Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Ataques en redes inalámbricas

(Redes WI-FI)

Autor: Gelson Alves Francisco Nunes

Tutor: Dr. Pedro José Arco Ríos

Santa Clara

2009

"Año 50 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Ataques en redes inalámbricas

(Redes WI-FI)

Autor: Gelson Alves Francisco Nunes

E-mail: galves_nunes@yahoo.com.br

Tutor: Dr. Pedro José Arco Rios

E-mail: parco@uclv.edu.cu

Consultantes: Dr. Vitalio Alfonso

Ing. Fouad Ziad Othman

Santa Clara

2009

“Año 50 de la Revolución "

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

Muchos optan

por escoger un camino a seguir

pero pocos se empeñan

en alcanzar

la meta que han escogido.

DEDICATORIA

Le dedico este trabajo a la persona cuya todo hiso para que se tornara posible la conclusión de esta carrera y que sin lugar a duda todo lo que soy y podre ser en el futuro, es gracias a ella, se trata de mi abuela, María Francisca que ha ejercido todas las funciones necesaria para que fuera posible un día estar yo a altura de realizar un trabajo de esta envergadura.

AGRADECIMIENTOS

Les dedico mis sinceros y profundos agradecimientos a todos cuanto colaboraron de forma directa y/o indirectamente en mi formación personal, profesional e intelectual, enfatizando en particular:

- *En los profesores de Facultad de Eléctrica que con mucha dedicación siempre estuvieron disponible en ayudar.*
- *Mi tutor y los consultantes que por la experiencia acumulada supieron orientarme hacia el objetivo del trabajo.*

❖*A la revolución Cubana por brindarme esta oportunidad para cursar una formación superior.*

❖*A mis compañeros de estudio que desempeñaron un papel de extremada importancia sobretodo en los momentos de estudio colectivo.*

❖*Mis amigos que siempre estuvieron conmigo en los buenos y malos momentos.*

❖*A mis familiares que a pesar de estar lejos siempre me acompañaron en los momentos más difíciles y tomas de decisiones.*

❖*Por último pero no menos importante a mi novia por su apoyo incondicional tanto moral, material como también afectivo.*

TAREA TÉCNICA

- Búsqueda y recopilación de información sobre las redes inalámbricas y los distintos ataques.
- Resumir los aspectos esenciales correspondientes a las topologías empleadas en estas redes.
- Estudiar los problemas técnicos esenciales correspondientes problemas de seguridad en estas redes.
- Estudiar y resumir las estrategias técnicas que se están investigando con el objetivo de mejorar la eficiencia en la utilización de redes inalámbricas.
- Desarrollar algoritmo con objetivo de frenar de forma eficiente las vulnerabilidades que fragilizan las redes inalámbricas.

Firma del Autor

Firma del Tutor

RESUMEN

En el presente trabajo se realiza un estudio dedicado a las redes WLAN en general, sus principales vulnerabilidades en cuestiones de seguridad y los ataques más frecuentes a los que son sometidas; revisándose distintas fuentes tanto nacionales como internacionales. Con el propósito de aliviar el impacto de los distintos ataques sobre la red se propone algunos métodos y ó algoritmos para lograr disminuir los efectos del ataque que tienden a reducir el desempeño de dichas redes. De igual forma se estudia la protección de seguridad en redes WLAN, los distintos mecanismos de seguridad para este tipo de redes y las herramientas específicas que utilizan estos, con el objetivo de proteger las áreas de la universidad, cibercafé, hoteles, aeropuerto, entre otras instituciones y empresas que estarán conectadas a redes WLAN.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Hoy en día y cada vez con más importancia, la rentabilidad y desempeño de las empresas dependen del uso de las telecomunicaciones en sus procesos de negocios y de correlación entre sus dependencias, colaboradores, clientes y suministradores. Esto implica una demanda creciente de servicios de telecomunicaciones y una evolución constante de las necesidades hacia el uso de las nuevas redes y servicios. Después del gran auge de Internet en los años noventa y tras la expansión de los teléfonos móviles en el nuevo milenio, las redes sin hilos ó *wireless* se han convertido en la perita en dulce de las comunicaciones. En la actualidad, dada la nueva tendencia en la que los empleados, en vez de permanecer sentados en sus puestos de trabajo, pasan la mayor parte de su tiempo en movimiento trabajando con portátiles y PDAs, la tecnología inalámbrica se posiciona como una herramienta fundamental para mejorar la productividad en las empresas de hoy. La flexibilidad y movilidad hacen de las redes inalámbricas una alternativa atractiva frente a las redes cableadas y a la vez una extensión de estas puesto que proporcionan la misma funcionalidad sin las restricciones del cable en sí mismo.

Debido a la gran cantidad de información relacionada con las redes inalámbricas y puesto que es inverosímil abarcar todas sus áreas, así como estándares y profundizar en cada una de ellos, en este trabajo están expuestos sus conceptos básicos y fundamentos, para de esta manera cumplir con el objetivo del presente trabajo, que es brindar un aporte que permita familiarizarse con este tipo de redes, su diseño y los beneficios que aportan. (Torres 2006)

El abaratamiento de costes de conexión, la mejora de la tecnología y la expansión de Internet mediante cables ha llevado a una conexión generalizada de los hogares y empresas

a Internet. Sin embargo el problema de extender esta conectividad dentro del hogar o en las distintas plantas de una fábrica mediante complicados cableados persistía de forma inamovible.(Torres 2006)

La consolidación de la telefonía móvil ha obligado al rápido avance de las tecnologías sin hilos que se han visto aún más potenciadas por el gran aumento de ventas de ordenadores portátiles y sistemas personales o PDA. Si dispongo de una batería que me permite moverme por mi casa/empresa/universidad, ¿Por qué debo permanecer conectado a un cable para acceder a Internet?(Alvarez 2004)

Una red inalámbrica ó WLAN es un sistema de comunicaciones de datos que transmite y recibe información utilizando ondas electro magnéticas, en lugar del par trenzado, coaxial ó fibra óptica utilizado en las LAN convencionales.(Yáñez-Mingot 2006)

Se deja en las manos del lector un trabajo realizado con mucha dedicación, y se espera que la información presentada sea de su total interés, entendimiento y sobre todo utilidad.

Objetivo general:

- Caracterizar los problemas generales de las redes inalámbricas en cuestiones de seguridad, enfatizando los ataques a que están expuestas dichas redes.

Objetivo específico:

- Analizar los mecanismos de protección y configuraciones necesarias para garantizar seguridad en una red inalámbrica.
- Destacar las debilidades que se encuentran en las redes inalámbricas en la capa MAC de 802.11
- Estudiar las más diversas formas de ataque que se puede lanzar a una red inalámbrica, así como el impacto de estos en el desempeño de la red.
- Analizar el comportamiento de la red ante el ataque de denegación de servicio basados en el tráfico desde el punto de vista del desempeño de la red, reducción del caudal y pérdidas de paquetes.
- Resumir aspectos esenciales relacionados con los métodos y técnicas para mitigar los ataques efectuados en la capa MAC.

Organización del informe

En el capítulo 1 se realiza un estudio general de lo que son las redes inalámbricas, así como todos los dispositivos que la componen. Se hace referencia a lo que es la tecnología inalámbrica en sus diversas variedades, las topologías ó modo de operación que podemos configurarla, bandas de frecuencia en que operan los equipos así como las normas internacionales que rigen el mundo de las comunicaciones inalámbricas estandarizadas por norma 802.11a/b/g de la IEEE. A continuación en el segundo capítulo se dedica a la definición del concepto de seguridad, bien como el estudio de los distintos mecanismos de seguridad en general que se emplea en las redes inalámbricas con la intención de minimizar la vulnerabilidad en las distintas capas del modelo OSI, sus principales vulnerabilidades en cuestiones de seguridad y en particular se profundiza de forma detallada los ataques más frecuentes a los que son sometidas estas redes. El capítulo 3 se hace mención a las técnicas de prevención y detención de los ataques en general, como reaccionar ante algunos ataques de denegación de servicio y por último se plantean las propuestas de configuraciones de seguridad a emplear.

CAPITULO 1 CONCEPTOS GENERALES DE REDES INALÁMBRICAS

En este capítulo se presenta una introducción teórica sobre aspectos de las redes inalámbricas. Las WLAN (Wireless Local Área Network) nos ofrecen un sistema de comunicación de datos inalámbrico flexible, muy utilizadas como alternativa a las redes LAN (*Local Área Network*) cableadas o como extensión de éstas. Utilizan tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Con la finalidad de potenciar el desarrollo y expansión de este tipo de redes, se ha creado toda una familia de estándares, dentro de las que se destaca, la IEEE 802.11. Las redes WLAN se difunden rápidamente en el escenario actual con un área de cobertura en entorno local, empleándose en empresas, oficinas, universidades, aeropuertos, hoteles y centros de congresos.

1.1 Proliferación de redes inalámbricas

En los últimos años las redes inalámbricas han ido tomando un protagonismo cada vez más fuerte. Para darnos cuenta de esto basta simplemente con disponer de una WNIC (tarjeta de red inalámbrica) conectada a un PC, y podremos verificar como en una gran mayoría de lugares donde nos situemos, nuestra WNIC detecta la existencia de algún PA asociado a una red inalámbrica. Varios han sido los motivos que han propiciado la proliferación de este tipo de tecnología para la transmisión de información entre estaciones móviles:

- Reducción del coste de hardware necesario
- Movilidad

- ❖ Rápida instalación
- ❖ Flexibilidad
- ❖ Escalabilidad

1.1.1 Reducción del coste de hardware necesario.

Únicamente necesitamos uno o varios puntos de acceso dependiendo del área de cobertura que queramos que abarque nuestra red, y disponer de tarjetas inalámbricas para cada uno de los equipos que formen parte de dicha red. Estos puntos de acceso, conectarían al resto de la LAN cableada, así como al resto del internet por medio del sistema de distribución (DS) en una topología ESS (Extended Service Set). Aún podríamos reducir más costes en equipamiento en el caso de que optáramos por montar una red "ad-hoc" o BSS, en la que solo harían falta las tarjetas de red inalámbricas para los equipos debido a que uno de ellos, (PC de sobremesa) podría disponer de una tarjeta de red Ethernet con conexión al resto de la internet, de modo que haría el papel de router para el resto.

1.1.2 Movilidad

Los usuarios pueden conectarse a internet sin tener que disponer de una conexión física con cables, por lo tanto permite esta movilidad a los usuarios dentro del área de cobertura de la WLAN manteniendo el ancho de banda y sin perder conexión.

1.1.3 Rápida instalación

Debido a que no es necesario hacer obras pasando cables a través de paredes, instalando tomas de acceso etc.

1.1.4 Flexibilidad

Es posible instalar nuevas WLANs o cambiar de emplazamiento las ya existentes, de forma rápida y sencilla.

1.1.5 Escalabilidad.

Se puede hacer una instalación empezando por pequeñas redes "ad-hoc" de unas pocas estaciones, e ir ampliándolas sucesivamente, hasta el punto de hacerlas muy grandes por medio de la utilización de puentes inalámbricos, utilizados para la interconexión de

WLANs en emplazamientos diferentes y situados a una distancia considerable (generalmente no más de 10 km) pudiendo suponer un ahorro frente al alquiler de circuitos telefónicos. Por todas estas ventajas y muchas otras son por las que el mercado de las WLAN se ha ido incrementando cada vez más en los últimos años y cada vez son más las empresas e instituciones públicas las que optan por esta solución en alternativa a las soluciones tradicionales que utilizan el cableado.(Carlos Varela 2002)

1.2 Tecnologías inalámbricas

Algunas de las tecnologías más populares en la actualidad que suportan redes inalámbricas son:

•Bluetooth

Corto alcance (10m aprox.), utilizado con frecuencia en dispositivos móviles (PDAs), teléfonos celulares y computadoras de automóvil, baja velocidad (1mb).

• **UWB** (Ultra wide band)

Corto alcance (20m aprox.), alta velocidad (+100mb), aplicaciones de audio y video.

• **Wimax** (IEEE 802.16)

Red de cobertura amplia (una ciudad completa por ejemplo), pretende ser una alternativa a tecnología cableada como ADSL.

• **Wi-Fi** (IEEE 802.11a/b/g)

La tecnología inalámbrica más popular en la actualidad, velocidades desde 1 Mbps hasta 54 Mbps, esta presentación está enfocada en esta tecnología.

1.3 Componentes y conceptos de redes inalámbricas

El concepto de redes inalámbricas ó WI-FI (wireless fidelity) como también se le designa, viene siendo ondas electromagnéticas que se propagan en el aire, usando radio de frecuencia para la comunicación entre los dispositivos. WI-FI Aliance ha desarrollado un conjunto de normas y reglas que rigen el mundo de los dispositivos que componen la fidelidad inalámbrica. Para las computadoras portátiles de nuevo fabrico vienen equipadas con tarjetas onboard que le permite funcionar en los distintos modos de operación a que se

le puede configurar. En el caso de las computadoras de mesa o sea, las desktop y las más antiguas laptop se ha desarrollado tarjetas adaptadoras tanto para el puerto USB como PCI permitiéndole así el acceso a la red sin la necesidad del cableado. En dependencia de la topología de la rede, la misma debe estar compuesta por los elementos que se menciona y en algunas ocasiones con los puntos de acceso. Los AP que sirven de puente para interconectar las redes LAN con las WLAN, las antenas que son de extremada importancia en este tipo de comunicación, pues estas definen el rango del alcance de las señales, el direccionamiento y en cierta instancia define la eficiencia del enlace. En dependencia del objetivo que pretenda alcanzar, ó sea, si se quiere enlazar redes con cierta distancia ó solamente cubrir una área limitada existen dos tipos de antenas: están las antenas omnidireccionales cuya finalidad es dar cubertura ó radiar en todas las direcciones, por otro lado existen las antenas directivas que a diferencia de las omnidireccionales estas radian hacia un sentido ó un sector reducido. Son estos los elementos básicos que se necesita para conformar una red WI-FI.

1.4 Topologías de redes inalámbricas

Existen dos formas de construir las redes inalámbricas: a través de un control central llamado infraestructurado (estrella) que se logra mediante la instalación de un punto de acceso (Access Point), a la cual acceden los equipos móviles. El punto de acceso actúa como puente entre la red cableada y la red inalámbrica y regulador de tráfico entre los equipos móviles. La otra forma es por medio de enlaces entre los mismos nodos sin la necesidad de un control central como una estación base o punto de acceso, llamadas redes Ad-Hoc. El último tipo de redes es de alta versatilidad y flexibilidad ya que no requiere de una infraestructura fija. Las redes Ad-Hoc compuestas por nodos móviles se le llaman "MANET o Mobile Ad-Hoc Network"

Redes infraestructura, en esta topología los dispositivos con tarjetas inalámbricas se conectan entre sí por medio de PA que se responsabiliza por la gestión del tráfico de las comunicaciones. En ocasiones es necesario saber el ESSD de la red gestionada por el PA para poder conectarse y poder hacer parte de la infraestructura. Sus estaciones pueden ser PCs, portátiles, PDA. Son redes basadas en la existencia de uno o varios PA cada uno de los cuales definirá una celda o BSS, ("Basic Service Set") y la unión de todas estas celdas

definirá lo que se conoce como ESS ("Extended Service Set"). La interconexión de PAs (lo que se conoce como sistema de distribución o DS) se podrá realizar por medio de una LAN convencional o bien por radio, es decir, interconexión entre PAs sin cables. Cada una de las celdas a las que dan cobertura los PAs permiten crear redes que den cobertura en zonas amplias (almacenes, edificios, universidades,…) permitiendo a los usuarios, la conexión a la red, desde prácticamente cualquier punto así como la movilidad pudiéndose desplazar por dentro de la red sin perder conectividad (roaming). Para ello es requisito indispensable que haya solapamiento entre celdas contiguas y la zona de solapamiento sea de la anchura apropiada.

Figura 1.1: Topología de red infraestructura

Red en modo Ad-hoc, proviene del acrónimo inglés punto caliente, redes de saltos como también se llama, el modelo más simple de red inalámbrica, consistente en situar varias estaciones con tarjeta de red inalámbrica próximas, que se encuentren dentro de la misma área (misma habitación por ejemplo). El modo de operación de esta topología, se corresponde como DCF ("Distributed Coordination Function") en la que no hay control centralizado y todas las estaciones son consideradas como iguales.(Tortosa 2005)

A diferencia de modo infraestructura, en esta topología se caracteriza por la ausencia del AP que gestiona la red, lo que aumenta las colisiones disminuyendo así el desempeño de la red. Las redes de múltiple salto como también se le conoce están construidas sobre el protocolo MAC IEEE 802.11 DCF el cual fue originalmente diseñado para redes de área

local. Esta adaptación revela problemas y vulnerabilidades que pueden ser explotadas por un ataque de denegación de servicio basado en tráfico.(Sarmiento 2008)

Figura 1.2: Topología de red Ad hoc

1.5 Normas estandarizadas

Introducción

El estándar 802.11 del IEEE (El Instituto de Ingenieros Eléctricos y Electrónicos) es el más usado de todos los estándares para LAN inalámbrica, debido a que supone la alternativa más viable y económica para proveer de servicio de red en ubicaciones en las que instalar el cableado para una red "convencional" es demasiado caro ó difícil. Como todos los estándares incluidos en el grupo 802, especifica únicamente la capa física y la subcapa MAC, adaptada a las peculiaridades específicas del medio inalámbrico. Las interfaces ofrecidas por (802.11) a las capas superiores son los mismos que los que ofrecen los demás estándares 802.x. El objetivo de este estándar es proveer de conectividad inalámbrica a dispositivos inalámbricos, que pueden ser portables o estar instalados en vehículos móviles, y que necesiten el establecimiento rápido de conexión en red local. El estándar 802.11 también trata de guiar a las organizaciones responsables del espectro radioeléctrico a estandarizar bandas de frecuencias para la comunicación de dispositivos en redes de área local vía radio. La capa MAC también debe ser capaz de tratar con varios tipos distintos de métodos de transmisión, como transmisión infrarroja o técnicas de espectro ensanchado.(Othman 2007)

Existen cuatro servicios, que son aportados por todos los nodos de la red, incluidos los AP:

- ✓ **Autenticación:** Este servicio es utilizado para establecer la identidad de cada estación. Es necesario debido a que solo los usuarios autenticados estarán autorizado a conectarse a la red, pero los esquemas de autenticación se basan en un intercambio de mensaje relativamente inseguro, ya que por defecto se suele usar un sistema abierto que suele desembocar en la autenticación de todas las estaciones que lo soliciten.
- ✓ **Desautenticación:** Termina una relación de autenticación, como lo define su nombre.
- ✓ **Privacidad:** En una red cableada, para acceder a la información, un atacante necesitaría obtener acceso físico al cable antes de intentar capturar tráfico. Sin embargo en una red de área local inalámbrica el acceso a la red es mucho más fácil, ya que solo necesitaríamos usar la antena y los métodos de demodulación correctos.
- ✓ **Reparto de datos:** Este es el servicio usado para transmitir y recibir datos, sin embargo, al igual que Ethernet, no garantiza que la transmisión sea completamente fiable.

