SEGURIDAD EN REDES DE ÁREA LOCAL INALÁMBRICA, ESTÁNDAR DE SEGURIDAD IEEE 802.11I

ROBERTO ENRIQUE SEPÚLVEDA FRANCO

ANTONIO JOSE SIMANCAS GUARDO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

SEGURIDAD EN REDES DE ÁREA LOCAL INALÁMBRICA, ESTÁNDAR DE SEGURIDAD IEEE 802.11I

Autores

ROBERTO ENRIQUE SEPÚLVEDA FRANCO

ANTONIO JOSÉ SIMANCAS GUARDO

Monografía, presentada para optar al titulo de ingeniero de sistemas

Director

GIOVANNI VÁSQUEZ

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

Nota de Aceptación

Firma de presidente del Jurado

Firma del Jurado

Firma del Jurado

Cartagena, Noviembre de 2004.

Cartagena, D. T. y C., Noviembre de 2004.

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADOS.

Universidad Tecnológica de Bolívar.

La Ciudad.

Respectados Señores:

Con toda atención, nos dirigimos a ustedes, con el fin de presentarles a consideración, estudio y aprobación, la monografía titulada "**SEGURIDAD EN REDES DE ÁREA LOCAL INALÁMBRICA, ESTÁNDAR DE SEGURIDAD IEEE 802.11I**", como requisito parcial para optar el titulo de Ingeniero de Sistemas.

Atentamente,

Antonio José Simancas Guardo

Roberto Enrique Sepúlveda Franco

Cartagena, D. T. y C., Noviembre de 2004.

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS DE GRADOS.

Universidad Tecnológica de Bolívar.

La Ciudad.

Cordial Saludo

A través de la presente me permito entregarle la monografía titulada "**SEGURIDAD EN REDES DE ÁREA LOCAL INALÁMBRICA, ESTÁNDAR DE SEGURIDAD IEEE 802.11I**", para su estudio y evaluación, la cual fue realizada por los estudiantes Antonio Jose Simancas Guardo y Roberto Enrique Sepúlveda Franco del cual acepto ser su director.

Atentamente,

Ing. Giovanni Vásquez

AUTORIZACIÓN

Cartagena, D. T. y C., Noviembre de 2004.

Yo, **Antonio Jose Simancas Guardo**, identificado con el número de cedula 9'296.113 de Turbaco, autorizo a la Universidad Tecnológica de Bolívar para ser uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

Antonio José Simancas Guardo.

AUTORIZACIÓN

Cartagena, D. T. y C., Noviembre de 2004.

Yo, **Roberto Enrique Sepúlveda Franco**, identificado con el número de cedula **73'199.057** de Cartagena, autorizo a la Universidad Tecnológica de Bolívar para ser uso de mi trabajo de monografía y publicarlo en el Catalogo Online de la biblioteca.

Roberto Enrique Sepúlveda Franco

DEDICATORIAS

Este trabajo es parte de mi vida y comienzo de otras etapas por esto y mas se lo dedico con todo mi amor, cariño…

A DIOS, ya que si Él no hay nada.

A Beni, mi abuela, por estar conmigo desde niño y contribuir en mi crecimiento social y espiritual.

A mis padres Roberto Sepúlveda y Matilde Franco, por siempre estar a mi lado, por instruirme, aconsejarme, impartirme valores, conducirme correctamente y hacer de mi una persona integral.

A mi hermano, Carlos Alberto porque a tu manera me enseñas otros puntos de vista.

A Jenisffer, mi amor, porque tu amor y tu estimulo han sido fuente de inspiración y apoyo y porque desde que estoy contigo todo ha sido mejor, TE TODO.

A todas las personas que siempre han estado a mi lado, mis amigos, mis compañeros y profesores de la U, mis familiares y todas aquellas personas que siempre se preocupan por mí y me apoyan.

Roberto Enrique Sepúlveda Franco

Esta Monografía la dedico con todo mi amor y cariño a ti **Dios Padre**, Todopoderoso, por haberme ofrecido toda una vida llena de aventuras y experiencias dentro de este mundo universitario.

A mis Padres **Antonio José e Idalides del Carmen** por darme las ganas, la fuerza y las costumbres necesarias por guiarme en la carrera para mi futuro.

A mi hijo **Santiago de Jesús Simancas Hernández** por ser la luz de mi sendero y motivarme cada día más a salir adelante.

A mi Señora **Katherine Hernández Gonzalez** por brindarme su amor incondicional, por soportarme y aconsejarme de la mejor manera posible.

A mis Hermanas **Idalides del Carmen e Inés Elena** por guiarme y colaborarme en toda mi carrera, gracias por trasmitirme todos sus conocimientos y experiencia en esta nueva aventura.

A mis Profesores por regalarme toda su sabiduría, por ayudarme en la formación integral del profesional del mañana.

A mi equipo del Alma **River Plate CA.** (Tetracampeon del CIF), por brindarme las mas

gratas alegrías en mi formación tanto cultural como deportivo.

A mis compañeros de facultad, **Dago, Javier, Leo, Jairo, Bray, Pacho, Narlinda y en especial a Juan Ospina (QEPD),** por ayudarme de una u otra manera a la consecución de todos mi logros.

Antonio José Simancas Guardo.

AGRADECIMIENTOS

Queremos mostrar nuestro agradecimiento a las muchas personas que han contribuido al desarrollo de este trabajo de grado.

En primer lugar a todas las personas que han colaborado con la realización de este trabajo, muy especialmente a los ingenieros Giovanni Vásquez e Isaac Zúñiga, los cuales nos han sabido guiar y asesorar, también al ingeniero Giovanni Magallanes por prestarnos su ayuda eficaz.

También queremos agradecer a la Universidad Tecnológica de Bolívar por brindarnos la oportunidad de poder presentar este trabajo para optar por nuestro titulo de Ingenieros de Sistemas.

