad Hoc? ¿Qué es lo que se requiere? La respuesta es que los servicios de seguridad pueden ser implementados siguiendo las soluciones preventivas y reactivas dependiendo de la particularidad de cada ataque.

La tercera pregunta fue ¿Cuáles son las contramedidas para los ataques? ¿Cómo está asegurado el sistema entero?, Me enfoque en las posibles soluciones o contramedidas usadas en las redes alámbrico e inalámbricas y también las que fueron designadas específicamente para las redes móviles Ad Hoc. Además podría decir que la seguridad debe de ser asegurada para todo el sistema ya que un solo punto vulnerable podría comprometer todo el sistema y así permitir al atacante acceder al sistema y ejecutar acciones maliciosas.

La última pregunta fue ¿Cuáles son los riesgos futuros? Todos los días hay avances con las nuevas aplicaciones y los nuevos conocimientos tanto para los atacantes como para la protección del sistema pero lo que es vital e imprescindible es asegurar en sistema en las múltiples capas a continuación explicare algunos de los peligros futuros y las investigaciones en progreso.

El futuro

Ha habido muchas investigaciones en las redes móviles Ad Hoc por muchos años, pero hasta ahora es cuando las investigaciones a fondo están siendo desarrolladas. Muchas de las soluciones actuales fueron diseñadas para detener ataques específicos. Y aunque se pueden adaptar par algunos de los demás ataques hay muchas combinaciones de ataques que son desconocidas y por lo tanto no hay defensa contra ellas. Un ataque DoS de consumición de recursos aun es difícil de resolver. Se necesita más investigación en los protocolos de enrutacion, llaves de seguridad, seguridad de datos multicapa y la cooperación forzada. Muchos de los protocolos actuales son objeto de múltiple ataques que pueden llevar a la víctima a elegir rutas no deseadas, por lo que una enrutacion más segura es necesaria. La criptografía es uno de los mecanismos de seguridad más comunes y su fuerza depende de que tan seguro sea el manejo de las llaves. El esquema de criptografía pública depende un certificado de autoridad centralizado por lo cual este es un punto débil de las redes MANET y es una de las líneas de investigación en proceso.

Bibliografía

[12] A. Perrig, R. Canetti, J. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol*," Internet Draft, 2000.

[15] B. Wu, J. Chen, J. Wu, M. Cardei, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*.

[2] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,"* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volumen: 40, pagina(s): 70- 75, ISSN: 0163-6804.

[4] H. Hsieh and R. Sivakumar, "*Transport OverWireless Networks,"* Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[16] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "*Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volumen- 11, Paginas(s):
38- 47, ISSN: 1536-1284

[7] IEEE Std. 802.11i/D30, *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,"* 2002.

[3] J.-P. HuBaux, L. Buttyan, and S. Capkun., "*The quest for security immobile ad hoc network,"* In Proc. ACM MOBICOM, Oct. 2001.

[8] J. Kong et al., "*Providing robust and ubiquitous security support for mobile ad-hoc networks,"* In Proc. IEEE ICNP, pages 251–260, 2001.

[14]K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "*Secure routing protocol for ad hoc networks,"* Proc del 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Pagina(s): 78- 87, ISSN: 1092-1648.

[18] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999,
Volumen: 13, Página(s): 24-30, ISSN: 0890-8044.

[11] P. Michiardi, R. Molva, "*Ad hoc networks security,"* IEEE Press Wiley, New York, 2003.

[10] P. Kyasanur, and N. Vaidya, *"Detection and Handling of MAC Layer Misbehavior in Wireless Networks,"* DCC, 2003.

[13] R. Ramanathan, J. Redi and BBN Technologies, "*A brief overview of ad hoc networks: challenges and directions,"* IEEE Communication Magazine, May 2002, Volumen: 40, pagina(s): 20-22, ISSN: 0163-6804.

[1] S. Capkun, L. Buttyan, and J. Hubaux, "*Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks,"* 2003.

[17] S. Yi, P. Naldurg, and R. Kravets, "*Security-aware ad hoc routing for wireless networks,"* Proc. De ACM Mobihoc, 2001.

[5] Y. Hu, A. Perrig, and D. Johnson, "*Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,"*

Proc. de MobiCom 2002, Atlanta, 2002.

[6] Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense AgainstWormhole Attacks In Wireless Ad Hoc Networks,"* Proc. de IEEE INFORCOM, 2002.