Actualmente podemos encontrar varias especificaciones de conexiones a redes sin hilos. En el momento existen tres estándares diferentes para las WLAN, desarrollados por la IEEE que se agrupan en el estándar 802.11, también referenciado en la bibliografía como 802.11x. Esta especificación se subdivide en varias categorías según la velocidad de transferencia y la frecuencia de operación en que trabajan.(Molina 2003)

Norma 802.11a

Se introdujo al mismo tiempo que 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial (802.11b se enfocó hacia las redes caseras y para pequeños negocios). Ofrece velocidades desde 11 hasta 54 Mbps (típicamente 22 Mbps) y opera en la banda de 5 GHz Su alto precio, el hecho de que la banda de 5 GHz esté regulada en algunos países, y su menor cubrimiento ha hecho que los equipos 802.11a sean menos populares que los 802.11b. Esta tecnología usada principalmente en Estados Unidos y Japón y el alcance es de unos 100 metros.(Molina 2003)

Norma 802.11b

Introducido en 1999, como extensión al estándar 802.11 publicado en 1997. Los equipos inalámbricos que operaban con la norma 802.11 nunca llegaron a tener una buena acogida, porque la máxima velocidad de conexión que ofrecían era de 2 Mbps. La norma 802.11b subsanó este problema al permitir lograr una velocidad más alta de transferencia de datos. Dicha velocidad tiene un límite de 11 Mbps En la práctica, se logran velocidades entre 2 y 5 Mbps, lo que depende del número de usuarios, de la distancia entre emisor y receptor, de los obstáculos y de la interferencia causada por otros dispositivos. El factor interferencia es uno de los que más influye, porque los equipos 802.11b operan en la banda de 2.4 GHz, en la que se presenta interferencia de equipos como teléfonos inalámbricos y hornos microondas. A pesar de sus problemas, el estándar 802.11b se ha convertido en el más popular, se utiliza principalmente en Europa.(Molina 2003)

Norma 802.11g

Surgió en 2003, como la evolución del estándar 802.11b. Denominada también Wi-Fi 2.0 se usa sobretodo en Europa esta norma ofrece velocidades hasta de 54 Mbps (22 Mbps típicamente) en la banda de 2.4 GHz, y es compatible hacia atrás con los equipos 802.11b, por lo cual ha tenido una gran acogida, y se prevé que reemplace por completo al estándar 802.11b en un futuro no muy lejano. (Molina 2003) El alcance es de unos 100 metros, esto hace referencia al máximo teórico y dista mucho del rendimiento real obtenido, por otro lado cada edificio/espacio es distinto.

1.6 Bandas de frecuencia de operación

El sistema WLAN trabaja en dos bandas de frecuencias, la banda de 2.4GHz y la banda de 5GHz, en la banda de 2.4GHz se utiliza un rango de frecuencias que va desde 2.4GHz hasta 2.4835GHz, para sistemas de telecomunicaciones de baja potencia (la potencia máxima de emisión permitida es en términos de PIRE (*Potencia Isotrópica Radiada Equivalente*) de 10mW, 20dBm) en redes de interiores o exteriores de corto alcance. El ancho de banda por canal es de 22MHz, con una separación entre canales de 5MHz. Por tanto, estamos hablando de 13 canales disponibles, 3 de ellos no solapados. El número de estos canales para Estados Unidos

es de 13 y 11 para Europa. Para la banda de 5GHz se utiliza un rango de frecuencia que va desde 5.150GHz hasta 5.725GHz, con un ancho de banda por canal de 20MHz, existiendo 12 canales no solapados, 8 para uso en interiores y 4 para exteriores. Esta banda de 5GHz se subdivide en dos rangos de frecuencia, el rango de frecuencia que va desde 5.150GHz hasta 5.350GHz, restringiendo su uso para redes de área local únicamente en el interior de recintos y el rango de frecuencia que va desde 5.470GHz hasta 5.725GHz, puede ser utilizado en redes de área local en el interior o exterior de recintos, con una potencia menor o igual a 1W (PIRE), disponiendo estos sistemas de técnicas de control de potencia (TCP) y selección dinámica de frecuencia (DFS). Ambas bandas están designadas para aplicaciones ISM y ninguna de las dos requiere licencia para su utilización, aunque si están sujetas a ciertas regulaciones.

Estándar	Velocidad Máxima	Banda Frecuencia
802.11	1 y 2 Mbps	2.4 Ghz
802.11a	54 Mbps	5.15 Ghz
802.11b	11 Mbps	2.4 Ghz
802.11g	54 Mbps	2.4 Ghz
802.11n Para 2008 –	> 100 Mbps	2.4 Ghz...40 Ghz

Tabla 1: Estándares de conexión inalámbricas.

CAPITULO 2 SEGURIDAD EN REDES INALÁMBRICAS

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más preponderante en el mundo de las telecomunicaciones. Esta popularidad ha crecido hasta tal punto, que las podemos encontrar en casi cualquier ámbito en nuestra vida cotidiana, teléfonos inalámbricos, PDA, ordenadores, teléfonos móviles; son algunos de los ejemplos más evidentes. La implementación más usual de red inalámbrica para entornos de redes de área local es el estándar IEEE 802.11 también comúnmente conocido como redes WI-FI.

Debido a sus muchas bondades, entre las que sin duda sobresalen su fácil conexión e instalación, se han convertido en una excelente alternativa. Es decir, que optando por esta tecnología de transmisión por radio, se puede llegar a tener las mismas funcionalidades que con una red cableada, pero con un costo menor y a su vez con mayor flexibilidad y versatilidad. La creciente aceptación de estas redes se debe en gran medida a un cúmulo de facilidades que las hacen únicas. Lo que las ha convertido en una opción cada vez más frecuente en instituciones, corporaciones y otros lugares, provocando que coexistan simultáneamente varias de estas redes en el mismo espacio radioeléctrico. Al utilizar ondas electromagnéticas como medio de propagación, son capaces de llegar hasta objetivos distantes, son de fácil implementación además de ser una alternativa económica, lo que las convierte en una solución muy práctica, pero a la vez, esto, constituye su mayor vulnerabilidad cuando de seguridad se habla. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en cierta área, un tercero podría acceder, sin estar ubicado en el lugar propiamente, bastaría con que se encontrara en una localización próxima donde le llegase la señal, ya que cualquier dispositivo equipado con una tarjeta de red inalámbrica situado en el área de cobertura puede acceder fácilmente a nuestra red.

La implementación de redes inalámbricas, se ha convertido en una alternativa necesaria para unir lugares estratégicos donde resultaría muy deficiente una infraestructura cableada.

Debemos tener bien claro que el concepto de seguridad es algo ambiguo, ningún tipo de red es totalmente intocable, incluso las redes con cable sufren de distintos tipos de vulnerabilidades. Las redes inalámbricas son aún más vulnerables que las redes cableadas, debido que la propagación de la señal es en todas las direcciones y están expuestas a cualquier tipo de ataque. A la seguridad en redes inalámbricas se le puede definir como conjunto de procedimientos, provisiones y recursos que se aplican para reducir la vulnerabilidad de los sistemas. Aunque hablar de seguridad en las redes inalámbricas parece una utopía, esto empieza a cambiar gracias al uso del protocolo 802.1x, que aunque poco conocido, ofrece las seguridades de una red física. Sin embargo, asusta pensar que más del 98% de las empresas emplean el protocolo 802.11, el cual puede ser reventado con una simple PDA en menos de 2 horas. La seguridad en las redes inalámbricas está más que cuestionada hoy en día. Muchas de las redes existentes en la actualidad, basadas en el protocolo 802.11, ni siquiera se encuentran cifradas, por lo que el acceso a estas redes es tan sencillo como dejar que Windows se conecte de manera automática o, como mucho, que tengamos que encontrar una IP válida para conectarnos a la red.(Othman 2007)

El objetivo de la seguridad en redes inalámbricas es proveer el mismo nivel de seguridad y confianza que se tendría con una red cableada, utilizando mecanismos basados en métodos de cifrado y de autenticación/autorización.(Krishnamuthy 2004)

2.1 Mecanismos de seguridad

Los sistemas inalámbricos por sus características presentan algunas vulnerabilidades extras, a las que se dirigen ataques que son específicos para este tipo de sistema. Estos se pueden clasificar de acuerdo a la capa del modelo de referencia OSI en el cual se ejecutan. La seguridad de las redes inalámbricas, se garantiza teniendo en cuenta dos aspectos, un primer elemento lo constituye la autenticación; que se emplea para identificar un usuario ante el punto de acceso y viceversa. Un segundo elemento, el proceso de cifrado de los datos, asegura que no sea posible decodificar el tráfico de usuario. Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. Se hará a continuación una

presentación de cada uno de ellos.(Molina 2003) Analizado este punto, se comenzará describiendo los protocolos de seguridad que operan en el nivel de enlace de datos del modelo de referencia OSI. (Othman 2007)

2.1.1 Mecanismos de seguridad del nivel de físico

Filtrado MAC

El Filtrado de direcciones MAC constituye el método más elemental y fácil de implementar de los mecanismos de seguridad, se basa en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Tiene como ventaja:

1. Su sencillez, por lo cual se puede usar para redes caseras o pequeñas.

Posee muchas desventajas que lo hacen poco práctico para uso en redes medianas o grandes:

1. No es escalable porque cada vez que se desee autorizar o dar baja a un equipo, es necesario editar las tablas de direcciones de los puntos de acceso.
2. El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
3. Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack o WellenReiter, entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
4. En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido.
5. No garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.(Othman 2007)

Falsificar una MAC es muy sencillo con Unix y lo mismo para Windows si la tarjeta lo permite.

-Linux: ifconfig <interface> hw ether <MAC>

-FreeBSD: ifconfig <interface> -L <MAC>

Programas empleados para ataques: Airopeek (Windows), WellenReiter, Kismet (Linux/BSD).

2.1.2 Mecanismos de seguridad del nivel de enlace

El protocolo **WEP**, contenido desde un inicio en la especificación original del estándar IEEE 802.11, intenta proporcionar niveles de confidencialidad equivalentes al de las redes cableadas, para ello se basa en la implementación conjunta de los dos aspectos descritos anteriormente, autenticación y cifrado. El protocolo de cifrado utiliza una clave secreta compartida entre una estación y un AP, cifrando con ella todos los datos enviados y recibidos. En la práctica, una misma clave es compartida por todas las estaciones y AP que componen un mismo sistema, a pesar de que el estándar permite que se asocie una para cada estación. Estas pueden ser de dos tipos, dependiendo del estándar en cuestión, para el IEEE 802.11, se utiliza una de 40 bits, considerada insuficiente o débil, por lo que en el IEEE 802.11b tendrá una longitud de 128 bits. Además este mecanismo empleará a RC4, como un generador de números seudo-aleatorios. (Fleites 2007)

El algoritmo WEP cifra de la siguiente manera (ver Figura 2.1):

• A la trama en claro se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Dicho ICV se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

• Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.

• Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas en claro iguales producirían tramas cifradas similares. Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama.

• La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo-aleatorios. El generador RC4 es capaz de generar una secuencia

seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

• El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el ICV).

• Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.

• El IV y la trama se transmiten juntos.

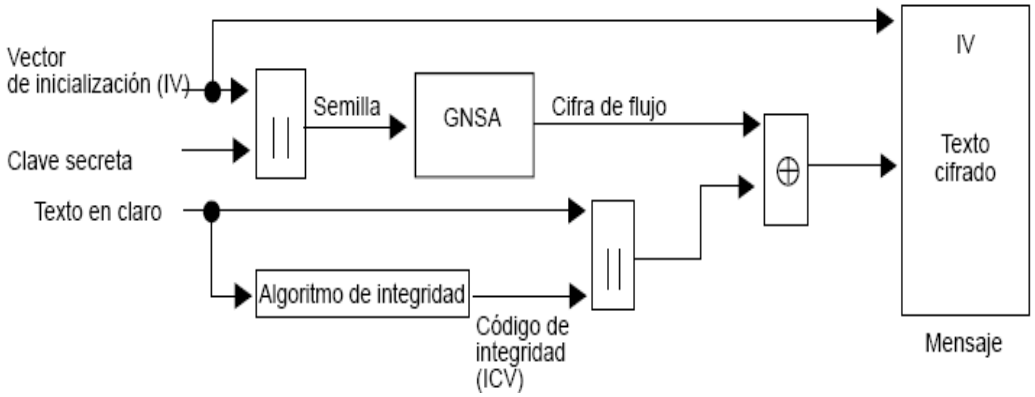


Figura 2.1 Funcionamiento del algoritmo WEP en modalidad de cifrado. (Molina 2003)

En el receptor se lleva a cabo el proceso de descifrado:

• Se emplean el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.

• Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.

• Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama en claro y el ICV.

• A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV, que se compara con el recibido.

• Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.(Molina 2003)

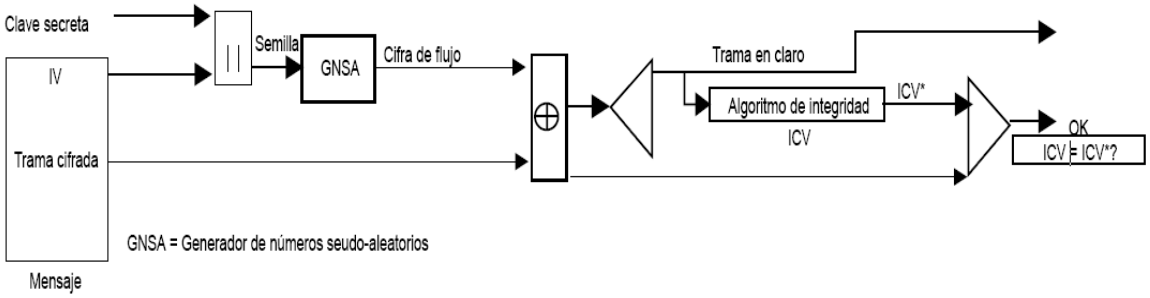


Figura 2.2 Funcionamiento del algoritmo WEP en modalidad de descifrado. (Molina 2003)

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el AP y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.
- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2□24 IV distintos. Esto no es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV en más o menos 5 horas. Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo; conociendo el funcionamiento del algoritmo RC4 es posible entonces obtener la clave secreta y descifrar toda la conversación.

WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el AP compartan la clave WEP para que la comunicación pueda llevarse a cabo. Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La

herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre AP y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respeto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP. 802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente /servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por al IEEE para uso en redes de área local alambrada, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad son compatibles con 802.1x. Este protocolo fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servicios fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se opto por emplearlos también para autenticación en las LAN. La autenticación se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS.

Según la complejidad de la red, un AP compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial:** para operar en esta modalidad requiere de la existencia de un servidor RADIUS en la red. El AP emplea entonces 802.1x y EAP para la autenticación y el servidor RADIUS suministra las claves compartidas que se usaran para cifrar los datos. Se requiere un certificado x.509 del lado del servidor

RADIUS. Los clientes solo requieren un nombre de usuario y password para acceder a la red como se muestra en la figura anterior.

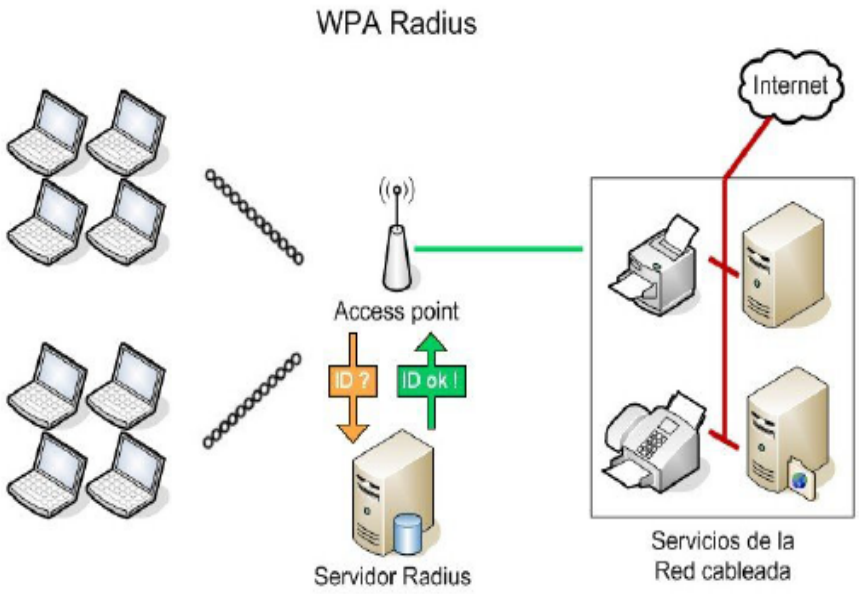


Figura 2.3: Red empresarial utilizando Radius

WPA con Radius ofrece la facilidad de administración de la red, debido al uso de llaves dinámicas en todo momento, se puede distribuir llaves de cifrado nuevas sin intervención de los usuarios. Los mecanismos de autenticación y auditoria son de los más fuertes hoy en día.