Y por ultimo, pero no por menos importantes, gracias a todas las personas que han confiado en nosotros y nos han apoyado a lo largo de la consecución de todos nuestros logros y han ayudado en la elaboración de esta monografía.

Esperamos no haber olvidado a nadie. Y asumimos toda la responsabilidad de cualquier tipo de errores que pudieran figurar en este trabajo. También esperamos que sea lo más provechoso para todos los interesados. Cualquier sugerencia, comentario, idea o corrección será bien recibido.

CONTENIDO

LISTAS ESPECIALES

Lista de Figuras.

Lista de Tablas.

RESUMEN

La acogida de la nueva tecnología de comunicaciones basada en redes inalámbricas ha proporcionado nuevas expectativas en cuanto al futuro del desarrollo de sistemas de comunicación.

Una red de área local inalámbrica (WLAN, wireless local area network), es un sistema de comunicaciones de datos si cables equivalente a las redes de área local cableadas, puede servir como alternativa o parte de estas. Estas redes poseen ciertas ventajas relevantes como son: la flexibilidad, movilidad, mejor escalabilidad, facilidad de instalación y menor costo.

Para el funcionamiento de estas redes se utilizan ondas de radio o infrarrojos los cuales so usados para el trasporte de los datos sin necesidad de un medio guiado.

Estas redes poseen dos topologías conocidas: **topología de infraestructura** o también llamada administrada, es aquella que hace parte de una red LAN cableada y **la topología en Ad Hoc** que es aquella en la cual solo existen dispositivos inalámbricos, es decir, todos los dispositivos se comunican entre si sin necesidad de un controlador central.

Los **estándares inalámbricos** mas conocidos son: **bluetooth, Home RF, HiperLAN2** y los estándares **802.11: 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, 802.11h, 802.11i** entre otros.

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema mas grave de este tipo de redes, ya que aquí es donde se encuentra su mayor vulnerabilidad debido a que cualquier persona puede acceder a una red insegura solo ubicándose en el rango de cobertura de esta con un equipo inalámbrico, Esto hace que este tipo de redes este expuesto a muchos riesgos. Los riesgos mas comunes a los que esta sometidas las redes inalámbricas de hoy son: el monitoreo de trafico inalámbrico, el acceso no autorizado o la corrupción de servicios inalámbricos.

Además Existen muchos tipos de ataques y amenazas a una red inalámbrica, estos tienen en común un solo objetivo, acceder de manera no autorizada a estas redes ya sea para tomar los servicios que presten estas o con fines mas malignos como sabotear la red o aprovecharse de la información que por esta se transmite y/o corromper esta. Los ataques y amenazas más conocidos son: el Netstumbler y amigos, el Wardriving, el Warchalking, el Sniffing/Ethereal/Airopeek, el Hacking, y la Intrusión.

Así como existen vulnerabilidades, ataques y amenazas, las organizaciones competentes con el tema de redes y seguridad se han tomado el trabajo de desarrollar un grupo de métodos y técnicas de seguridad para hacer más robustas este tipo de redes. Los métodos de seguridad se basan en tres principios fundamentales, la **autenticación**, que busca evitar el uso de la red por personas no autorizadas, la **privacidad**, que consiste en encriptar la información para evitar

la captura y posterior corrupción de esta, y la **integridad**, que pretende que los datos no sean manipulados por agentes externos preservando así su confiabilidad.

Los métodos básicos de seguridad son: las **medidas de seguridad física**, estas medidas son solo para proteger físicamente a las WLANs, es decir, son el conjunto de condiciones del contexto para hacer físicamente segura la red. Otros métodos de seguridad lógicos utilizados son: el **WEP** (*Wired Equivalent Privacy*, privacidad equivalente al cable), que fue el primer método utilizado para la seguridad de estas redes, por tener sus deficiencias a partir de este método se crearon algunos otros avanzados. Además hay otros métodos de seguridad básicos lógicos como lo son: **NOMBRE DE LA RED INALAMBRICA** (SSID, ESSID, IBSSID)**, FILTRADO DE DIRECCIONES MAC** y los **SISTEMAS ADICIONALES DE SEGURIDAD (FIREWALLS, VPN** (Virtual Private Network) **y DMZ** (Demilitarized Zone)**).**

Para reforzar los métodos básicos de seguridad las organizaciones encargadas han creado unos métodos más eficientes, algunos de los cuales son basados en los métodos rudimentarios, estos son llamados métodos avanzados de seguridad, estos métodos son: el **Protocolo de integridad de clave temporal (TKIP, Temporal Key Integrity Protocol),** el **CCMP (Counter-Mode/CBC-MAC Protocol)**, Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado, este protocolo es complentario al TKIP, otro método es el **Protocolo de autenticación extensible (EAP,**

Extensible Authentication Protocol), este método posee muchas variantes según el algoritmo usado para el cifrado, ahora la variante de EAP mas utilizada es **EAPOL**, EAP over LAN, Además existe el **AES (Advanced Encryption Standard)**, que es un algoritmo de cifrado fuerte y el **MIC (Message Integrity Code)** o algoritmo de Michael, que verifica la integridad de los datos de las tramas.

De la integración de algunos de los mejores métodos de seguridad avanzados nace el **WPA** (*Wi-Fi Protected Access*, acceso protegido Wi-Fi), este método es la respuesta a la seguridad que demandan los usuarios y que WEP no puede proporcionar, pretende solucionar todas las debilidades conocidas de WEP, este método se considera suficientemente seguro. WPA integra el control de acceso a redes que brinda el **Estándar IEEE 802.1x,** este estándar es basado en puertos, es decir, los puertos de los Puntos de Acceso se mantendrá cerrado para las estaciones hasta que estas se autentiquen**,** el protocolo de autenticación extensible EAP, que es utilizado para llevar a cabo las tareas de autentificación, autorización y contabilidad, el TKIP que se encarga de la generación de claves para cada trama y el MIC que es usado para verificar la integridad de los datos transmitidos. WPA se considera un subconjunto del nuevo método de seguridad, el **ESTANDAR IEEE 802.11i**.