- **Modalidad de red casera, o PSK (Pre-Shared Key):** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el AP y en los dispositivos móviles. Esta clave puede ser de hasta 63 caracteres (504 bits). Cuando se logra el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Es recomendado que las contraseña sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta. Por su simplicidad, este modo es más apropiado para casas o pequeñas redes, y por eso se le llama WPA-Personal.

  WPA-PSK proporciona privacidad a los usuarios de la WLAN, puesto que se genera una cana cifrado independiente para cada uno de ellos. La llave de acceso

(PSK) se proporciona a los usuarios antes de conectarse a la red como se muestra en la figura. Este método es fácil de instalar, y proporciona confidencialidad, pero a la vez presenta varias debilidades como:

- La llave utilizada para cifrar es común para todos los usuarios de la red, aunque representa un avance respecto a WEP, dado que el canal de comunicación esta cifrado individualmente.
- WPA-PSK no proporciona control de acceso, cualquier usuario conociendo la llave (PSK) puede asociarse a la red.
- La forma de distribución de las llaves PSK representa un problema logístico similar al de distribuir una llave WEP, puede volverse impractico actualizar la llave de acceso a la red.
- El mecanismo se puede vulnerar por medio de un ataque de fuerza bruta fuera de línea. Bajo este ataque un intruso solo requiere grabar el inicio de la sesión de un usuario en la red y posteriormente atacarlo en un equipo poderoso, limitando el tiempo de ruptura de la contraseña a unos cuantos minutos en un caso extremo.
- Captura de trafico es posible por medio del ataque conocido como ARP cache poisoning en diversos fabricantes.
- La manera conocida para crackear WPA-PSK es solamente por un ataque de diccionario.

Herramientas para romper la clave WPA-PSK: Cowpatty (Linux).

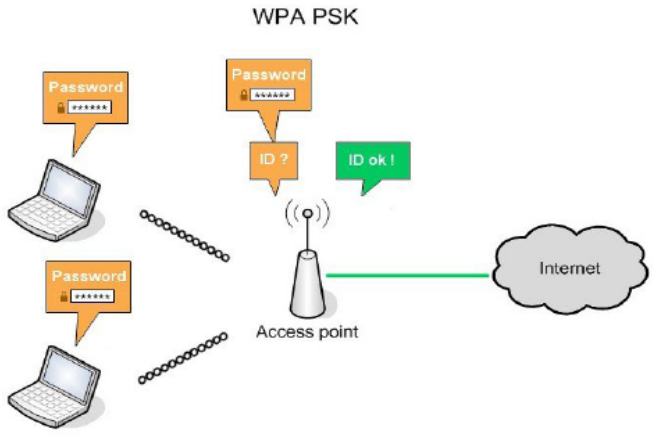


Figura 2.4: Modalidad de red casera

WIFI Alliance lanza en septiembre de 2004 su versión **WPA2** *(Wi-Fi Access Protected 2)*. WPA2, diseñado específicamente para las exigencias de entornos empresariales, se apoya en su predecesor WPA, resultan completamente compatible, siendo su principal diferencia que WPA2 utiliza un mecanismo de cifrado más avanzado como es AES. Sus principales diferencias con el estándar IEEE 802.11i, se basan principalmente en dos aspectos. El primero de ellos lo establece precisamente el hecho de su interoperabilidad con WPA, este permite a los usuarios anteriores de WPA asociarse a los nuevos puntos AP WPA2. En segundo lugar se encuentra que, tanto WPA como WPA2, están preparados para su utilización en entornos empresariales, pero adolecen de aspectos que sí presenta IEEE 802.11i para servicio de voz inalámbrico, como prevenir la pérdida de información durante el roaming o la latencia de la señal. WPA2 también admite dos modos de llevar a cabo la autenticación en dependencia del ámbito de aplicación: empresarial (IEEE 802.11i/EAP) y personal (PSK). Tanto el protocolo WAP, IEEE 802.11i, como WPA2, utilizan los mecanismos EAP e IEEE 802.1x para encargarse de la autenticación y gestión de claves. IEEE 802.1x no es una alternativa al cifrado. Solo contempla un marco para la autenticación y la distribución de claves, por lo que debe emplearse de forma conjunta con protocolos de autenticación para llevar a cabo la verificación de las credenciales de usuario, como puede ser cualquier tipo de EAP, así como la generación de claves de cifrado. Para implementar una solución basada en IEEE 802.1x, se hace necesario registrar en el servidor RADIUS todos los AP WLAN que pueden actuar como autenticador. Eliminando de esta forma el riesgo de ataques mediante la instalación de rogues APs o AP intrusos. En los AP a su vez se configurará toda la información relativa al servidor RADIUS del sistema IEEE 802.1x, evitándose ataques de suplantación de identidad. La autenticación entre el AP y el servidor RADIUS se realiza mediante una clave pre-compartida configurada en ambos extremos y conocida en el caso del protocolo RADIUS como "RADIUS secret".

En realidad IEEE 802.1x es un mecanismo de reparto y no proporciona la autenticación, por lo que se hace necesario seleccionar un tipo de EAP que defina las credenciales necesarias para llevar a cabo la autenticación. EAP lleva a cabo tareas de AAA (Authentication, Authorization, Accounting), diseñado inicialmente como una extensión del protocolo PPP (Point – To – Point Protocol). Proporciona conjuntamente un mecanismo estándar para aceptar métodos de autenticación adicionales. Por lo que puede emplear

múltiples esquemas de autenticación. Básicamente en el proceso autenticación las estaciones tratan de conectarse a un puerto del AP. Este, requerirá al terminal identificarse enviando los datos requeridos a un servidor de autenticación, por ejemplo, un servidor RADIUS; que comprueba la veracidad del nuevo dispositivo y envía su respuesta al AP, todo esto antes de establecer la comunicación IP con la estación. Hasta que el usuario se autentique, se mantendrá el puerto bloqueado. Una vez autenticado correctamente el usuario, el AP permitirá el tráfico DHCP. El servidor DHCP le asignará una dirección IP y permitirá el paso del tráfico desde y hacia el terminal abriendo el puerto.(Fleites 2007)

2.1.3 Mecanismos de seguridad del nivel de red

Básicamente la utilización de una **VPN** consiste en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto, dentro de protocolos que trabajan a nivel 2, en ellos se encuentran PPTP y L2TP o en el nivel 3 IPsec VPN de la pila del modelo OSI. El usuario solo puede comunicarse con la red corporativa a través del túnel establecido por el VPN. Este protocolo es un marco de estándares abiertos para asegurar comunicaciones privadas sobre redes IP, ideado y administrado para proporcionar seguridad al actual estándar IP. Además de proteger cualquier protocolo que se ejecute sobre IP, como lo pueden ser ICMP (Internet Control Message Protocol), UDP *(User Datagrama Protocol)*, TCP, este protocolo proporciona servicios criptográficos para la autenticación, confidencialidad e integridad de los paquetes, seguridad y control de acceso. Con la finalidad de proteger la integridad de los datagramas IP, IPsec VPN emplea códigos de autenticación de mensaje basados en HMAC (Hash Message Autentication Code) que son calculados aplicando algoritmos de resumen como MD5 y SHA, cuyo cálculo se basa en la clave secreta y los contenidos del datagrama IP. HMAC va incluido en la cabecera del protocolo IPsec VPN, por lo que puede ser comprobado por el receptor del paquete si tiene acceso a la clave secreta.(Fleites 2007) De forma similar es protegida la confidencialidad de los datagramas, pero esta vez utilizando algoritmos estándar de cifrado simétrico, actualmente son utilizados a tal efectos, 3DES (168 bits), AES (168/128, 192, 256 bits) y Blowfish. IPsecVPN necesita de un usuario IPsecVPN instalado, así como hardware adicional, un Gateway o controlador VPN, con el empleo de diferentes filtros para eliminar todo el tráfico que no provenga del Gateway ó de los servidores DHCP ó DNS. También se

hace necesario que los participantes de una comunicación de este tipo, consten con mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas. Los cuales se almacenan en asociaciones de seguridad, y definen ciertos parámetros como, dirección IP de origen y destino, protocolo IPsec (AH o ESP), algoritmo y clave secreta empleados, índice de parámetros de seguridad (número de 32 bits que identifica la asociación de seguridad). A su vez estas asociaciones de seguridad son almacenadas en bases de datos de asociaciones de seguridad, algunas de ellas permiten incluso almacenar más parámetros, modo IPsec, tamaño de la ventana deslizante y tiempo de vida de una asociación de seguridad. (Fleites 2007) Las asociaciones de seguridad solo especifican en qué forma se supone que este protocolo protegerá el tráfico, para definir qué tráfico proteger y cuando hacerlo se necesita información adicional que es almacenada en la política de seguridad (SP) que a su vez se almacenará en sus bases de datos.

IPsec emplea dos protocolos diferentes para asegurar la autenticación, integridad y confidencialidad de la información, AH (Authentication Header) este protege la integridad del datagrama IP, calculando una HMAC, basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP, tras esto, añade la cabecera AH al paquete; ESP (Encapsulating Security Payload), asegura la integridad del paquete y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. Estos dos protocolos pueden ser aplicados de forma combinada o individual. Cada uno, puede ser operado en una de dos formas; modo túnel, cuando el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP y el modo transporte, cuando IPsec solo maneja la carga del datagrama IP insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores IP. Por lo que IPsec puede proteger el datagrama IP completo o solo los protocolos de capas superiores. Un problema crítico de este protocolo lo constituye el intercambio de claves simétricas cuando aun no se ha establecido ningún tipo de cifrado. Empleándose IKE (Internet Key Exchange), se permite la autenticación de los participantes en la conexión y el intercambio de claves simétricas, permitiendo a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP. IKE en una primera fase autentica a los participantes y en una segunda fase negocia las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie

Hellmann así mismo se ocupa de renovar periódicamente las claves para asegurar su confidencialidad. (Faloutsos 2002) Otra desventaja es que las VPN basadas en IPsec, no proporcionan seguridad a nivel de enlace y solo protegen tráfico IP. Además resulta ser el método más efectivo de todos, pero el más complejo y costoso de implementar. Una solución VPN basada en IPsec es compatible con el uso de WPA e IEEE 802.11i. Este tipo de soluciones es recomendable para los casos en que la plantilla de la institución sea itinerante, para proporcionar seguridad al conectarse a Internet o la red de la institución desde otras redes que no sea la propia de la institución. (Molina 2003) Dentro de los elementos claves de la arquitectura de una red WLAN en la que se emplea una solución VPN basada en la tecnología IPsec se encuentran los dispositivos inalámbricos que proporciona la conectividad inalámbrica a los puntos de acceso, los software específicos IPsec VPN instalados en el dispositivo inalámbrico, aquí el usuario inicia la sesión VPN a través de este software especifico y es el concentrador VPN el encargado de autenticar y validar el acceso del usuario a la red WLAN. El punto de acceso inalámbrico proporciona la conectividad Ethernet a la red corporativa. Si el punto de acceso tiene capacidades de filtrado, se puede filtrar el trafico para permitir únicamente los protocolos DHCP e IPsec. El Gateway/concentrador IPsec VPN autentica y valida a los usuarios inalámbricos, puede realizar también funciones de servidor DHCP para los usuarios inalámbricos. Se recomienda ubicar un Firewall después del concentrador VPN que aplique políticas de seguridad al flujo no cifrado.

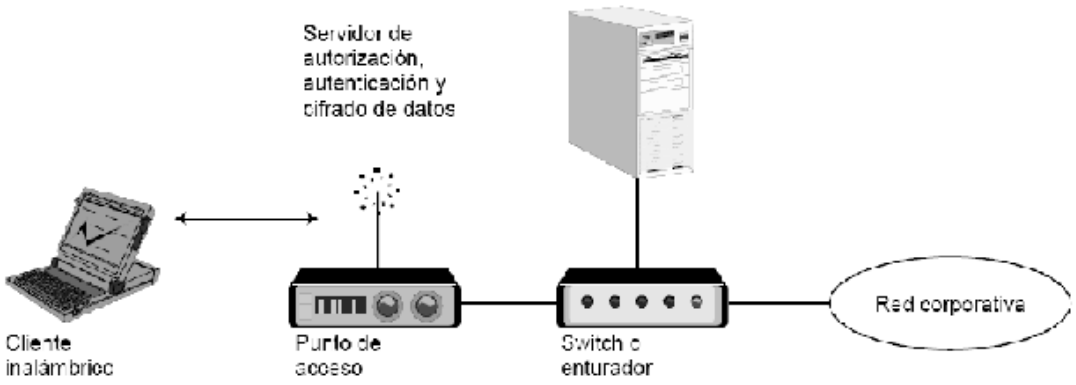


Figura 2.5: Estructura de una red privada virtual (Molina 2003)

Cuando se emplea el mecanismo VPN basado en IPsec se pueden utilizar varios mecanismos de autenticación: Servidor RADIUS, Servidor PKI que proporciona certificados X.509 para la autenticación de usuario servidor, recomendándose que los certificados de usuario sean accesibles solamente mediante hardware protegido con contraseña como por ejemplo smart-cards o llaves USB; servidor OTP que proporciona autenticación OTP mediante servidores RADIUS.

Para establecer los túneles IPsec en lugar de llaves pre-compartidas se recomienda utilizar políticas basadas en certificados. El empleo de llaves pre-compartidas es peligroso ya que si un atacante las obtiene, es difícil detectar que las llaves están comprometidas. Por lo que implica sobrecarga en el mantenimiento al tener que cambiar periódicamente las llaves pre-compartidas. Dentro de las ventajas e inconvenientes de esta solución de seguridad VPN basada en IPsec se encuentran:

Ventajas:

Emplear una solución de seguridad que permite al personal acceder a todos los recurso de la red

1. Permite definir diferentes perfiles de usuario.
2. Reutilización de la VPN fuera del entorno institucional.

Inconvenientes:

1. Necesidad de un concentrador VPN.
2. Sobrecarga de configuración de usuarios VPN.
3. Excluye a los invitados.
4. Es una solución costosa.

2.1.4 Mecanismos de seguridad del nivel de transporte

El tercer grupo de mecanismos de seguridad corresponde al del nivel de transporte, donde se encuentran SSL/TLS y a SSL VPN.

SSL (Secure Sockets Layer) se ha convertido en el estándar para comunicaciones seguras entre usuarios y servidores de Internet. Permite realizar transacciones en línea segura combinando para ello, tres elementos claves. El primero es la autenticación, que se basa en un certificado digital asociado a un nombre de dominio específico. Un segundo elemento resulta el cifrado; un certificado digital especial, SSL, une una identidad con un par de claves electrónicas que se pueden usar para cifrar y firmar información digital transmitida por Internet a través del protocolo " HTTP". Por último, integridad del mensaje, después de establecer una sesión SSL, los contenidos de todas las comunicaciones entre el usuario y el servidor están protegidas de ser manipuladas en la ruta. Con la combinación de estos tres elementos, SSL resulta una solución simple y extremadamente potente. Permite llevar a cabo transacciones autenticadas en línea y cifrado de la transmisión de datos de los visitantes de su página Web, no repudio de usuario y servidor, así como protección de los datos transmitidos. Para establecer una conexión SSL se necesita que el servidor tenga un certificado digital instalado.

Al pedir el usuario una conexión segura al servidor, este abre un puerto cifrado, gestionado por el software “Protocolo SSL Record”, ubicado encima de TCP, este software y el puerto abierto, serán empleados para comunicarse de forma segura con el usuario utilizando el software de alto nivel “Protocolo SSL Handshake”, a través del cual, usuario y servidor negocian mejoras de seguridad, que consisten en autenticar el servidor de usuario; permitirle a este y al servidor seleccionar los algoritmos criptográficos que ambos soportan; utilizar técnicas de encriptación de clave pública para generar secretos compartidos; establecer una conexión SSL cifrada hasta autenticar opcionalmente el usuario al servidor. Este proceso de intercambio de mensajes es iniciado por el usuario y consta de cuatro fases fundamentales; la de establecimiento, se establecen el conjunto de algoritmos para garantizar la confidencialidad e integridad y para la autenticación mutua; la fase de autenticación del servidor, en ella el servidor se autentica ante el usuario; la de autenticación de usuario e intercambio de claves y una última fase, en la que se verifican mutuamente la autenticidad de las partes involucradas y que el canal seguro ha sido correctamente establecido.

En lo adelante todos los paquetes transmitidos por SSL, durante la sesión segura abierta, son cifrados a demás de incorporarle un mecanismo para corroborar en todos sus pasos su autenticidad. Para el cifrado se utiliza cifrado simétrico, RC4 o IDEA y también se cifra la clave de sesión mediante un algoritmo de cifrado de clave pública como RSA (Rivest, Shamir y Adelman).

2.1.5 Mecanismos de seguridad del nivel de aplicación

Por último se analizarán los mecanismos que pertenecen a la capa superior del modelo de referencia OSI, específicamente al protocolo SSH (Secure Shell) y al HTTPS (HyperText Transfer Protocol Secure).