El **ESTÁNDAR IEEE 802.11i** es el nuevo método de seguridad desarrollado por el task group i (TGi) de IEEE, es el estándar mas efectivo y hasta el momento el mas

seguro, es desarrollado básicamente con el propósito de cubrir todos los agujeros de seguridad de las redes inalámbricas. Este estándar toma como base de su funcionamiento al WPA pero añade algunas mejoras que lo hacen mas eficiente, estas mejoras son: **mejoras en la autenticación**, el IEEE 802.11i utiliza el estándar IEEE 802.1x junto con servidor de autenticación y el protocolo EAP para proveer los servicios de de autenticación y manejo de claves. Otra mejora que plantea este estándar esta en el manejo y establecimiento de claves, IEEE 802.11i utiliza un handshake en cuatro vías para proveer la mejora al servicio de establecimiento de claves temporales para la transmisión de tramas. Además este estándar hace una mejora en la encriptación, esto con el fin de optimizar la confidencialidad, esta mejora es lograda con la implementación de dos algoritmos criptográficos avanzados, Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (CCMP, Counter-Mode/CBC-MAC Protocol) y el Protocolo de integridad de clave temporal (TKIP, Temporal Key Integrity Protocol).

La seguridad de una red local inalámbrica en general esta dada básicamente por la implementación de un buen método lógico de seguridad, como lo es el WPA o el nuevo estándar IEEE 802.11i, los cuales son los mas utilizados y los mas efectivos actualmente. Además se debe tener presente la seguridad del contexto, es decir, contar con un buen método físico de seguridad y establecer unas buenas políticas de seguridad.

1. INTRODUCCIÓN

Cuando nos referimos a la *tecnología inalámbrica* nos damos cuenta que este termino hace referencia a una amplia gama de dispositivos, desde teléfonos móviles, PDAs hasta redes locales inalámbricas. Los dispositivos más simples como lo son los teléfonos móviles celulares, los beepers o buscas, han estado presentes desde hace mucho tiempo. Aunque la comunicación entre teléfonos móviles todavía no es la más óptima, ahora estos dispositivos tienen muchas más funciones y mejores características.

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos.

Las redes inalámbricas, tales como las del estándar IEEE 802.11, son un nuevo territorio para los desarrolladores. Como en todos los nuevos territorios, hay características únicas en el contexto que deben tomarse en cuenta. Las redes inalámbricas no tienen fronteras físicas, lo cual enfrenta a los expertos en seguridad a nuevos retos que resolver.

No esperamos que el usuario común y corriente evalúe los riesgos de seguridad de sus aparatos inalámbricos, ni mucho menos de todo el conjunto de estos que representan una WLAN. Por lo tanto las organizaciones encargadas de los estándares de seguridad deben balancear la conveniencia de los elementos y de las aplicaciones inalámbricas contra los riesgos de seguridad y decidir si los beneficios son al menos apropiados para el medio de transmisión.

Las redes inalámbricas son inseguras, aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes es la optimización de las características de seguridad tales como: la autenticidad y la privacidad de los usuarios así como la integridad de los mensajes que son transmitidos por la red.

Las organizaciones competentes al tema de las redes y de la seguridad de estas, en conjunto con las diferentes empresas creadoras de dispositivos y desarrolladoras de aplicaciones, han trabajado arduamente en la realización de una serie de métodos para tratar de proporcionar la mejor seguridad posible a las WLANs, estos métodos han ido evolucionando a medida que se han presentado nuevas necesidades de seguridad, desde el dominado WEP hasta el nuevo estándar de seguridad IEEE 802.11i que incluye las técnicas mas avanzadas y reúne los mejores protocolos y estándares para la resolución del problema de la seguridad en las redes inalámbricas.

El estándar IEEE 802.11i hasta el momento es el mecanismo de seguridad mejor dotado ya que combina las técnicas de autenticación del estándar IEEE 802.1x con un mejoramiento de en el manejo y establecimiento de claves, utilizando un handshake en cuatro vías. Además de los métodos de mejora de integridad de mensajes mediante algoritmos de encriptación lo suficientemente robustos para que los mensajes sean lo mas confiable posibles.

2. OBJETIVOS

2.1 Objetivo general

Dar a conocer una visión general del estado actual de la seguridad en las redes de área local inalámbricas, desde los riesgos y vulnerabilidades existentes en el diseño e implementación de estas redes, hasta los métodos y técnicas propuestas para subsanar dichas fallas pasando por consideraciones recomendadas en cuanto al diseño de las WLANs y terminando con las especificaciones del estándar mas efectivo que existe actualmente, el estándar IEEE 802.11i.

2.2 Objetivos específicos

- Describir las generalidades de las redes de área local inalámbrica, tales como su concepto, sus principales características, ventajas y desventajas, sus topologías y los estándares inalámbricos mas utilizados hoy en día.
- Exponer y analizar las principales vulnerabilidades, riegos y ataques de seguridad mas comunes presentes en las redes de área local inalámbrica, sus principales características y de que manera afectan a estas redes.

- Estudiar los métodos de seguridad de las WLANs tanto los métodos básicos como los avanzados utilizados para proteger estas redes.
- Conocer y analizar el nuevo estándar IEEE 802.11i, encargado de la seguridad en WLANs y poder hacer comparaciones con otros métodos avanzados ya existentes.
- Desarrollar la capacidad de hacer determinaciones y recomendaciones relacionadas con el establecimiento de políticas de seguridad en una infraestructura de redes inalámbricas.