SSH se utiliza para acceder a máquinas remotas a través de la red, de forma similar a como lo hace telnet, lo que utilizando técnicas de cifrado para no descubrir ante un atacante, al usuario, la contraseña de la conexión y lo que se escribe durante toda la sesión. Este protocolo ofrece mecanismos robustos de autenticación con un incremento de la confidencialidad, donde la comunicación es transparente y automáticamente cifrada. El cifrado comienza antes de la autenticación y permite que las contraseñas no se transmitan claramente. Cualquier conexión TCP/IP puede ser redireccionada a través de un canal de cifrado SSH en ambas direcciones. (Othman 2007)

HTTPS, una versión segura del protocolo HTTP, utiliza un cifrado basado en Secure Socket Layer para crear un canal de cifrado; siendo más apropiado para el tráfico de información sensible que HTTP. Esta versión segura es empleada para redes WLAN públicas y se utiliza el método de autenticación universal (UAM) que es uno de los más extendidos en redes de este tipo. UAM permite solamente la autenticación de usuario en la red WLAN. Pero no se permite autenticar el AP al que se conecta el usuario. Ni implica el cifrado de la información enviada tras la autenticación del usuario en la red.

HTTPS redirecciona el navegador Web del usuario, un portal Web HTTPS, conocido como portal cautivo, que es una página Web de autenticación ubicada generalmente en un servidor Web local, situado en un Gateway de control de acceso. Para ello el usuario deberá introducir sus credenciales en este portal Web, que serán validadas por un servidor de

autenticación, generalmente un servidor RADIUS, que los verificará contra una base de datos de usuarios centralizada. Una vez que haya sido corroborada, el usuario puede hacer uso de la red. En dependencia del tipo de usuario, el sistema podrá asignarle un ancho de banda y le concederá acceso a diferentes servicios (ver Figura 2.6). (Othman 2007)

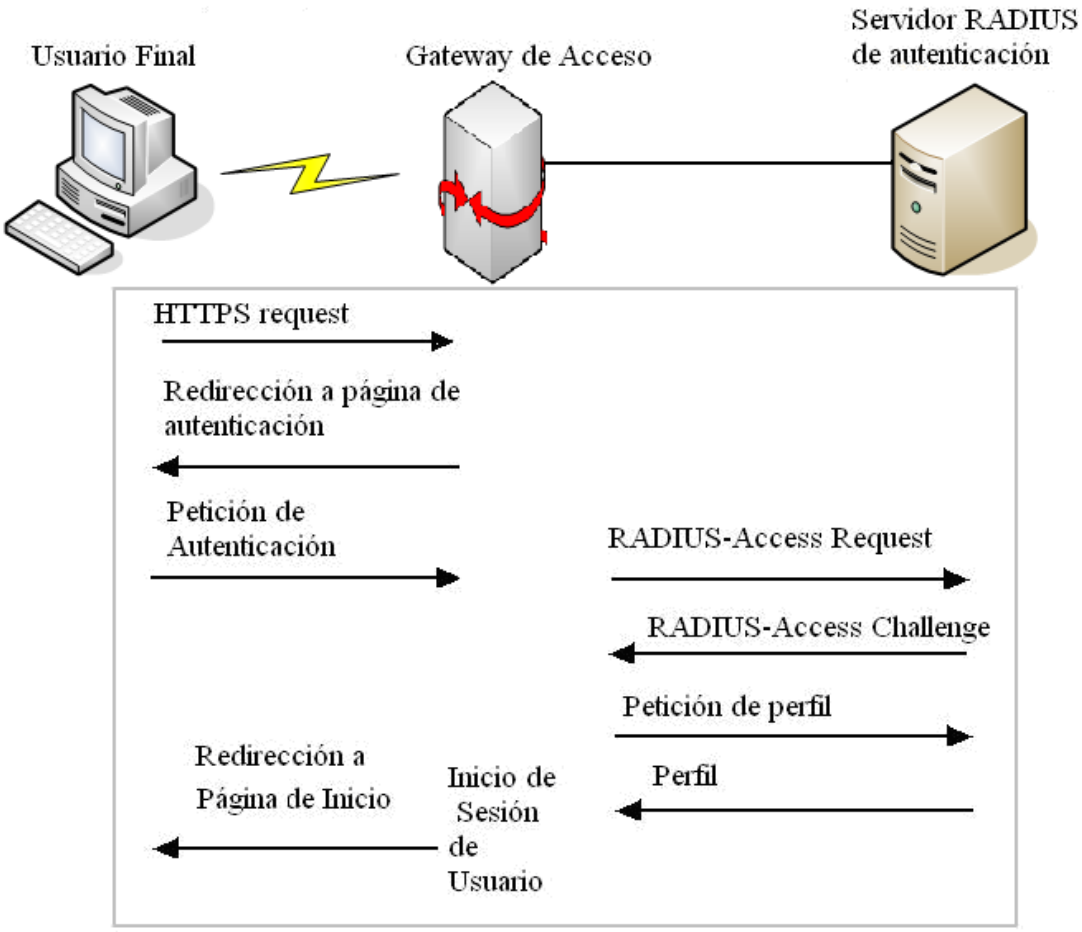
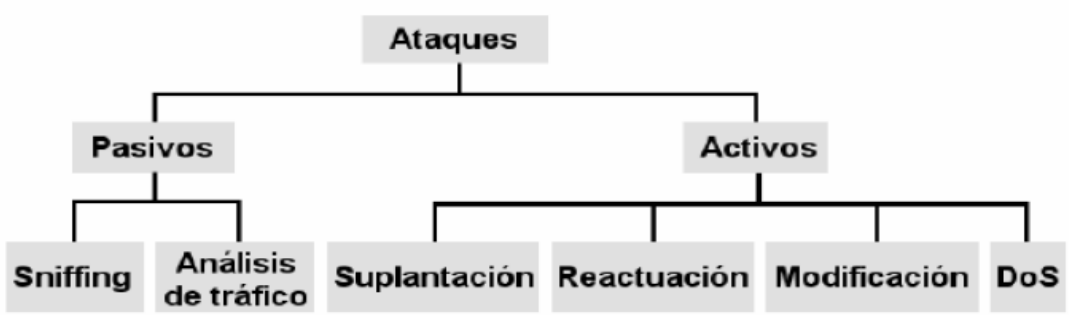


Figura 2.6: Autenticación UAM: intercambio de mensajes RADIUS(González 2007)

2.2 Ataques de seguridad

Un ataque informático es un método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático. Los ataques a las redes inalámbricas se hacen en dos etapas, en la primera se obtiene información de la red mediante ataques pasivos, y en la segunda se accede a la red mediante ataques activos. (Flores 2009)

En cuestiones de seguridad, es imprescindible conocer cuáles son las amenazas y ataques que puede sufrir en determinado momento la red, ya que son varios los métodos para descubrir, interceptar y atacar una red inalámbrica. Los ataques pasivos centran su actividad en métodos de monitoreo y escucha de la red, con el objetivo de obtener información, más bien para detectar la existencia de rede inalámbricas, así como los mecanismos de seguridad existente, generalmente utilizada en ataques posteriores a dicha red, mientras que los ataques activos crean un falso flujo en la transmisión de datos o sencillamente se modifica dicho flujo.



Esquema 2.1: Tipos de ataques en redes inalámbricas

2.2.1 Ataques pasivos

Warchalking

Consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red. (Molina 2003)

Wardriving

Propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada (que se puede elaborar fácilmente con una lata de conservas o de papas fritas) un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en el internet. Notablemente NetStumbler para Windows,

KisMac para Macintosh y Kismet o SWScanner para GNU/Linux. Una vez localizada una red inalámbrica, una persona podría llevar a cabo dos tipos de ataques:

• Ingresar a la red y hacer uso ilegítimo de sus recursos.

• Configurar un punto de acceso propio, orientando la antena de tal modo que los computadores que son clientes legítimos de la red atacada se conecten a la red del atacante. Una vez hecho esto, el atacante podría robar la información de dichos computadores, instalarles software maligno o dañar la información.(2008)

Sniffing

Tiene como objetivo monitorear la red con la finalidad de capturar información sensible, pero esta vez relacionada con contraseñas, identificadores de usuarios, las direcciones MAC, los IP de origen y destino, claves WEP, por lo que es considerado un paso previo a ataques posteriores. En este caso se necesita que el dispositivo que va a llevar a cabo el ataque este equipado de varios elementos; una tarjeta WLAN que actúa en modo monitor o modo promiscuo, para así poder recibir todo el tráfico que circula por la red, además de contar con la instalación de un software especial llamado Sniffer, que se encarga de monitorear toda la información. (González 2007)

Captura de contraseñas

Para descubrir contraseñas de usuarios, claves de cifrado de la información que viaja por la red, es necesario cierto tiempo previo de escucha y recopilación del tráfico en la red. Este tipo de ataque se basa principalmente en dos métodos, por fuerza bruta y de diccionario. El método por fuerza bruta intenta romper un cifrado probando todas las combinaciones posibles, mediante ellos se puede llegar a obtener las claves de los algoritmos de cifrados, los nombres de los usuarios y sus contraseñas de autenticación. Este método siempre consigue su propósito, de ahí que se diga que un cifrado seguro solo se puede romper por este tipo de ataque, su mayor problema radica en el tiempo que invierte en lograrlo. Mientras que el de diccionario emplea una serie de palabras probables, generalmente extraídas de un glosario de palabras y nombres, en vez de posibles combinaciones. De encontrarse la clave en estas posibles palabras, reduce considerablemente el tiempo necesario. Este tipo de ataque es la base para el descubrimiento de claves de mecanismos de cifrado como WEP (Wired Equivalent Privacy). Para ello utiliza software como, Aireplay,

Chopchop, Weplab, Aircrack; que prueban las posibles contraseñas a gran velocidad. El algoritmo para llevar a cabo un ataque de este tipo es el siguiente:

- El atacante comienza enviando tráfico sin cifrar o tráfico plano, como también se le conoce, a través de la red a un usuario legítimo.
- Dicho usuario cifra el tráfico y lo envía al punto de acceso.
- Tráfico cifrado, que es interceptado por el atacante, quien establece una comparación del contenido, obteniendo finalmente la clave de cifrado WEP de la red.

Descubrimiento de SSID ocultos

Un usuario para poder conectarse a una WLAN primeramente debe conocer de antemano la existencia de dicha red. La SSID (Service Set Identifier), nombre de la red de un Hotspot que es transmitido continuamente en texto legible a través del Punto de Acceso (Broadcasting), es un código con un máximo de 32 caracteres alfanuméricos incluidos en todos los paquetes de una red WLAN para identificarlos como parte de ella. Todos los ordenadores existentes en su radio de acción reciben esta señal y pueden ponerse en contacto con el Punto de Acceso.

Basándose en el modo en que funcione la red (Ad-Hoc /infraestructura) el SSID se denominará, BSSID (Basic Service Set Identifier) o ESSID (Extended Service Set Identifier) respectivamente. El BSSID suele ser la dirección de la capa MAC del equipo y por tanto única; mientras que el ESSID es el nombre de 32 caracteres de la red que debe ser el mismo para todos los puntos de acceso de la misma red. Este último parámetro es clave a la hora del descubrimiento de una WLAN, para ello existen dos procesos fundamentales siempre y cuando la WLAN se encuentra en modo infraestructura, el de escaneo pasivo donde el dispositivo de usuario espera recibir la señal del punto de acceso y el escaneo activo en el cual la estación lanza tramas a un punto de acceso determinado y espera una respuesta.(González 2007)

Para descubrir el ESSID oculto se puede hacer sniffing y esperar a que un cliente se conectara, y veríamos el ESSID en la trama Prove Request del cliente (en el caso de que no se manden Beacon Frames), o en la trama Prove Response del AP. Pero también podemos ``provocar´´ la desconexión de un cliente, utilizando el mismo método que en el ataque DoS, pero mandando sólo una trama de desasociación o de desautenticación en lugar de

mandarlas repetidamente, es decir, nos ponemos la dirección física del AP y mandamos una trama de desautenticación ó disociación a la dirección MAC del cliente (o a la de broadcast), entonces el cliente intentará volver a asociarse ó autenticarse, con lo que podremos ver el ESSID en los management frames.(Gutierrez 2006)

2.2.2 Ataques activos

Como ya se había descrito con anterioridad con el esquema de figura 2.7, se puede distinguir cuatro técnicas en el proceso de los ataques activos que se describe a continuación:

- Suplantación (Fabricación): mediante un sniffer para hacerse con varias direcciones MAC validas. El análisis de tráfico será de ayuda para poder conectarse suplantando un usuario. Otra forma de implementar este ataque es instalar puntos de acceso ilegitimo (rouge) para engañar a usuario legitimo para que se conecten a este AP en lugar del autorizado, afectando así la autenticidad de los datos.
- Reactuación (Interceptación): Inyectar en la red paquetes interceptados utilizando un sniffer para repetir operaciones que habían sido realizados por el usuario legítimo, afectando así la confidencialidad de los datos.
- Modificación: el atacante manipula, añade, borra o reordena los mensajes transmitidos, afectando así la integridad de los datos.
- Denegación de servicio (DOS): un atacante puede generar interferencias hasta que se produzcan tantos errores en la transmisión que la velocidad caiga a extremos inaceptables o la red deje de operar en absoluto. También se hace posible mediante la inundación de solicitudes de autenticación, solicitudes de desautenticacion de usuarios legítimos, tramas RTS/CTS para silenciar la red, afectando así la disponibilidad.

Ataque de denegación de servicio (DoS)

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima ó sobrecarga de los recursos computacionales del sistema de la víctima. En las redes inalámbricas los ataques

de denegación de servicio pueden ser clasificados principalmente en dos tipos, aquellos en la capa de enrutamiento y aquellos en la capa de acceso al medio MAC. En el caso de las redes wireless lo que se realiza son transferencias de paquetes de información. Cada paquete contiene entre otros datos las direcciones de origen y destino, número de paquete dentro de la secuencia de transmisión, la información a transferir y un valor de comprobación de la integridad del paquete (CRC) para asegurar que no han existido errores en la transmisión. (García 2003)

De esta forma a diferencia de la televisión o la radio no podemos "perder" o recibir un paquete de información erróneo y continuar tranquilamente. Este paquete debe ser retransmitido hasta que llegue de forma correcta y en la secuencia o posición adecuada.

El ataque más obvio a las redes sin hilos consiste en la emisión de ruido de forma que consigamos degradar los paquetes de datos transmitidos de forma que se vuelva prácticamente imposible la comunicación. De hecho, si el atacante logra un simple cambio en un bit del paquete de datos, el CRC lo detectará y se deberá retransmitir. (Alvarez 2004)

El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado sin un número de formas. Aunque básicamente consisten en:

1. Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
2. Alteración de información de configuración, tales como información de rutas de encaminamiento.
3. Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
4. Interrupción de componentes físicos de red.
5. Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.(Zubieta 2006)

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice

"denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Para realizar este ataque basta con hacer sniffing durante un momento la red y ver cuál es la dirección MAC del AP. Una vez conocemos su MAC, nos la ponemos y actuamos como si fuéramos nosotros mismos el AP. Lo único que tenemos que hacer para denegarle el servicio a un cliente es mandarle continuamente notificaciones (management frames) de desasociación o desautenticación. Si en lugar de a un solo cliente queremos denegar el servicio a todos los clientes de la WLAN, mandamos estas tramas a la dirección MAC de broacast.

Port Stealing (robo de puerto)

En este ataque el atacante envía muchos frames Ethernet (paquetes de capa 2), con la dirección MAC de la víctima como origen, y como destino su propia dirección MAC. Esto hace que el switch crea que la víctima está conectada en el puerto del atacante (de ahí el nombre de esta técnica).

Cuando el atacante recibe un paquete destinado a la víctima, este genera un ARP request preguntando por la MAC asociada a la IP de la víctima. Cuando la víctima responde el switch vuelve a conocer en donde está ubicada realmente la víctima, es entonces cuando el atacante reenvía el paquete recibido (intacto o modificado, dependiendo de los intereses del atacante). Luego vuelve a robar el puerto y espera por el próximo paquete con destino final a la víctima. Esta técnica degrada la conectividad de la víctima notablemente y es fácilmente detectable por los IDS. El uso de entradas ARP estáticas en las PC no resuelve el problema. Una herramienta capaz de realizar este ataque es el Ettercap con el plugin confusión.(Miquel Oliver 1999)

DHCP Spoofing

Los requerimientos de DHCP son hechos con frames de tipo broadcast, ya que deben ser escuchados por todos los dispositivos dentro de la red local. Si un atacante responde antes que el verdadero servidor, este puede pasarle información errónea a la víctima, como por ejemplo puede decirle que la puerta de enlace es él.
Para algunos servidores de DHCP suele ser bastante sencillo responder antes que él, debido a que muchos verifican si no hay otro dispositivo en la red con la dirección que van a

entregar; mientras el servidor real comprueba, el atacante tiene tiempo valioso en el que puede responder antes. Los IDS detectan este ataque debido a que se producen múltiples respuestas para una única solicitud. Así como las anteriores, ettercap también es capaz de realizar este ataque.(Yáñez-Mingot 2006)

Smurf

El ataque smurf, es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar (flood) un objetivo (sistema atacado).

En este tipo de ataque, el perpetrador envía grandes cantidades de tráfico ICMP (ping) a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada (spoofing) a la dirección de la víctima. Si el dispositivo de ruteo envía el tráfico a esas direcciones de broadcast lo hace en capa 2 donde está la función de broadcast, y la mayoría de los host tomarán los mensajes ICMP de echo request y lo responderán, multiplicando el tráfico por cada host de la subred. En las redes que ofrecen múltiples accesos a broadcast, potencialmente miles de máquinas responderán a cada paquete. Todas esas respuestas vuelven a la IP de origen (la IP de la víctima atacada).

Algunos años atrás, todas las redes ruteaban smurf ataques -- en la jerga se dice que eran "smurfeables" -- Hoy día la mayoría de los administradores han inmunizado sus redes contra estos abusos aunque muchas redes permanecen smurfeables. (Faloutsos 2002)

Ping flood

Consiste en saturar una línea lenta con un número de paquetes ICMP suficientemente grande. Esta saturación causará una degradación del servicio importante. El ataque en cuestión utiliza las definiciones de la longitud máxima de protocolos así como la capacidad de fragmentación de los datagramas IP.