2.3 Justificación

La motivación a realizar esta investigación esta originada en el incremento uso de la tecnología inalámbrica en nuestra ciudad y el país. Y en el hecho de que muchos usuarios desconocen los riesgos que tiene en utilizarla y que se han vuelto tan comunes para cierto grupos de personas. A diarios somos testigo de la utilización de esta novedosa tecnología WLANS para el beneficios de muchas empresa. Como sabemos, la seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

3. GENERALIDADES DE LAS REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)

3.1 Descripción general de las redes inalámbricas de área local

Las redes de área local inalámbrica representan un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.

Las redes LAN inalámbricas ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el

usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años.

3.2 Tecnologías de las WLANs

Según el uso que se le vaya a dar a la red se pueden aplicar distintas tecnologías:

3.2.1 Banda estrecha

Se transmite y recibe la información en una banda de frecuencia lo más estrecha posible. Los usuarios tienen distintas frecuencias de comunicación entre ellos de modo que se evitan las interferencias entre los mismos. Así mismo en el receptor

de radio un filtro se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada de modo que no se producen interferencias.

3.2.2 Banda ancha

Es la que se usa principalmente en los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor debe conocer los parámetros de la señal que se ha difundido. En caso de no estar en la frecuencia correcta el receptor, la señal aparece como ruido de fondo. Hay dos tipos de tecnología en banda ancha:

- Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.
- Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

3.2.3 Infrarrojos

No es una técnica muy usada. Se usan frecuencias muy altas para el transporte de datos. Como la luz, los infrarrojos no pueden traspasar objetos opacos. Por lo que o bien se utiliza una comunicación con línea de visión directa o bien es una difusión.

Los sistemas directos baratos se utilizan en redes personales de área reducida y ocasionalmente en LANs específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales.

3.3 Funcionamiento de las WLANs

Se utilizan tanto ondas de radio como infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponer a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver)

conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena. La naturaleza de la conexión sin cable es transparente a la capa del cliente.[1]

3.4 Topologías de WLANs

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc". En este documento se utilizarán los términos “infraestructura” y “ad hoc”. Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

3.4.1 Topología de infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base,

[1] Universidad Politécnica de Madrid, Redes sin cables. Articulo. 2002

denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

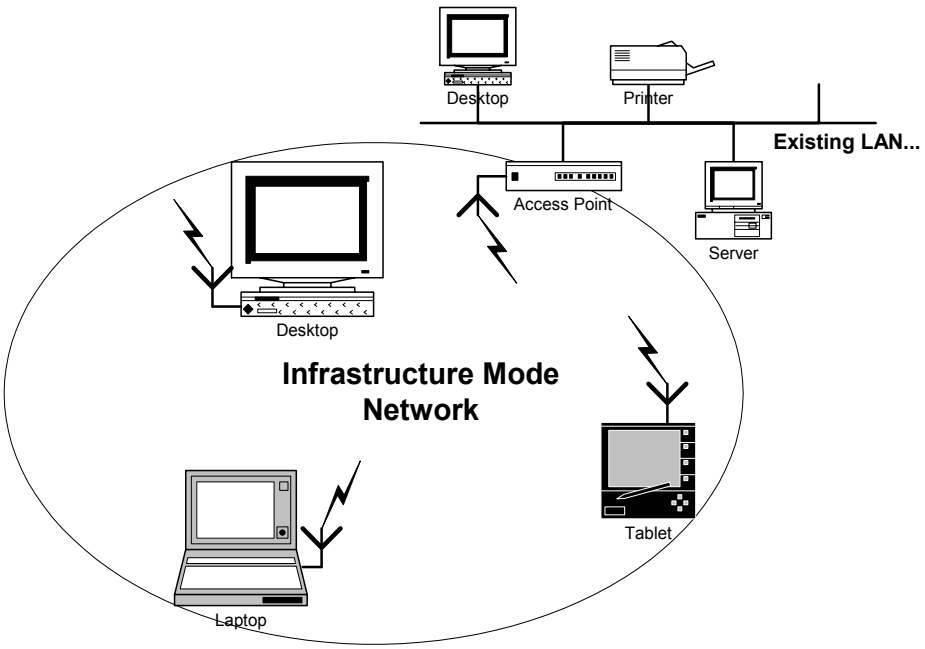

Figura 1. Red de la modalidad de infraestructura

3.4.2 Descripción general del funcionamiento de la modalidad de infraestructura

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes

disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la

modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

3.4.3 Topología Ad Hoc

En una topología ad hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

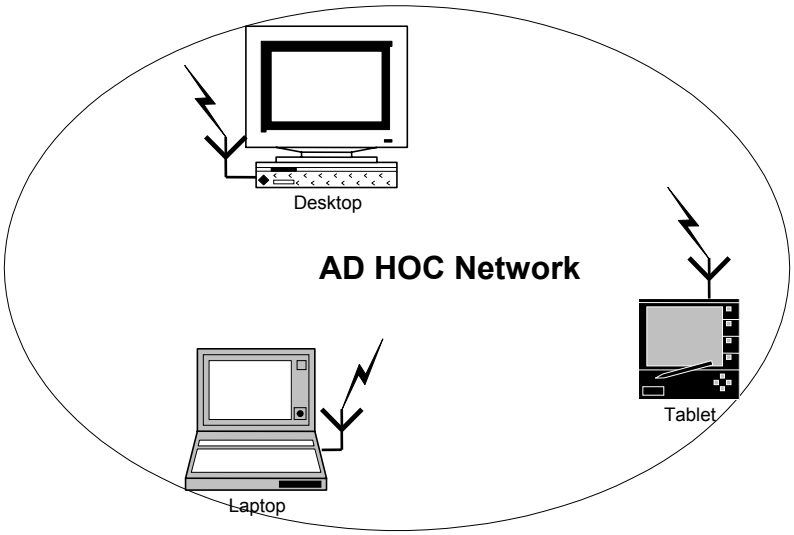

Figura 2. Red de la modalidad ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo,

transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

3.4.4 Descripción general del funcionamiento de la modalidad ad hoc

Después de explicar el funcionamiento básico de la modalidad de infraestructura, del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.[2]

3.5 Estándares inalámbricos

Los grupos de trabajo de la IEEE han estado trabajando en los nuevos estándares que deben cubrir las necesidades de este tipo de redes, sacando a la luz numeras especificaciones dentro del marco del 802.11. Existen diferentes planes que luchan entre si en algunos ámbitos, sobre todo para el mercado de casa, donde encontramos estándares como Bluetooth, HomeRF y 802.11.

3.5.1 Bluetooth

Es una especificación de la industria que describe la forma en la que teléfonos móviles, ordenadores, PDA entre otros dispositivos pueden conectarse entre sí o

[2] Microsoft, Tecnologías para Redes LAN Inalámbricas y Windows XP. Febrero 2002

con cualquier otro tipo de aparato utilizando emisiones inalámbricas de corto alcance. Su desarrollo comenzó hace unos siete años de la mano de Ericsson para conectar por radio los móviles con diferentes accesorios. Los emisores y receptores integran un chip con dicha función que les permite comunicarse en la banda de frecuencias de 2.4 Ghz y más concretamente entre 2,402 y 2,480 GHz, que es una banda que se puede usar libremente. Debido a que esta banda, la banda ISM, está abierta a cualquiera, el sistema de radio Bluetooth está preparado para evitar las múltiples interferencias que se pueden producir. En los sistemas de radio Bluetooth se suele utilizar el método de salto de frecuencia debido a que ésta tecnología puede ser integrada en equipos de baja potencia y bajo coste. Éste sistema divide la banda de frecuencia en varios canales de salto, donde, los emisores, durante la conexión van cambiando de uno a otro canal de salto de manera pseudo-aleatoria.

Bluetooth está capacitado para realizar transmisiones tanto de voz como de datos a través de múltiples sistemas operativos y es también válido para la creación de redes inalámbricas, aunque se ha visto superado por otros estándares. Cada uno de los dispositivos que usan esta tecnología posee una dirección única de 48 bits que lo identifica de manera inequívoca siguiendo el estándar IEEE 802. Las conexiones pueden ser punto a punto o multipunto y el alcance máximo es de unos 10 metros pero se puede llegar a los 100 metros empleando amplificadores o repetidores de la señal. Las transmisiones de datos podrán alcanzar tasas de hasta 721 Kbps en upstream y 56Kbps en downstream (en la segunda generación de dicha tecnología). Para asegurar la protección de la información se ha definido

un nivel básico de encriptación, que se ha incluido en el diseño del clip de radio para proveer de seguridad en equipos que carezcan de capacidad de procesamiento. Dos de los puntos importantes de esta tecnología es el bajo consumo de energía lo cual le otorga una gran movilidad y el bajo coste. Por el desarrollo visto hasta ahora se puede prever que el campo de aplicación del Bluetooth estará circunscrito a la comunicación de móviles, PDAs, portátiles y PCs con diversos accesorios y periféricos: manos libres, auriculares, micrófonos, ratón, impresora, teclado, etc.

3.5.2 HomeRF

Las redes de este tipo están diseñadas principalmente para su uso en ambientes domésticos. La base de estas redes es el protocolo de acceso compartido *(Shared Wireless* Access *Protocol,* Protocolo de Acceso Inalámbrico Compartido), que define las características para que la red inalámbrica sea capaz de soportar tanto tráfico de voz como de datos, siendo a su vez capaz de integrarse tanto con las redes de telefonía como con Internet. Esta tecnología es administrada por el grupo HRFWG *(HomeRF Working Group,* Grupo de Trabajo de Radiofrecuencias Domésticas), que engloba diferentes fabricantes y regula las características de la norma para evitar incompatibilidades en los elementos que se fabriquen y asegurar así la interoperatividad entre ellos. Este tipo de redes operará bajo la frecuencia de 2,4 GHz con transmisión por FHSS, y para las labores de seguridad contará con un identificador de red de 24-bits, encriptación de datos de 128-bits, y otras características adicionales de seguridad. Recientemente, el grupo HRFWG

ha anunciado que está trabajando para aumentar la zona del espectro electromagnético hasta los 5 GHz, pero esto está aún por llegar y en algunos paises como España el uso de dicha banda todavía no está regulado por la administración.

HomeRF se encarga de cubrir las necesidades los usuarios domésticos, que podrán establecer una comunicación sin cables entre los diferentes dispositivos que incorporen este estándar, y dispositivos como un teléfono móvil, un ordenador personal o cualquier otro elemento electrónico del hogar que sea susceptible de comunicarse con otro que esté integrado en un red local personal (WPAN), permitiendo entre otras muchas cosas jugar en modo multijugador, control remoto de equipos, compartir impresoras, centralita de llamadas, etc. . El gran inconveniente de este tipo de topología es que no puede integrarse con otras soluciones de redes inalámbricas. No obstante, su sencillez de uso y manejo la convierten en una solución ideal para uso doméstico o pequeñas oficinas.

Actualmente se han conseguido conexiones de hasta 10Mbps para distancias de 45 m con la versión 2.0 y afirman que para la futura revisión 3.0 permitirá una velocidad de 40Mbps además de una completa compatibilidad con la tecnología actual. En la actualidad el máximo número de dispositivos que se pueden conectar es de 127.

3.5.3 HiperLAN2

Esta tecnología se está desarrollando de mano de la ETSI una alianza de fabricantes del mercado de las telecomunicaciones, muchos de los cuales también

participan en las alianzas de los estándares vistos anteriormente. Sus principales características son: una alta velocidad de transmisión, es orientado a la conexión, permite administrar la calidad del servicio (QoS, Quality-of-Service), permite conexiones seguras y el ahorro de energía, muy importante para facilitar la movilidad. A primera vista destaca su alta velocidad, 54 Mbps, debida a la modulación que emplea: OFDM (Orthogonal Frequency Digital Multiplexing) Multiplexación Digital de Portadoras Ortogonales que es bastante eficiente en ambientes dispersivos como oficinas donde las señales provienen de diferentes reflexiones, con lo que se tienen diferentes tiempos de propagación.