La longitud máxima de un datagrama IP es de 64K (65535 Bytes) incluyendo la cabecera del paquete (20 Bytes). El protocolo ICMP es el que se utiliza para la comunicación de mensajes de control de flujo en las comunicaciones. Luego para enviar un mensaje ICMP tenemos disponibles 65535(datos) 20 (cabecera IP) 8 (cabecera ICMP) = 65507 Bytes. En el caso de enviar órdenes al sistema operativo para que envíe un datagrama de longitud de 65510 bytes (inferior a los 65535) con lo que los datos a enviar cogen un único paquete IP (fragmentado en N trozos, pero pertenecientes al mismo datagrama IP).

Si sumamos:

65510 + 20 + 8 =65538

Debido a que el espacio disponible tan sólo es de 65535 bytes al reensamblar el paquete en el destino se suelen producir errores de overflow/coredump que causan la parada del servicio o del sistema atacado.

Es importante señalar que estas técnicas de ataque informático sólo pueden ser usadas cuando se tiene un alto grado de conocimientos informáticos, pues no es fácil determinar la cantidad de bytes ICMP que debe contener el paquete ICMP.(Pellegrino 2006)

ARP Poisoning

ARP Poisoning ó ”Envenenamiento ARP”, es un ataque al protocolo ARP (Adress Resolution Protocol) y que sólo se puede llevar a cabo cuando el atacante está conectado a la misma LAN lógica que las víctimas, limitando su efectividad a redes conectadas con switches, hubs y bridges, pero no routers. La mayoría de los AP 802.11b actúan como bridges transparentes de capa 2, lo que permite que los paquetes ARP pasen de la red inalámbrica hacia la LAN donde está conectado el AP y viceversa. Esto permite que se ejecuten ataques de ARP cache poisoning contra sistemas que están situados detrás del AP, como por ejemplo servidores conectados a un switch en una LAN a los que se pueda acceder a través de la WLAN. (Gutierrez 2006)

El Pc1 se comunica con Pc3 a través del switch, si un atacante desde la WLAN envenena la tabla de ARP´s de Pc1 y de Pc3 podría realizar un ataque del tipo hombre en el medio situándose entre los dos hosts de la red cableada. El atacante manda paquetes `ARP REPLY´ a Pc3 diciendo que la dirección IP de Pc1 la tiene la MAC del atacante, de esta manera consigue `envenenar´ la caché de ARP´s de Pc3. Luego realiza la misma operación atacando a Pc1 y haciéndole creer que la dirección IP de Pc3 la tiene también su propia MAC. Como ARP es protocolo `stateless´, Pc1 y Pc3 actualizan su caché de acuerdo a la información que el atacante ha inyectado a la red. Como el switch y el AP forman parte del mismo dominio de broadcast, los paquetes ARP pasan de la red inalámbrica a la red con cables sin ningún problema.(Gutierrez 2006)

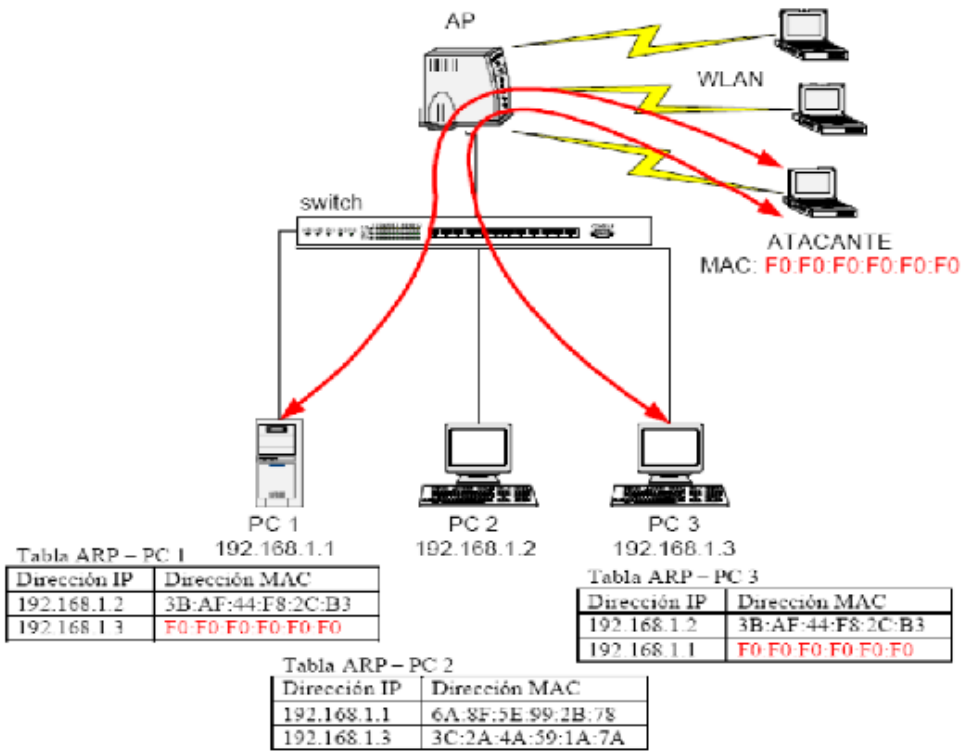


Figura 2.8: Envenenamiento ARP (Gutierrez 2006)

Puntos de acceso no autorizados

Este es uno de los ataques más nocivos, para lograrlo se hace necesario tener acceso a la instalación física de la red y así poder conectar un punto de acceso de forma no autorizada directamente a ella. Al no ser gestionados por el personal de la red, tampoco se tienen que ajustar a sus políticas de seguridad y por tanto implican una importante brecha de seguridad ante cualquier tipo de ataques, vulnerando todos los mecanismos de seguridad que se basan en cifrado de datos entre extremos, dígase por ejemplo: WEP, WPA entre otros. Estos puntos de acceso suelen, por lo general, emitir con más potencia que los válidos a fin de que los usuarios se conecten por defecto a ellos.

Ataque de Denegación de Servicio Distribuido

Un ataque DDOS (Distributed Denial Of Service Attack) es un tipo especial de DoS consistente en la realización de un ataque conjunto y coordinado entre varios equipos hacia un servidor víctima. La particularidad de este ataque, a diferencia del simple DoS, es el hecho de que el ataque proviene de diferentes partes del mundo, haciendo imposible cerrar la ruta de donde proviene el mismo, ya que no sólo es una, sino varias, dejando como única

opción desconectar el servidor de la red y esperar a que el ataque cese. Normalmente los ataques se llevan a cabo por varias oleadas. Pueden durar un par de minutos o incluso días, como ha sucedido en casos reales. Esto es posible gracias a un cierto tipo de malware que permite obtener el control de esas máquinas y que un atacante ha instalado previamente en ellas, bien por intrusión directa o mediante algún gusano. Los DDoS consiguen su objetivo gracias a que agotan el ancho de banda de la víctima y sobrepasan la capacidad de procesamiento de los routers, consiguiendo que los servicios ofrecidos por la máquina atacada no puedan ser ofrecidos. A consecuencia de esto, generalmente el servidor queda fuera de servicio voluntariamente por los administradores y proveedores, debido al alto gasto de recursos y ancho de banda.

A las máquinas infectadas por el malware mencionado anteriormente se las conoce como máquinas zombie, y al conjunto de todas las que están a disposición de un atacante se le conoce como botnet.

Ataque de fuerza bruta

La semilla de 32 bits que utiliza el PRNG es obtenida a partir de la passphrase normalmente contiene caracteres ASCII, por lo cual el bit más alto de cada carácter siempre es cero. El resultado de la operación XOR de estos bits también es cero y esto provoca una reducción de la entropía de la fuente, es decir, las semillas sólo podrán ir desde 00:00:00:00 hasta 7F:7F:7F:7F en lugar de hasta FF: FF: FF: FF

El uso del PRNG con esta semilla también reduce la entropía. De la semilla de 32 bits sólo utilizan los bits del 16 al 23. El generador es un generador lineal congruente (LGC: linear congruential generator) de módulo 2^32, esto provoca que los bits más bajos sean `menos aleatorios´ que los altos, es decir, el bit 0 tiene una longitud de ciclo de 2^1, el bit 1 de 2^2, el bit 2 de 2^3, etc. La longitud de ciclo del resultado será por tanto 2^24. (Gutierrez 2006)

Con esta longitud de ciclo sólo las semillas que vayan de 00:00:00:00 a 00: FF: FF: FF producirán llaves únicas. Como las semillas sólo llegan hasta 7F:7F:7F:7F y la última semilla que tiene en cuenta el PRNG es 00: FF: FF: FF, sólo necesitamos considerar las semillas desde 00:00:00:00 hasta 00:7F:7F:7F por lo que la entropía total queda reducida a 21 bits. El conocimiento de estos datos nos permite hacer ataques de fuerza bruta contra la encriptación WEP generando llaves de forma secuencial utilizando las semillas desde 00:00:00:00 hasta 00:7F:7F:7F. Utilizando este proceso, un procesador PIII a 500Mhz

tardaría aproximadamente 210 días en encontrar la llave, aunque se puede usar computación en paralelo para obtener la llave en un tiempo más razonable.

También existe la posibilidad de utilizar un diccionario para generar sólo las semillas de las palabras (o frases) que aparezcan en el diccionario, con lo que si la passphrase utilizada está en el diccionario conseguiríamos reducir sustancialmente el tiempo necesario para encontrarla. (Gutierrez 2006)

Ataque inductivo Arbaugh

Este ataque se basa en explotar la vulnerabilidad de MIC independiente de la llave aprovechando también la redundancia de información producida por el CRC. La estación receptora en WEP únicamente aceptará un mensaje si el ICV (Integrety Check Value) es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV
- Los CRCs son lineales: CRC (m k)= CRC(m) CRC(k)

Debido a que los CRCs son lineales, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es linear y esto permite hacer el `bit flipping´ como veremos a continuación:

-Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m´:

$$m' = m \oplus \Delta$$

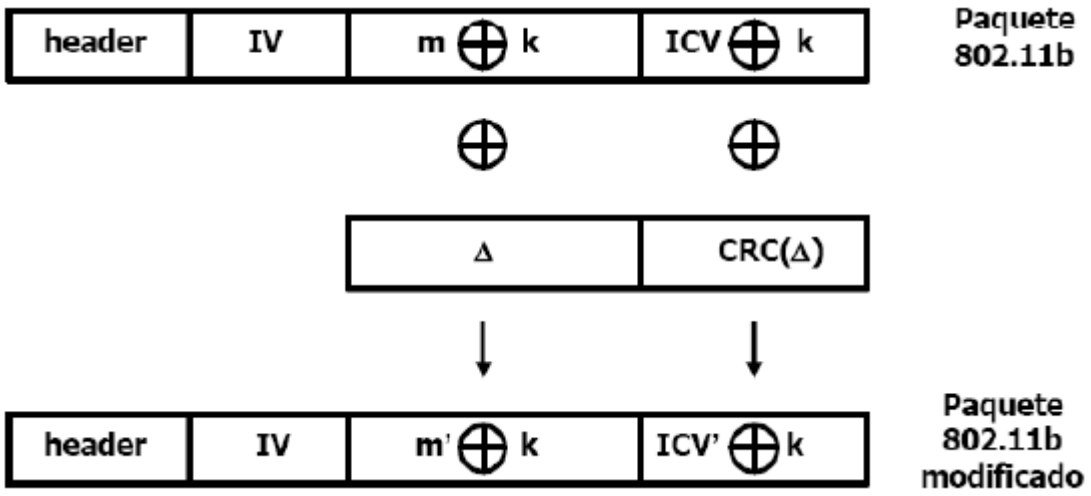
- Como el CRC-32 es linear, puede generar un nuevo ICV´ a partir del ICV de m:

$$IC' = IC \oplus h(\Delta)$$

- ICV´ será válido para el nuevo cyphertext c´

$$c' = c \oplus \Delta = k \oplus (m \oplus \Delta) = k \oplus m'$$

Todo este proceso se puede resumir en el esquema siguiente:



Ataque al método Shared Key

Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición ``resolved condition´´ o condición resuelta. Cada uno de estos paquetes resueltos sólo tiene ausencia de información de un byte de la llave. Para realizar el ataque más rápidamente sólo se buscan los IVs débiles que cumplen esta condición. Hay una posibilidad del 5% de adivinar el byte de la llave correctamente cuando encontramos un paquete resuelto (con un IV débil). Pero como hay gran cantidad de paquetes resueltos viajando por la red, las posibilidades son aún mayores.

El atacante captura el segundo y el tercer management messages de una autenticación mutua (Authentication Challenge y Authentication Response). El segundo mensaje contiene el texto de desafío en claro, y el tercer mensaje contiene el desafío encriptado con la clave compartida. Como el atacante conoce el desafío aleatorio (plantext, P), el desafío encriptado (cyphertext, C), y el IV público, el atacante puede deducir el flujo pseudo-aleatorio (keystream) producido usando WEP utilizando la siguiente ecuación:

$$WEP_{PR}^{K,IV} = C \oplus P$$

El tamaño del keystream será el tamaño de la trama de autenticación, ya que todos los elementos de la trama son conocidos: número de algoritmo, número de secuencia, status code, element id, longitud, y el texto de desafío. Además, todos los elementos excepto el texto de desafío son los mismos para todas las Authentication Responses. El atacante envía un Authentication Request al AP con el que se quiere asociar. El AP contesta con un texto de desafío en claro. El atacante entonces, coge el texto de desafío aleatorio, R, y el flujo

pseudo-aleatorio WEP k, IV PR y genera el cuerpo de una trama Authentication Response válido, realizando una operación XOR con los dos valores. El atacante entonces debe crear un nuevo ICV valido aprovechando la vulnerabilidad de Características lineares de CRC32. Una vez creado el nuevo ICV, el atacante acaba de completar la trama de Authentication Response y la envía de esta manera se asocia con el AP y se une a la red.

Con este proceso el atacante sólo esta autenticado, pero todavía no puede utilizar la red. Como el atacante conoce la clave compartida, para poder utilizar la red debe implementar algún ataque al protocolo WEP. (Gutierrez 2006)

Ataque contra ACL (Acess Control List)

Para llevar a cabo el ataque basta con hacer sniffing durante un momento el tráfico y fijarnos en la MAC de cualquiera de los clientes, sólo hace falta que nos pongamos su misma MAC y ya habremos saltado la restricción. Esto es sencillo de implementar, por ejemplo en el OS Linux se puede realizar con el comando ``ifconfig´´ dependiendo del tipo de tarjeta que tengamos. También existen otras utilidades para cambiar la MAC como ejemplo ``setmac´´. Hay que tener en cuenta que si hay dos máquinas en la red con la misma dirección MAC podemos tener problemas, aunque generalmente en las redes wireless esto no suele ser un problema muy grave ya que el AP no puede distinguir que verdaderamente hay dos máquinas con la misma MAC. De todas formas, si queremos podemos ``anular´´ a la máquina que le hemos ``robado´´ la dirección MAC. (Gutierrez 2006)

Hombre en el medio

El ataque de ``Man in the middle´´, también conocido como ``Monkey in the middle consiste en convencer al cliente (la victima) de que el host que hay en el medio (el atacante) es el AP, y hacer lo contrario con el AP, es decir, hacerle creer al AP que el atacante es el cliente. Para realizar este ataque, primero debemos esnifar para obtener:

- El ESSID de la red (si está oculto, usaremos el método anterior)
- La dirección MAC del AP
- La dirección MAC de la víctima

Una vez conocemos estos datos, utilizamos el mismo método que en el ataque DoS, para desautenticar a la víctima del AP real, es decir, el atacante hace spoofing (suplantación) de su MAC haciéndose pasar por el AP y manda tramas de desautenticación a la víctima. La

tarjeta wi-fi de la victima empezará entonces a escanear canales en busca de un AP para poderse autenticar, y ahí es donde entra en juego el atacante. El atacante hace creer a la victima que él es el AP real, utilizando la misma MAC y el mismo ESSID que el AP al que la víctima estaba autenticada anteriormente, pero operando por un canal distinto. Para realizar esto la tarjeta wi-fi del atacante debe estar configurada en modo máster. Por otra parte, el atacante debe asociarse con el AP real, utilizando la dirección MAC de la víctima. De esta manera hemos conseguido insertar al atacante entre la víctima y el AP, todos los datos viajan entre la víctima y el AP pasan a través del atacante. Como el ataque ha sido realizado a nivel de enlace (nivel 2), el atacante puede ver, capturar e incluso modificar las tramas en los niveles superiores del modelo OSI. Hay que tener en cuenta muchas soluciones de seguridad están pensadas asumiendo que las capas 1 y 2 son seguras, esto como hemos visto es incierto para las redes inalámbricas y por tanto el uso de según que tipo de solución podría no ser adecuado para estas redes. (Gutierrez 2006)

Ataque de inundación RREQ

La inundación de paquetes RREQ en toda la red consume muchos recursos. Para reducir la congestión en una red, el protocolo de AODV adopta algunos métodos. Un nodo no puede originar más de RREQ_RATELIMIT mensajes RREQ por segundo. Después de transmitir un RREQ, un nodo espera por un RREP. Si para dicha ruta no se recibe el RREP dentro de "roundtrip" milisegundos, el nodo puede intentar descubrir la ruta de nuevo transmitiendo otro RREQ, a un máximo de intentos al valor de TTL máximo. Repetidos esfuerzos por un nodo fuente al descubrimiento de ruta para un solo el destino debe utilizar un "binary exponential backoff". La primera vez un nodo fuente transmite un RREQ, él espera un tiempo "roundtrip" para la recepción de un RREP. Si un RREP no se recibe dentro de ese tiempo, el nodo fuente envía un nuevo RREQ. Al calcular el tiempo de espera para el RREP después de enviar el segundo RREQ, el nodo fuente debe usar un "binary exponential backoff". Por lo tanto, el tiempo de espera por el RREP correspondiente al segundo RREQ es 2 * roundtrip time. Los paquetes RREQ son transmitidos en un anillo creciente reduciendo el overhead causado por la inundación de la red entera. Los paquetes se inundan en una área pequeña (un anillo) primero definido por un TTL inicial (tiempo de vida) en la cabecera IP. Si no se ha recibido el RREP, el área inundada se agranda

aumentando el TTL por un valor fijo. El procedimiento se repite hasta que un RREP se reciba por el creador del RREQ, es decir, la ruta se ha encontrado.(Yáñez-Mingot 2006)