En estas redes los datos se transmiten entre los terminales móviles (MT) y los puntos de acceso (AP) que previamente han realizado un establecimiento de la conexión empleando las capacidades de señalización de la capa de control. Nos podremos encontrar con dos tipos de conexiones: punto a punto y punto a multipunto, la primera es bidireccional, mientras que la segunda es unidireccional. En cuanto a la frecuencia de emisión de los diferentes canales, HiperLAN2 lleva incluido en los puntos de acceso un selector automático de frecuencia, que elige el canal más adecuado para la transmisión. Como se ha mencionado, HiperLAN2 permite la administración del QoS, lo cual nos otorga la capacidad de asignar diferentes características a cada conexión en lo referente al ancho de banda, el jitter, la tasa de error, etc. También nos permite trabajar de un modo más sencillo asignando simplemente a cada conexión diferentes niveles de prioridad. Todo esto nos permite tener diferentes canales de transmisión adaptados al tipo de datos que se van a transmitir por ellos: video, voz, datos.

En cuestiones de seguridad este protocolo permite el cifrado de datos y la autenticación, esta última se realiza entre el terminal móvil y el punto de acceso. En cuanto a la movilidad la forma de actuar es la siguiente: La terminal detecta de que punto de acceso, en caso de que existan varios, recibe una señal con mejor relación señal-ruido y se conecta con ese punto, en caso de que desplacemos la terminal se volverá a realizar dicha comprobación y se conectará con punto de acceso que presente una mayor calidad de transmisión. El ahorro de energía se basa en el establecimiento por parte del terminal de periodos de inactividad, de modo que le indica al punto de acceso que se se apague durante un cierto tiempo al final del cual le vuelve a indicar si debe seguir inactivo o no.

A pesar de las excelentes características que presenta este estándar su impacto comercial ha sido muy escaso y se ha visto ampliamente superado por Wi-Fi. Una de las posibles causas es la falta de regulación, en algunos países, del uso de la banda de frecuencias en torno a los 5 GHz.

3.5.4 Estándar IEEE 802.11

El Comité de estándares IEEE 802 formó el Grupo de Trabajo de estándares de Redes LAN inalámbricas 802.11 en 1990. El Grupo de trabajo 802.11 asumió la tarea de desarrollar una norma global para equipos de radio y redes que operaban en la banda de frecuencia ilícita de 2.4GHz,

El estándar IEEE 802.11 transmite los datos a través de señales de radio, posee una capa de enlace de datos muy similar a la de Ethernet cableada de estándar IEEE 802.3, El protocolo para 802.11 utiliza un tipo de protocolo conocido como

CSMA/CA (Carrier-Sense, Múltiple Access, Collision Avoidance). Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. Es difícil descubrir colisiones en una red de transmisión RF y es por esta razón por la que se usa la anulación de colisión. La capa MAC opera junto con la capa física probándola energía sobre el medio de transmisión de datos. ademas soporta el protocolo tcp/ip lo que lo hace el mas utilizado actualmente.

El estandar IEEE 802.11 es basado en: FHSS y DSSS.

FHSS: viene del inglés Frequency Hoping Spread Spectrum o salto en frecuencia de ancho espectro y se basa en modular en diferentes frecuencias los datos que se envían. De este modo y siempre dentro de la banda de 2.4 GHz se manda parte de la información, se cambia a otra frecuencia y se sigue enviando la información. Este proceso se repite de forma indefinida mediante que por un segundo canal se transmite la secuencia de saltos. En total el ancho de banda para FHSS es de 83 MHz.

DSSS: viene del inglés Direct Sequence Spread Spectrum. En este tipo no se producen saltos en frecuencia, en su lugar se envía continuamente una secuencia de datos predeterminada de 11 bits de modo que al mandar un 0 se mandan los bits tal cual y si se envía un 1 la secuencia se invierte, los ceros se convierten en unos y viceversa. Esto se realiza expandiendo el espectro de la forma de onda sobre el ancho de banda empleado, que es menor que para la FHSS.

3.5.4.1 Tipos de estándares 802.11

Entre los tipos más comunes de este estándar tenemos a 802.11, 802.11a, 802.11b, 802.11f y 802.11g, 802.11h, además de algunos estándares encargados de la calidad de servicio y seguridad como lo son el 802.11e y el 802.11i.

3.5.4.1.1 IEEE 802.11

Es el estándar original WLAN, soporta velocidades entre 1Mbps y 2Mbps. Este estándar es no orientado a conexión y soporta Ethernet.

3.5.4.1.2 IEEE 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 de 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.

3.5.4.1.3 IEEE 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 (similar al de una red Ethernet convencional). 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.

3.5.4.1.4 IEEE 802.11f

Este estándar define las comunicaciones entre dos puntos de acceso para facilitar múltiples redes distribuidas en la WLAN.

3.5.4.1.5 IEEE 802.11g

Surgió en 2003, como la evolución del estándar 802.11b. 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.

3.5.4.1.6 IEEE 802.11h

Al contrario que en Ethernet, las especificaciones de radio 802.11 no escuchan la red antes de transmitir para comprobar que la línea esta libre. Estas, en cambio, transmiten y sin esperar la respuesta apropiada, paran y retransmiten. Los dispositivos Ethernet escuchan, envían, y si encuentran algún problema, esperan una cantidad de tiempo determinada antes de retransmitir. 802.11h se basa en 802.11a para resolver los problemas de interferencias y uso, así como mejorar la coexistencia con otras especificaciones que trabajan en el mismo ancho de banda. La especificación h chequea si las frecuencias están en uso antes de la transmisión (Dynamic Frequency Selection o DFS) y de que transmitan con el nivel

de energía mínimo (Transmit Power Control o TPC). Estas mejoras fueron formuladas para conseguir los requisitos de uso de la banda de 5GHz en la Unión Europea que denomina a su especificación equivalente como HiperLAN2.

3.5.4.1.7 IEEE 802.11e

Cada paquete que se envía por la red en 802.11b tiene las mismas posibilidades de llegar a su destino que cualquier otro. 802.11e pretende cambiar esto, permitiendo incorporar calidad del servicio (QoS) que proporcione prioridad de nos paquetes sobre otros. Esta es una tarea compleja que involucra la coordinación entre las radios de los diferentes clientes, puntos de acceso y administradores de sistemas. QoS es necesario para la emisión de voz de calidad utilizando VOIP (voz sobre IP) y para *streaming* multimedia. Las ventajas que proporcionan HomeRF y otras especificaciones de 2.4GHz frente a 802.11b es la posibilidad de priorizar los paquetes lo que asegura el envío de voz sin cortes que también se soluciona con 802.11e.

3.5.4.1.8 IEEE 802.11i

Inicialmente 802.11e cubría QoS y seguridad. Pero con los constantes informes de debilidad en el sistema de cifrado WEP (Wireless Equivalent Privacy) la parte de seguridad adquirió su propia identidad en **802.11i**. El grupo de esta especificación ha estado trabajando en la sustitución de WEP y afortunadamente se definirá con la suficiente compatibilidad como para no tener que revisar los sistemas ya creados.[3]

[3] MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis, Universidad ICESI, Valle del Cauca, Colombia, 2004

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

Tabla 1. Tipos de estándares IEEE 802.11[4]

[4] CUELLAR RUIZ, Jaime. Redes Inalámbricas, Estándares y Mecanismos de Seguridad. Articulo

4. RIESGOS DE LAS REDES INALÁMBRICAS

4.1 Vulnerabilidad de las redes inalámbricas

Hace algún tiempo, se publicó en varios medios de comunicación, la posibilidad de que exista cierta *vulnerabilidad* en el del protocolo 802.11. y esto lo podemos reflejar en el siguiente caso de la vida cotidiana en el ámbito de la informática.

Un ejemplo calve fue cuando se detectaron vulnerabilidades en las implementaciones de hardware del protocolo IEEE 802.11 que habilitan a un usuario que desee atacar, poder hacerlo con un dispositivo de bajo rango y costo. Varias compañías en conjuntos han informado que han sido detectadas fallas en las implementaciones de hardware del protocolo inalámbrico IEEE 802.11., estas fallas permiten un ataque trivial, pero efectivo en contra de la disponibilidad de los dispositivos de WLAN.

Un atacante, usando un dispositivo potable de bajo poder como un PDA electrónico con tarjeta de red inalámbrica puede causar una disrupción significativa a todo el rango de tráfico de un WLAN de que manera que hace difícil la detección o localización del atacante.

La falla está relacionada a la función Medium Access Control (MAC) del protocolo IEEE 802.11 dentro del procedimiento Clear Channell Assessment (CCA), el cual

es usado en todos los dispositivos inalámbricos que cumplen el estándar y que es fundamental para la transmisión simultánea dentro de una WLAN.

El protocolo de red inalámbrico IEEE 802.11 usa el algoritmo Clear Channel Assessment (CCA) para determinar si el canal de radio de frecuencia se encuentra libre para que el dispositivo pueda transmitir data. El algoritmo CCA usado en conjunto con la transmisión Direct Sequence Spread Spectrum (DSSS), es vulnerable a un ataque en el cual una señal de radio de frecuencia, especialmente diseñada, causará que el algoritmo concluya que el canal está ocupado haciendo que ningún dispositivo transmita data.

Una persona que ataque y explote dicha vulnerabilidad en la función CCA en la capa física, causará que la transmisión de datos durante el ataque entre los nodos de la WLAN, ya sean clientes o puntos de acceso y, cuando estén siendo atacados los dispositivos, éstos se comportarán como si el canal estuviese siempre ocupado, previniendo la transmisión de cualquier tipo de datos sobre la red inalámbrica.

La particularidad de esta falla es que no se necesitan equipos sofisticados, ni mucho dinero y tampoco muchas habilidades para poderla llevar a cabo. El potencial de daño de esta falla se incrementará en el tiempo a medida que el uso de las redes inalámbricas para infraestructuras críticas.

Los dispositivos de hardware inalámbrico que implementan el protocolo IEEE 802.11 usando la capa física DSSS. Incluye también IEEE 802.11, 802.11b y dispositivos inalámbricos 802.11g (debajo de los 20Mbps). Excluye IEEE 802.11a y dispositivos high-speed 802.11g (por encima de 20Mbps).

Los dispositivos en el rango de dispositivos de ataque estarán afectados. Si un AP está en un rango, todos los dispositivos asociados con ese AP serán denegados del servicio; si un A no está dentro del rango, únicamente esos dispositivos en el rango de ataque tendrán denegación de servicio.

Existen ciertas amenazas en las redes inalámbricas de área local, estas amenazas se caracterizan mínimo por:

- ✓ Un atacante puede usar hardware o drivers comodity, no se requiere hardware inalámbrico o dedicado.
- ✓ Un atacante consume recursos limitados en un dispositivo atacante, así que no es costoso para montar.
- ✓ La vulnerabilidad no será mitigada por capas emergentes MAC en mejoras de seguridad, por ejemplo, IEEE 802.11 TGi.
- ✓ Los vendedores independientes han confirmado que actualmente no hay defensa en contra de este tipo de ataques a DSSS basadas en WLANs.

- ✓ El rango de alcance del ataque puede crecer si se incrementa el poder de transmisión del dispositivo atacante o se usa una antena de alto aumento.[5]

4.2 Riesgos de las redes inalámbricas

Varios son los riesgos derivables de las vulnerabilidades de las redes inalámbricas. Por ejemplo, se podría perpretar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posibilite la denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2.4GHz (frecuencia utilizada por las redes inalámbricas).