El Ataque de Inundación en redes ad hoc, el nodo atacante viola las reglas anteriores para agotar los recursos de la red. Primeramente, el intruso selecciona muchas direcciones IP que no están en la red, esto es, si él sabe el alcance de direcciones IP en la red. Porque ningún nodo puede responder los paquetes de RREP para éstos RREQ, la ruta inversa en la tabla de ruteo del nodo será conservado mucho tiempo. El atacante puede seleccionar al azar las direcciones IP si es que él no puede saber alcance de las direcciones IP. Después, el atacante origina masivamente mensajes RREQ para estas direcciones IP nulas. El atacante intenta enviar RREQ's sin considerar un RREQ_RATELIMIT por segundo. El atacante reenviara paquetes RREQ sin esperar por el RREP o roundtrip time. El TTL de los RREQ's se inicializan al máximo sin usar el método de expansión de anillo. En los ataques de inundación, la red entera estará llena de paquetes RREQ que el atacante envía. El ancho de banda de la comunicación es agotada por la inundación de paquetes RREQ así como los recursos en los nodos. Por ejemplo, el almacenamiento de la tabla de ruteo es limitada. Si masivos paquetes de RREQ están llegando a un nodo en poco tiempo, el almacenamiento en la tabla de ruteo del nodo se agotará y éste no podrá recibir nuevos paquetes RREQ. Como resultado, los nodos legítimos no pueden no descubrir rutas para enviar datos. La figura 1 muestras un ejemplo de un ataque por inundación de paquetes RREQ. El nodo H es el atacante e inunda con paquetes RREQ toda la red para que otros nodos no puedan construir rutas. (Yáñez-Mingot 2006)

Ataque por inundación de datos

Primero, el atacante crea rutas a todos los nodos en la red. Después, manda excesivamente paquetes de datos inútiles a través de dichas rutas. Los excesivos paquetes de datos en la red agotan el ancho debanda disponible para las comunicaciones entre los nodos. El nodo destino estará ocupado recibiendo los paquetes y no podrá trabajar normalmente. La característica común de dos tipos de ataques de inundación es agotar el ancho de banda disponible de la red afectando así la comunicación legítima. Por otra parte, cada ataque tiene sus características particulares. El ataque por inundación de paquetes RREQ produce desbordamiento en la tabla de ruteo del nodo para que el nodo no pueda recibir nuevos

paquetes RREQ. En el ataque de inundación de paquetes de DATOS, el proceso de recibir el ataque de paquetes consumirá muchos recursos en los nodos. Si el atacante combina dos tipos de ataques, producirá el colapso de la red entera. (Miquel Oliver 1999)

CAPITULO 3 TÉCNICAS DE PREVENCIÓN Y CONTRAMEDIDAS AL ATAQUE EN REDES INALÁMBRICAS

Mientras que los ataques DoS han sido ampliamente estudiados en las redes tradicionales, se ha hecho poca investigación para analizar y prevenir estos ataques en las redes inalámbricas y pocos trabajos se encuentran al respecto. Cuando un ataque ocurre, técnicas de prevención y contramedidas como encriptamiento y autenticación, son usualmente las primeras líneas de defensa. Sin embargo, estas técnicas pueden no ser suficientes a medida que los sistemas se van volviendo más complejos y siempre existen debilidades que se pueden explotar debido a errores de programación y de diseño o la fragilidad y poca compatibilidad de los protocolos y estándares existentes.(Faloutsos 2002)

3.1 Garantizando la seguridad en una red inalámbrica

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

• Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

• Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

• Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

3.2 Denegación de servicio en la capa MAC

Efecto captura

El efecto captura sucede cuando debido a un tráfico mucho mayor, los tráficos que circulan por una red son suprimidos casi en su totalidad. Esto ocurre ya que el algoritmo de Backoff de 8002.11, BEB, siempre favorece al último nodo que ganó el turno de transmitir, es decir, al nodo más activo. Cuando un nodo transmite exitosamente, la ventana de contención del algoritmo se reinicia a su límite mínimo: 31. Mientras los otros nodos han estado retrocediendo sin lograr transmitir y sus ventanas de contención son mucho mayores, el nodo con la ventana de contención igual a 31nuevamente gana el derecho a transmitir. Este efecto muestra sus peores consecuencias cuando la transmisión es hecha sobre nodos en la vecindad de una fuente de tráfico o de su destino, creando congestiones que evitan que el flujo normal sea enviado por su cliente o sea recibido por el nodo servidor, ya que el nodo con la tasa de envío alta siempre tiene prioridad para acceder al canal y bloquea el normal intercambio de paquetes de control, haciendo que los otros nodos siempre escuchen el canal como ocupado y se vean obligados a retroceder en su transmisión. Los dos factores en orden de importancia, que llevan a que el efecto se produzca son: El número de saltos, es decir, cuanto menor número de saltos tenga una transmisión mayor es la prioridad de suprimir el tráfico ganando el acceso al medio y la cantidad de tráfico enviado, a mayor tráfico peores las consecuencias pues los nodos con carga más pesada tienden a ganar el canal y hacen que los otros entren en su proceso de Backoff continuamente. El efecto captura es la causa principal para que la presencia de ataques de denegación de servicio basados en congestión sobre la capa MAC de una red de múltiple salto, se puedan presentar y sean muy fáciles de lanzar y de lograr. Cuando un nodo realiza una transmisión a una tasa muy alta, es decir, ataca otro nodo (sea éste cómplice o no) en la vecindad de un tercero, el tráfico que envía lo recibe este tercero o puede llegar a suprimirse y el efecto es aún peor si sobre la estación convergen varios tráficos, ya sea por ser el destino final o por ser un paso necesario en la ruta a su destino. (Krishnamuthy 2004)

Escenario de simulación

Los escenarios de simulación son redes de topología en malla, con diferentes números de nodos (25, 36, 49, 64, 81, 100, 121, 144, 169). El área de simulación varía de acuerdo con

el número de nodos de la red (ej. para 169 nodos, 13*350m=4.550m*4.550m). Este escenario fue escogido debido a su simplicidad en mostrar el impacto de la inequidad e injusticia de la capa MAC sobre TCP debido al ataque. Los nodos están separados 350 metros con la potencia ajustada para que el rango de transmisión cubra esta distancia hasta 376 metros, por lo tanto la transmisión es posible solo en forma horizontal y/o vertical. Desde los nodos de la esquina y en la mitad del borde exterior de la malla son enviados 1000 paquetes de 512 bytes de tipo TCP en 8 diferentes sesiones hacia el nodo central de la red durante 900 segundos de simulación (1000*512*8=4096Kbytes), las cuales representan el tráfico normal de la red. El ataque es simulado por una sesión de tráfico CBR. La frecuencia de operación es 2.4GHz como es sugerido para estas redes, el ancho máximo del canal inalámbrico es de 2Mbps y los parámetros de la capa física y MAC son los definidos en el estándar 802.11b en modo DCF que trae el software de simulación Qualnet por defecto. Los nodos son estáticos para mantener constante el ataque pues el ataque sobre un nodo estático es peor que sobre un nodo en movimiento y así descartar las pérdidas de paquetes por rompimiento del enlace. La sesión de ataque tiene el mismo tiempo de duración y es simultánea a las 8 sesiones de tráfico FTP. Si el ataque cesa el tráfico normal continúa y el desempeño de la red mejora. La tasa de ataque usada fue de 2Mbps, sin embargo desde tasas de ataque cercanas a 1Mbps se obtienen resultados similares. El protocolo de enrutamiento usado fue AODV. (Faloutsos 2002)

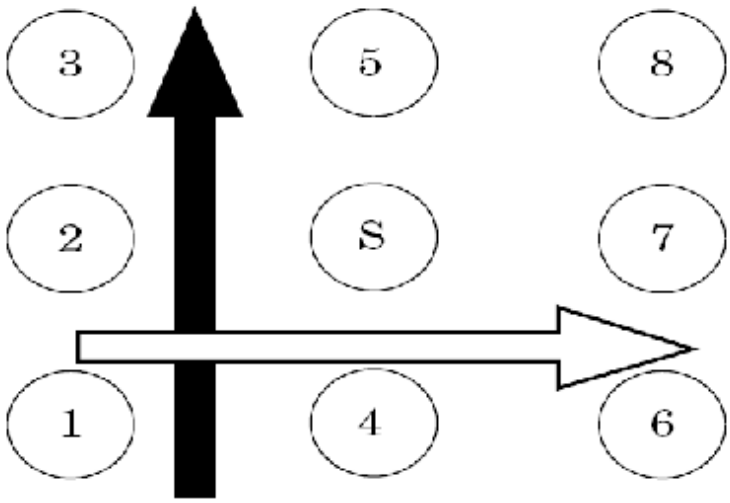


Figura: 3.1 Ataques de múltiple salto, partición de la red.(Faloutsos 2002)

Descripción de ataque

El ataque produce una gran pérdida de paquetes, de casi el 100%, ya que los nodos usan todos sus intentos de retransmisión sin lograr que los paquetes lleguen a su destino. El número de paquetes RTS y CTS en las redes con ataque es mayor que en la red sin ataque buscando lograr establecer la comunicación, sin éxito, por la presencia del ataque. Este, produce el efecto captura ya que al tener una tasa más alta y tener un solo salto de camino, gana siempre la contención y por lo tanto tiene la prioridad para transmitir mientras que los demás nodos retroceden y entran nuevamente a realizar sus respectivos Backoff. La figura 3.1 muestra con las flechas dos casos posibles de cómo el atacante podría buscar partir la red, por ejemplo lanzando un ataque desde un vecino de 1 hasta un vecino de 3 y suprimir los servicios de los nodos 1, 2 y 3. Los resultados en la tabla 3.1 muestran que aunque sí hay un descenso en el caudal de los 3 clientes en la partición (1, 2 y 3), los peores resultados los tiene el nodo 1, ya que el atacante está en su vecindad y la red se comporta como si el ataque estuviese a un salto del cliente, reduciendo su caudal y el número de paquetes entregados a cerca del 2%. El nodo 2 alcanza a entregar todos sus paquetes pero su caudal se ve disminuido a cerca del 30%. La relación de entrega de paquetes del nodo 3 es 1, su caudal disminuye a cerca del 45%. Los efectos sobre el nodo 3 son menores, ya que está más alejado de la fuente del ataque y por lo tanto la intensidad del ataque ha disminuido por el mayor número de saltos. Los resultados del ataque desde un vecino del nodo 1 hasta un vecino del nodo 6 presentan comportamientos similares ya que toda la información, es decir, todos los paquetes son entregados en forma satisfactoria, aunque hay una reducción del caudal.(Faloutsos 2002)

Tabla 3.1 Resultados de ataque de múltiple salto en una red de 169 nodos.(Faloutsos 2002)

	Con ataque		Sin ataque	
Cliente	Caudal (bps)	kbytes entregados	Caudal (bps)	kbytes entregados
1	158	13.3	6151	512
2	6722	512	19164	512
3	4892	512	12407	512
4	10275	512	13576	512
5	8117	512	8505	512
6	5728	512	6899	512
7	7921	512	11198	512
8	11770	512	10576	512

3.3 Métodos de defensa ante denegación de servicio

Ajuste en los límites de retransmisión

El límite de retransmisión corto es el número máximo de transmisiones configurado para una estación, esperadas para recibir un paquete CTS, es decir, el número máximo de veces que es posible retransmitir un paquete RTS. El límite de retransmisiones largo es el valor límite de transmisiones esperadas para que una estación reciba un paquete ACK, ó el número máximo de veces que una estación puede retransmitir un paquete de datos. El estándar de 802.11 define un valor al límite de retransmisión corto de 7intentos y al límite de retransmisión largo de 4 intentos. Tarjetas comerciales como las Cisco Aironet asignan un valor variable de 16 para los límites de retransmisión largo y corto, en un rango de 1 a 128; sin embargo, el estándar no define un número máximo para los límites de retransmisión para 802.11b. Para 802.11a el estándar define que el rango de los límites de retransmisión es de 1 a 255.(Sarmiento 2008)

Al aumentar los límites de retransmisión se reduce el número de paquetes perdidos debido a colisiones por congestión y por tanto al efecto captura, haciendo la capa MAC más insistente en buscar que el envío y recepción de los paquetes sea satisfactorio. No obstante, un aumento en estos valores podría no ser recomendable para la red ya que se

desperdiciarían recursos de ancho de banda y se estaría muy alejado de los valores comerciales para estos parámetros.

Para darle una mayor insistencia a la capa MAC al retransmitir los paquetes que se pierden debido a la presencia del ataque en la red, teniendo en cuenta el comportamiento de múltiple salto y así los paquetes puedan llegar a su destino y el rendimiento de la red mejore, se aumentaron los límites. Aunque aumentar los límites de retransmisión no muestra una tendencia clara en el aumento del caudal de la red, sí ayuda a aliviar el efecto del ataque. Con valores de los límites de transmisión por encima de 20, por ejemplo 23 y 18, 25 y 20, 20 y 25 (límite de retransmisión de paquetes cortos y límite de retransmisión de paquetes largos) el caudal total de la red en presencia del ataque DoS mejora desde un 10% hasta aproximadamente el 25%, tal y como se muestra en la figura 3.2, ya que más paquetes son entregados a su destino.(Munilla 2006)

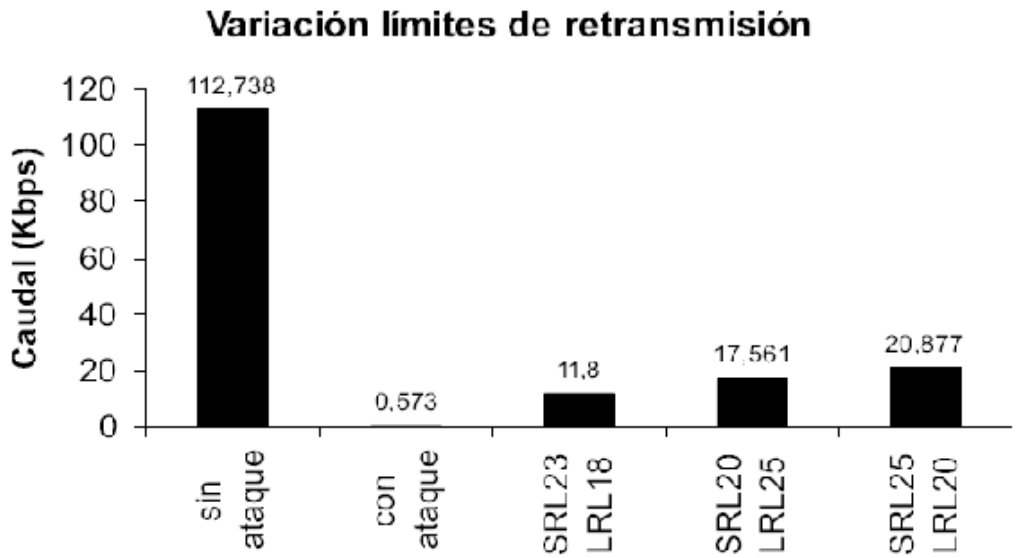


Figura: 3.2 Caudal total de la red ante DoS, ajustando límites de retransmisión (Sarmiento 2008)

Modificación del algoritmo de Backoff

El efecto captura hace que el ataque de degeneración de servicio, con menor número de saltos y mayor cantidad de tráfico, tenga privilegio sobre el acceso al medio ya que el retroceso del algoritmo de Backoff lo favorece, pues cuando reanuda su ventana de contención el tiempo de Backoff siempre es el menor, venciendo a los demás modos por el acceso al canal. Para evitar que el tiempo de Backoff del nodo atacante siempre fuera el

menor y siempre hubiese una gran diferencia con los tiempos de Backoff de los clientes, obligándolos a ceder el acceso al canal continuamente, se aumento el valor del límite mínimo de la ventana de contención para todos los escenarios de simulación, en busaca de hacer más equitativa la oportunidad de todos para transmitir. A partir de esto se encontró que el caudal y la relación de paquetes entregados aumentaban a medida que CWmin era mayor, sobre todo cuando la red tiene un mayor número de nodos y saltos para los tráficos normales. Un ejemplo de esto se muestra en la figura 3.3

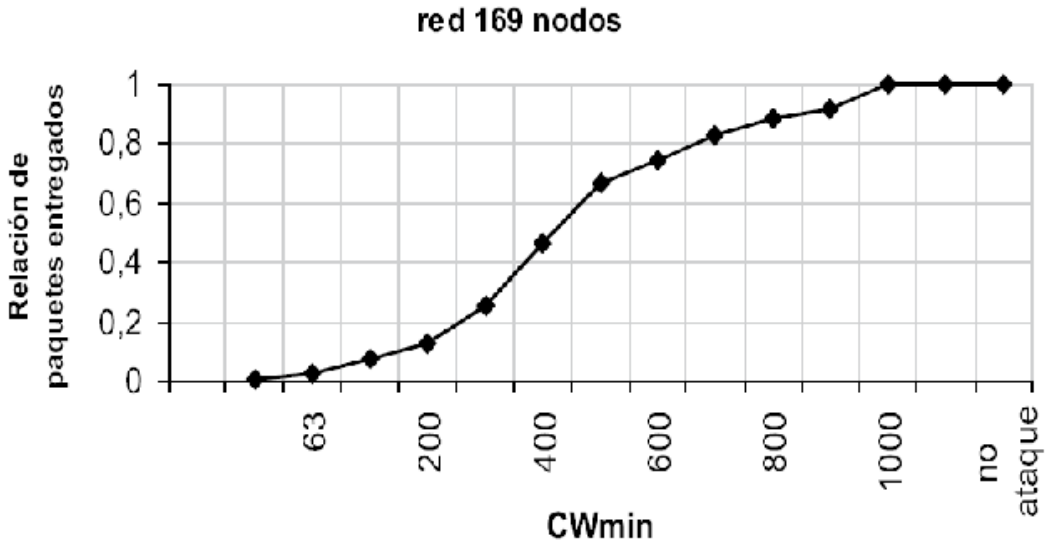


Figura: 3.3 Relación de paquetes entregados en red de 169 nodos bajo ataque aumentando CWmin (Sarmiento 2008)

La relación de entrega de paquetes en la red de 169 nodos, figura 3.3, va aumentando hasta alcanzar 1 (100%). El caudal en la red bajo ataque aumenta considerablemente y llega hasta por encima del 60%. Debido a este comportamiento más equitativo, el número de veces que transmite el nodo atacante disminuye y por tanto su tráfico, aumentando así el desempeño de los clientes. Este mismo comportamiento puede notarse en todos los tamaños de red y se muestra en la figura 3.4, para la red de 144 nodos. Teniendo en cuenta lo anteriormente descrito, se propone una modificación en el algoritmo que no es tan agresiva en la forma como retrocede y que fuese igual de suave para que no aumentara la injusticia e inequidad en las transmisiones de los clientes. También se buscó que fuera dinámica, similar a las mejoras para la red de 1 salto, de tal forma que no hubiese necesidad de dejar fijo CWmin.

Por esto se realizó la siguiente modificación en el algoritmo de Backoff de 8002.11 dejando los límites mínimo y máximo de la ventana de contención, tal y como los trae el estándar:

$$\begin{cases} CW \leftarrow \min(2 \cdot CW, CW_{max}) & después\ de\ colisión \\ CW \leftarrow \max(CW-1, CW_{min}) & después\ de\ transmisión \end{cases}$$

Cuando hay una colisión, al igual que en el esquema BEB, la ventana de contención se dobla hasta alcanzar su límite máximo (1.023). Después de una transmisión exitosa, en lugar de reanudar la ventana de contención a 31, escoge el máximo entre el valor mínimo de CW y el valor actual de la ventana de contención menos 1 time slot (en tiempo 20 µs). Esto hace que los tamaños de las ventanas de contención de todos los nodos, incluido el nodo de ataque, sean similares, entonces los clientes pueden tener la misma ó mayor oportunidad de transmitir ya que su tiempo de Backoff puede ser menor que el del atacante. Usando el algoritmo propuesto, en las redes de mayor tamaño, la mejora del caudal alcanza hasta el 60% y la relación de entrega de paquetes desde el 80% hasta 100% como se muestra en la figura 3.4(Sagarminaga 2005)

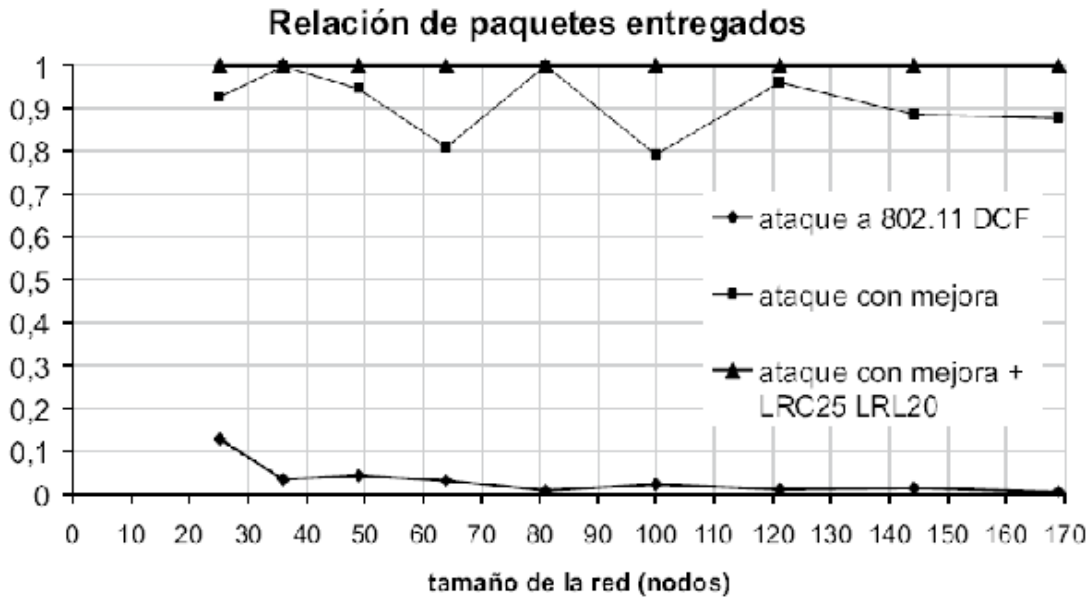


Figura: 3.4 Relación de paquetes de algoritmo mejorado para DoS(Sarmiento 2008)

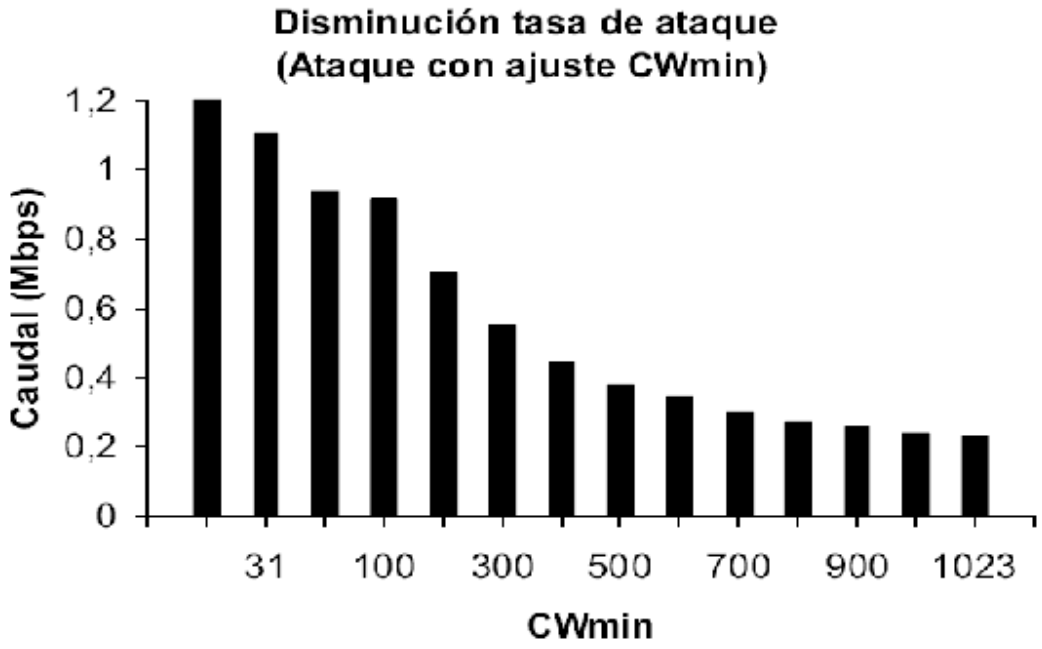


Figura: 3.5 Disminución tasa de ataque con ajuste de CWmin, 144 nodos.(Sarmiento 2008)

El grado de retroceso del algoritmo de Backoff (-1) fue escogido debido a que un mejor desempeño sobre otros también considerados bajos y lineales. En las gráficas a continuación 2CW-16 significa que se dobla la ventana de contención cuando hay colisión y se disminuye 16 linealmente cuando ocurre una transmisión exitosa, para cualquier tamaño de red. Como ejemplo la figura 3.4 muestra el comportamiento en una red de 144 nodos.(Tortosa 2005)

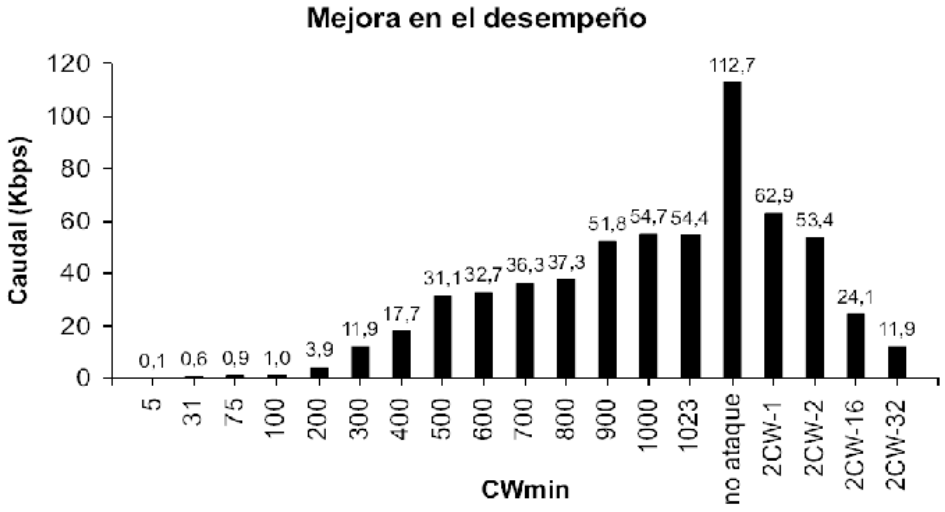


Figura: 3.6 Comparación del caudal entre mejoras al BEB en red de 144 nodos.(Sarmiento 2008)

Siendo esta mejora al algoritmo una medida de fortalecimiento de la capa MAC, es necesario observar el comportamiento de la red sin ataque. El caudal disminuye en redes pequeñas, debido a que mayores tiempos de Backoff en tráficos de pocos saltos llevan a una mayor demora en la entrega de los paquetes. Sin embargo, en redes de mayor tamaño con tráficos de más saltos, el algoritmo incluso mejora el caudal.

La relación de entrega de paquetes siempre permanece alta, tanto con el BEB como con el algoritmo propuesto, como se observa en la figura 3.5, luego no hay disminución en esta métrica y el algoritmo propuesto funciona correctamente.

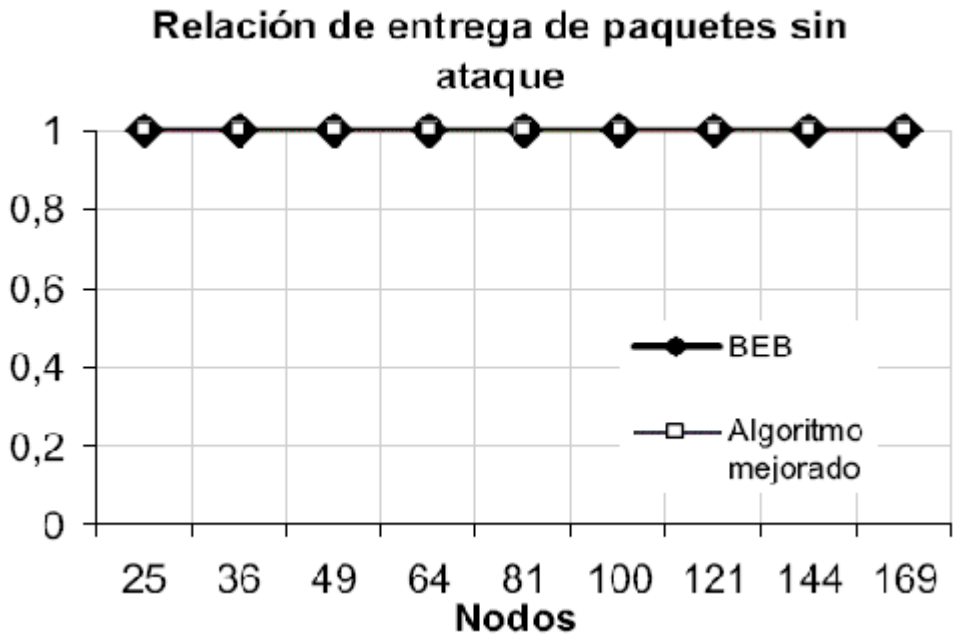


Figura: 3.7 Relación de entregas de paquetes BEB vs Algoritmo mejorado para DoS, sin ataque

Si adicionalmente, además de modificar el algoritmo de Backoff frente al ataque de denegación de servicio, se aumenta la insistencia de envío de un paquete en la capa de acceso al medio a unos valores más acordes con la red de múltiple salto, la mejora ante el ataque es evidente y se muestra en la figura 3.3. La relación de paquetes entregados crece al 100% para todas las redes y el caudal incluso sobrepasa el desempeño sin ataque en las redes de mayor número de nodos.(LUTHER 2003)

Eliminación de vecinos

El método de eliminación de vecino es usado para prevenir el ataque por inundación de paquetes RREQ. Las redes móviles Ad Hoc son redes inalámbricas múltiple salto, y los nodos mandan y reciben paquetes a través de sus nodos vecinos. Si todos los nodos vecinos alrededor de un nodo se rehúsan a retransmitir sus paquetes, el nodo no se podrá comunicar con los otros nodos en la red ad hoc, aislándose así de la red. La figura 3.8 muestra una topología de red ad hoc móvil. El nodo H se comunica con los otros nodos a través de los nodos D, F, G e I. Si los nodos vecinos D, F, G e I se negasen a recibir paquetes del nodo H, el nodo H no podrá enviar ningún paquete a los otros nodos. En AODV, los nodos colocan los paquetes RREQ de acuerdo a la regla "firstin, firstout" (FIFO). Con dicha regla, los excesivos paquetes RREQ del atacante harán que se sature la cola y los nodos no podrán recibir los paquetes RREQ posteriores. Se cambiara la cola FIFO por una cola de prioridad. Además se tendrá un umbral de paquetes que se podrán recibir por cada vecino. La prioridad de un nodo es inversamente proporcional a la frecuencia que origina RREQ. El umbral es el número máximo de paquetes RREQ que origina un nodo en un periodo determinado, tal como 1 seg. Si la frecuencia de originar RREQ del atacante excede el umbral, su vecino no recibirá más RREQ del atacante. Así como entre más paquetes RREQ mande menor será su prioridad en la cola. Para clarificar, tomamos el nodo F y sus vecinos A, C, H, G de la figura 3.8. El nodo F prepara el proceso de prioridad para sus vecinos A, C, H, y G. Los valores iníciales de las cuatro prioridades en el nodo F son 1's. Después del nodo A transmite dos paquetes RREQ en 1 segundo, la prioridad del nodo A cambia a 1/2. Si el nodo C origina 5 paquetes RREQ en 1 segundo, la prioridad del nodo C se cambia a 1/5. Después de esto, si el nodo A y C transmiten paquetes RREQ al mismo tiempo, el nodo F primero transmitirá el paquete RREQ del nodo A porque la prioridad de A es más alta que de C. Si el nodo H (intruso) transmite excesivamente paquetes RREQ en un período de tiempo, la prioridad de H será muy baja. Si la frecuencia excede el umbral, nodo F negará la retransmisión de los paquetes RREQ de H, esto es semejante, para el nodo D, I, G. Como resultado, será cancelado el ataque por inundación de RREQ por medio de los vecinos. (2008)

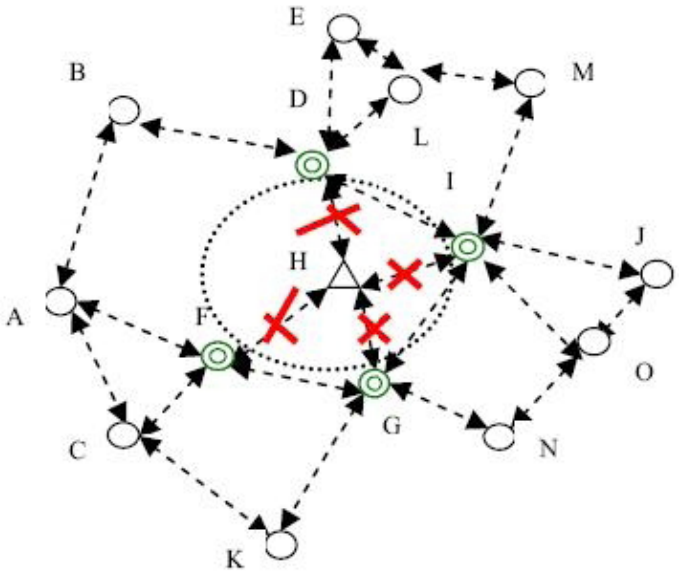


Figura 3.8 Corte de ataque por eliminación de vecino

Corte de ruta

Cuando el intruso origina un ataque de inundación de datos; para los nodos vecinos es difícil identificarlo, ya que no pueden juzgar que un paquete de datos sea inútil en la red. Pero el nodo destino puede fácilmente determinar en la capa de aplicación cuando recibe un paquete de datos inútil. Se presentará un método llamado "corte de ruta" para prevenir el ataque por inundación de paquetes de datos. Cuando un atacante origina dicho ataque, éste encuentra un camino hacia la víctima. Cuando la víctima se da cuenta que está siendo atacado, él puede cortar la ruta, originando un mensaje RRER dirigido al atacante. Los nodos intermedios por los que pasa el RRER borraran la ruta del atacante hacia la víctima. El mensaje RERR podría quitar algunas rutas, las cuales, no están relacionadas con el ataque, estas rutas pueden ser reparadas por los nodos en el futuro. Así las rutas se van cortando y el ataque es gradualmente terminado. Cuando el ataque es terminado, el atacante puede originar un nuevo RREQ, y el nodo victima puede rehusarse a responderlo, no contestando con el RREP. Pero ya que en el protocolo AODV los nodos intermedios pueden responder los RREQ si tienen rutas válidas aunque la víctima no quiera que la ruta se reactive. Para evitar esto, la función de que los nodos intermedios puedan contestar RREQ debe ser cancelada. Solamente el destino puede responder los RREQ.(Carlos Varela 2002)

3.4 Conclusiones

En esta investigación comprueba que la causa de la fragilidad de la red ante un ataque de denegación de servicio basado en tráfico es el efecto captura, que ocurre porque el algoritmo de Backoff de 802.11 favorece al nodo más activo de la red, es decir al último en ganar el derecho a transmitir entre los nodos que contienden por el acceso al canal. Poco se ha estudiado acerca de este fenómeno en las redes de múltiple salto y se ha buscado adaptar métodos de las redes tradicionales como mecanismo de defensa ante estos ataques tales como encriptación y autenticación, los cuales no son suficientes para mitigar el impacto del ataque sobre la red. Se mostró que los límites de retransmisión, tal y como vienen definidos en el estándar, no son adecuados para las redes de múltiple salto y menos ante una red bajo ataque. Ajustando los límites a valores por encima de 20, se aumenta la insistencia de la capa MAC en el envío de paquetes, lo que hace que se pierdan menos cuando hay un ataque, aumentando el caudal y la relación de paquetes entregados. Esta medida mejora el desempeño de la capa MAC ante la presencia del ataque pero no es considerada como definitiva. Una mejora adecuada del algoritmo de Backoff no solo aumenta el número de veces que pueden transmitir los nodos frente a un ataque de denegación de servicio, sino que puede servir como base para mejorar la calidad de servicio en la red. La mejora propuesta y realizada aumenta el rendimiento en la red hasta un 60% y la relación de paquetes entregados hasta el 95% frente a un ataque. Al aplicar el algoritmo a la red en condiciones normales el caudal en redes pequeñas es menor; sin embargo, la relación de entrega de paquetes permanece en 1. Si adicionalmente se realiza el ajuste de los límites de retransmisión a 25 y 20, el caudal aumenta considerablemente y se entrega el 100% de los paquetes enviados.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El objetivo propuesto en el presente trabajo se desarrolló plenamente arrojando los siguientes resultados:

- Las herramientas y protocolos de seguridad disponibles hasta el momento para un entorno inalámbrico, no han logrado por sí solos, garantizar de forma eficiente la protección en estas redes.
- Es posible detectar fácilmente estos tipos de ataques, pero es muy difícil de prevenir ya que pueden tener muchas procedencias.
- Mediante mecanismos adecuados y técnicas apropiados se puede lograr una configuración de seguridad más eficiente, disminuyendo considerablemente las deficiencias que caracterizan estas redes.
- Aunque no se pueda mitigar por completo los ataques en las redes inalámbricas, bien se puede lograr aliviar dichos ataques mediante técnicas de prevención y contramedidas.

Recomendaciones

Teniendo en cuenta que las redes inalámbricas constituyen el proceso de migración para las tecnologías futuras de las telecomunicaciones y presentan un sin número de beneficio que sobresalen de forma inequívoca frente a las desventajas, se recomienda que se tenga en cuenta los detalles fundamentales a la hora de configurar dichas redes con el método de seguridad más recomendado en función de las características de la red y estar atento a los

demás intentos efectuados por personas mal intencionada que atentan contra esta tecnología que solo trae beneficio siempre y cuando es utilizado para fines benéficos. Por todo eso se recomienda:

- ✓Filtrado de direcciones MAC.
- ✓Utilización de redes privadas virtuales (VPN).
- ✓Limitar la potencia de emisión de los AP.
- ✓Habilitar el AP en el modo pasivo.
- ✓Utilizar cifrado fuerte con el esquema WPA/WPA2.
- ✓ Instalar sistemas de detectores de intrusos.
- ✓Firewalls
- ✓Antivirus actualizados

Estas son algunas de las configuraciones que se puede emplear para prevenir de cierto modo los ataques en las redes inalámbricas y que por sí sólo ya se ha demostrado que presentan ciertas debilidades, pero se les combina podría ofrecer alguna robustez en la red. Sin embargo podemos advertir que ningún sistema es 100% seguro, pero las redes inalámbricas no tienen porque ser inseguras si se configura adecuadamente.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Fleites, A. R. (2007). Diseño de un red de Area Local Inalámbrica. Departamento de Electronica y Telecomunicaciones. Santa Clara, Universidad Central "Marta Abreu de las Villas".

Torres, J. C. (2006) Praticas de Laboratorio Utilizando OPNET. **Volume**, DOI:

(2008). "Introducción a Wi-Fi (802.11 o WiFi)." from http://es.kioskea.net/contents/wifi/wifiintro.php3.

Alvarez, G. V. (2004). Ataques de Denegación de Servicio en Redes Wireless. Seguridad en Redes Inalambricas. **2:** 123.

Carlos Varela, L. D. (2002). "Redes Inalámbricas." from http://www.blyx.com/public/wireless/redesInalambricas.pdf.

Faloutsos, M. (2002). Denial of Service Attacks at the MAC Layer in Wireless ad hoc Networks. National Science Foundation. M. Anaheim.

Fleites, A. R. (2007). Diseño de un red de Area Local Inalámbrica. Departamento de Electronica y Telecomunicaciones. Santa Clara, Universidad Central "Marta Abreu de las Villas".

Flores, J. L. G. (2009). Análisis y Diseño de una Red LAN Inalambricas para la Empresa Bio-Electronica Blancos S.A. Departamento de Telecomunicaciones. Quito, Escuela Politécnica Nacional.

García, J. G. O. (2003). Redes Wireles MESH Tecnologia 3G, .

González, E. F. (2007). "Wi-Fi: nuevos estándares en evolución." from http://www.ceditec.etsit.upm.es/dmdocuments/wifi.pdf.

González, R. M. C. (2007). Propuesta de Configuraciones de Seguridad para la Red Inalámbrica de la UCLV. Departamento de Electrónica y Comunicaciones, Universidad Central "Marta Abreu " de las Villas.

Gutierrez, J. D. (2006). Ataques en 802.11. **1:** 84.

Krishnamuthy, S. (2004). the performance of TCP in the presence of interacting UDP flows in ad hoc networks. National Science Foundation. M. Anaheim.

LUTHER, J. (2003). "El alfabeto 802.11." from http://www.mnlab.cs.depaul.edu/seminar/fall2003/802-11e.pdf.

Miquel Oliver, A. E. (1999). REDES DE ÁREA LOCAL INALÁMBRICAS SEGÚN EL ESTÁNDAR IEEE 802.11. Departamento de Matemática Aplicada i Telemática, Universidad Politécnica de Catalunya.

Molina, J. M. (2003). Seguridad en redes inalámbricas 802.11.

Munilla, J. (2006). Enlace Inalambrico Seguro para Redes de Sensores. Redes Inalambricas.

Othman, F. Z. (2007). Configuraciones de Seguridad para la Red Inalámbrica de la UCLV. Departamento de Electronica y Telecomunicaciones, Universidad Central "Marta Abreu" de las Villas.

Othman, F. Z. (2007). Redes Inalambricas de Multiples Saltos (Redes Ad-Hoc). Departamento de Electronica y Telecomunicaciones. Santa, Universidad Central "Marta Abreu" de las Villas.

Pellegrino, G. (2006). Security in Mobility. Mini Workshop on Security Framework. Catania.

Sagarminaga, P. G. (2005). Protección y Vulnerabilidades. Seguridad en Redes Inalambricas 802.11 a/b/g. **1:** 254.

Sarmiento, C. A. R. (2008). Desempeño de Redes de Multiple salto ante ataque de denegación de servicio en tráfico.

Torres, J. C. (2006) Praticas de Laboratorio Utilizando OPNET. **Volume**, DOI:

Tortosa, C. C. (2005). Seguridad en Redes Inalambricas.

Yáñez-Mingot, P. S. (2006). "Estrategias de configuración de redes WLAN IEEE 802.11e EDCA." from http://dialnet.unirioja.es/servlet/tesis?codigo=2193.

Yáñez-Mingot, P. S. (2006). ESTRATEGIAS DE CONFIGURACIÓN DE REDES WLAN IEEE 802.11e EDCA. MADRID, CARLOS III

Zubieta, A. A. (2006). "Ataque de Denegación de Servicio." Retrieved 13 Abril de 2009, 2009, from http://es.wikipedia.org/wiki/ataque_de_denegacion_de_servicio.

Mecanismo de seguridad vs ataques Leyenda: V-vulnerable, M-Mitigado

			ENLACE									RED	
			WEP	WAP				802.11i				IPsec VPN	
				LEAP	EAP-TLS	EAP-TLS	PEAP	LEAP	EAP-TLS	EAP-TLS	PEAP	Pre-Shared Keys	Certificados X509
Ataque	Pasivo	Escuchas/Eavesdropping/ sniffing/wardriving	M	M	M	M	M	M	M	M	M	M	M
		Ataques a contraseñas (por fuerza bruta, de diccionario, descifrado de claves)	V	V	V	V	V	M	M	M	M	M	M
	Activo	Puntos de acceso no autorizados/Rogue APs	V	M	M	M	M	M	M	M	M	V	V
		Hombre en el medio	V	M	M	M	M	M	M	M	M	M	M
		Secuestro de sesiones/Hijacking	V	M	M	M	M	M	M	M	M	M	M
		Spoofing	V	M	M	M	M	M	M	M	M	M	M
		Denegacion de servicio (DOS)/Jamming	V	V	V	V	V	V	V	V	V	V	V

Síntesis de EAP

EAP	Propietario	Autenticación del servidor	Autenticación del cliente	Generación de claves dinámicas	Seguridad de las credenciales	Re-autenticación rápida	Tunelado	Compatible con WPA	Riesgos no mitigados
MD5	No	No	No	No	No	No	No	No	Exposición de identidad Ataque de diccionario Hombre en el medio Secuestro de sesiones
LEAP	Si	Password hash	Password hash	Si	Débil	No	No	Si	Exposición de identidad Ataque de diccionario
TLS	No	X.509 certificate	X.509 certificate	Si	Fuerte	Si	No	Si	Exposición de identidad
TTLS	No	X.509 certificate	PAP, CHAP, MS-CHAPv2, any EAP	Si	Fuerte	Si	Si	Si	Ataque de diccionario
PEAP	No	X.509 certificate	Cualquier EAP	Si	Fuerte	Si	Si	Si	Ataque de diccionario
SIM	No	Pre shared key/ key derivation	Pre shared key/ key derivation	Si	Fuerte	Si	No	Si	No independencia de la sesión Ataques de 64 bits

802.1X-EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	None	Password Hash	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Password Hash	Public Key (Certificate or Smart Card)	CHAP, PAP, MS-CHAP(v2), EAP	Any EAP, like EAP-MS-CHAPv2 or Public Key
Dynamic Key Delivery	No	Yes	Yes	Yes	Yes
Security Risks	Identity exposed, Dictionary attack, Man-in-the-Middle (MitM) attack, Session hijacking	Identity exposed, Dictionary attack	Identity exposed	MitM attack	MitM attack; Identity hidden in Phase 2 but potential exposure in Phase 1

Glosario de Acrónimos

ACK	Acknowledgements (confirmaciones)
AP	Punto de Acceso
ARQ	Automatic repeat request
CCA	Clear Channel Assesment
CRC	Verificación de redundancia cíclica
CSMA/CA	Carrier sense multiple access with collision avoidance
CTS	Clear to send
DCF	Distributed Coordination Function
ECN	Notificación explicita de congestionamiento
FEC	Forward Error Correction
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineering
ISM	Industrial Scientific Medical band (2.4 GHz)
MAC	Media Access Control
MIMO	multiple-input multiple-output
MT	Terminales Móviles
MTU	Maximum Transfer Unit
NAV	Network Allocation Vector
PCF	Point Coordination Function
PCMCIA	Personal Compute Memory Card International Association
PLCP	Physical Layer Convergence Protocol

PMD	Physical Medium Dependent sublayer
QoS	Quality of Service
RTO	Round Trip Overtime
RTS	Request to send
RTT	Round Trip Time
SAP	Service Access Point
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TO	Time Out
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN

Glosario de Términos

CALIDAD DE SERVICIO: es la capacidad de cumplir con las restricciones temporales cuando se transmiten y se procesan flujos de datos multimedia en tiempo real. Las aplicaciones que transmiten datos multimedia requieren tener garantizados uno ancho de banda y unos límites de latencia en los canales que utiliza. Algunas aplicaciones varían sus demandas dinámicamente, y especifican tanto la calidad de servicios aceptable mínimo como la óptima deseada.

CSMA: acceso múltiple con sentido de portador. Cuando una estación tiene datos para mandar, primer examina si alguien está usando el canal. Espera hasta que el canal esté desocupado y entonces transmite un marco. Si hay un choque, espera un período aleatorio y trata otra vez.

CWm (congestion window): La ventana de congestión es una variable que limita la cantidad de datos que TCP puede enviar (en ningún momento TCP podrá enviar segmentos con un número de secuencia mayor que la suma del ACK con mayor número de secuencia recibido y el menor de los tamaños de las variables rwnd y cwnd). Su tamaño variará dependiendo de las condiciones de la red, si la red no descarta paquetes, el tamaño de la ventana aumentará, aumentando la velocidad de transmisión del receptor.

Decibel (dB): La unidad estándar utilizada para expresar ganancia o pérdida de energía.

Distancia de salto: El numero de saltos que tiene que tomar un paquete para viajar desde la fuente hacia su destino final. Un diámetro de red es el máximo número de saltos por los que tiene que pasar un paquete de un nodo a otro.

ICMP: Protocolo de mensaje de control Internet, permite que los ruteadores en una red de redes reporten los errores o informaciones de control hacia otros ruteadores.

IEEE: El Institute of Electrical and Electronics Engineers (IEEE) también conocido como i-e-cubo, es una organización profesional técnica sin ánimo de lucro que incluye a más de 377.000 persona en 150 países. El IEEE se ha convertido en una autoridad en varias áreas técnicas, desde ingeniería informática hasta ingeniería en telecomunicaciones, pasando por otras como ingeniería biomédica o ingeniería eléctrica.

A través de su extensa red de publicaciones, conferencias y actividades destinadas al desarrollo de estándares, el IEEE produce el 30% de las publicaciones en ingeniería eléctrica e informática. Actualmente lleva a cabo anualmente 300 conferencias con reconocido prestigio internacional, y patrocina el desarrollo de más de 900 estándares.

MAC: El término MAC (Media Access Control) se utiliza para referirse a la dirección física de un dispositivo de red. Esta dirección debe ser única para cada dispositivo de red y es asignado en el momento de su fabricación. Una dirección MAC esta formada por 6 bytes que se representan en formato hexadecimal de esta forma: 11:22:33:44:55:66. De esos 6 bytes los 3 primeros corresponden con el identificador del fabricante, y los 3 siguiente con el identificador único de cada dispositivo. El identificado del fabricante es asignado por el IEEE para asegurar su unicidad. Es responsabilidad del fabricante asegurarse la unicidad del identificador del dispositivo para evitar repeticiones.

Nodos expuestos: Una estación que cree que el canal está ocupado, pero en realidad está libre pues el nodo que le oye no le interferiría para transmitir a otro destino.

Nodos ocultos: Una estación que cree que el canal esta libre, pero en realidad está ocupado por otro nodo que no oye.

Producto ancho de banda retardo de propagación (BDP): Esto define la cantidad de datos que el protocolo puede tener "volando" en cada instante para la completa utilización de la capacidad del canal. El retardo usado en esta ecuación es el tiempo de ida y regreso de un paquete.

Protocolos: Los protocolos de comunicación son grupos de reglas que definen los procedimientos convenciones y métodos utilizados para transmitir datos entre dos o más dispositivos conectados a la red.

Protocolo de control de transporte (TCP): Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a otra en la Internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.

Razón de transmisión: Es el número máximo de bits de información que pueden ser transmitido en un enlace de transmisión por unidad de tiempo. Típicamente se expresa en megabit por segundo (Mbps).

Red de múltiple salto: Una red en la cual un paquete debe pasar por varios nodos antes de llegar a su destino final.

RMSS (Receiver Maximum Segment Size): Es el mayor tamaño de segmento que el receptor puede admitir. La cantidad máxima de datos que el receptor puede recibir.

RTO: Tiempo de espera de la confirmación de un paquete (ACK).

RTT: Tiempo que transcurre desde que el segmento ha sido enviado, hasta que se recibe la confirmación de que ha sido recibido por el receptor. El RTT determina la velocidad de transmisión de TCP, ya que el emisor TCP envía cada RTT el tamaño determinado por cwnd.

Ruido: El termino ruido representa una señal que no contiene información, formada por una mezcla aleatoria de longitudes de onda.

RWND (Receiver Window): es la cantidad máxima de datos que puede recibir un receptor de tráfico TCP.

Segmento: Se utiliza para designar cualquier paquete TCP, ya sea un paquete de datos o uno de reconocimiento (Ack).

Servicio orientado a conexión: Como el sistema telefónico. La conexión es como un tubo, y los mensajes llegan en el orden en que fueron mandados.

Servicio sin conexión: Como el sistema de correo. Cada mensaje trae la dirección completa del destino, y el ruteo de cada uno es independiente.

SMSS (Sender Maximum Segment Size): Es el mayor tamaño de un segmento que el emisor puede transmitir. La cantidad máxima de datos que el emisor puede enviar.

SSTHRESH: Esta variable se utiliza para determinar qué algoritmo de control de congestión se debe utilizar, partida lenta o la evasión de congestión.

Ventana: es el número de tramas que pueden estar pendiente de confirmar por el receptor.