Los puntos de acceso (AP) están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción de una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros son fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

[5] Canarias Wireless, Vulnerabilidades Inalámbricas. Articulo. Mayo 2003.

Si a diario observamos los distintos pensamientos de los hackers que existen en el mundo contemporáneo, podemos deducir que en el ámbito de la seguridad para redes inalámbricas un hacker puede entrar a la WLAN de una compañía a través de un punto de acceso sin protección o a través de una estación de trabajo una vez que esté asociado con la red, va a ser difícil de detectar porque probablemente no sean visibles en o cerca del sitio de la red, además, un hacker inteligente no se arriesga, por ello utilizará los recursos de la compañía silenciosamente, y como resultado, es probable que nunca lo detecten".

Para protegerse, los negocios deben asegurarse que los empleados o los hackers no instalen puntos de acceso que no están autorizados en la red y que los puntos de acceso que sí lo están, estén configurados de manera segura. En ambientes densos, como las áreas urbanas o edificios de oficinas con múltiples locatarios, las compañías tienen que asegurarse de que los usuarios no se conecten a las redes de otras compañías.[6]

4.3 Ataques a redes inalámbricas

Los ataques a las redes inalámbricas se basan en las identificaciones estas, este es el método para detectar la existencia de un AP de una red inalámbrica. Para ello, se utiliza una WNIC (tarjeta de red inalámbrica) funcionando en modo

[6] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas: Trabajo Ampliación de Redes. Tesis, Universidad de Valencia España.

promiscuo conjuntamente con un software que permite verificar la existencia de puntos de acceso.

En el momento en que se detecta la existencia de una red abierta, habitualmente se dibuja una marca en el suelo donde se anotan las características de la misma. Esto se conoce Wardriving y, una vez realizado, permite disponer de un autentico mapa donde se anotan todos los puntos de acceso con sus datos (SSID, WEP, direcciones MAC, etc...). además del Wardriving existen otros ataques y herramientas para la realización de estos como es el caso del WarChalking y el AirSnort respectivamente.

4.3.1 WarDriving

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza una análisis de la misma.

Para realizar el Wardriving se necesitan realmente pocos recursos. Los más habituales son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el AP en un mapa y el software apropiado (AirSnort para Linux o NetStumbler para Windows).

4.3.2 WarChalking.

No es ni ningún invento, ni un rumor más de los que corren por la red, aunque parezca mentira, grupos de internautas de todo el mundo están catalogando aquellas redes "vulnerables" para aprovecharlas gratuitamente como trampolín de acceso a Internet.

Este concepto se ha extendido rápidamente por los EEUU, Inglaterra y Dinamarca, aunque nadie, puede saber hasta donde ha llegado, dada la popularidad de los distintos foros en los que se esta promocionando este fenómeno, que ya tiene nombre propio, "Warchalking".

Un fenómeno, que, además, parte de un concepto totalmente colaborativo y en el que sus promotores dan a conocer sus hallazgos a otros interesados, para que estos mismos se beneficien del acceso.

Este ataque básicamente funciona así: Un pequeño ejército de internautas recorre las ciudades y las zonas de oficinas donde se presume que puedan existir redes WIFI. Equipados con portátiles y tarjetas inalámbricas, exploran las redes existentes e intentan encontrar aquellas que puedan ser usadas, por no contar con la protección debida, para el acceso a Internet.

Seguidamente, se toma nota de la dirección (que entrará a formar parte de algunos de los listados que ya empiezan a circular) y se marca la casa con tiza, para advertir a otros "geekies" de las posibilidades de esta red y si esta, o no, protegida.

Como muestra del espíritu del "Warchalking", se adopto la idea de los símbolos de los vagabundos que viven por las calles de las ciudades y su hábito de marcar los domicilios que ofrecen algún tipo de caridad para recordarlos y comunicar al resto de la comunidad de las ventajas que pueden conseguir en esas casas.

Por lo que parece, la fiebre esta tomando tal envergadura, que responsables de seguridad informática, temen ver marcada su casa o empresa... lo que significaría un trabajo mal hecho y una puerta abierta para decenas de usuarios que con sus portátiles buscan redes "libres" para navegar por Internet.

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que 'pasen por allí. El lenguaje como tal es realmente simple:

Símbolo	**Significado**
)(	Nodo abierto
()	Nodo cerrado
(W)	Nodo WEP

Tabla 2.

Lenguaje utilizado en Warchalking

Por ejemplo, el símbolo

Figura 3. Ejemplo del uso de Warchalking

Esto significa:

Prueba

)(

2.0

Identifica a un nodo abierto, que utiliza el SSID "Prueba" y dispone de un ancho de banda de 2.0 Mbps.[7]

4.3.3 Hacking

Con frecuencia la señal Wi-Fi no se queda entre las cuatro paredes de la oficina, sino que puede ser detectada, utilizada y/o explotada por aquellos atacantes

[7] MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis, Universidad ICESI, Valle del Cauca, Colombia, 2004

conocidos como hackers de redes inalámbricas (War Drivers) y hackers de señales inalámbricas (War Chalkers). Con la ayuda de un equipo sencillo y un software "rastreador" de los puntos de acceso inalámbrico que está listo para su descarga de Internet, estos individuos recorrerán ciudades y pueblos en busca de puntos inseguros de acceso inalámbrico.

Los hackers de redes inalámbricas tienen mucha práctica y han dedicado muchos sitios Web y carteleras de anuncios para mejorar sus actividades y compartir sus ideas. Los hackers de redes inalámbricas dedicados consiguen la ayuda del equipo más sofisticado, como antenas que ayudan a recoger las señales y receptores del Sistema de Posicionamiento Global (GPS) que se utilizan para obtener las coordenadas exactas (longitud y latitud) de un punto de acceso inalámbrico detectado con fines de mapeo.

4.3.4 Técnicas de intrusión

Algunas de las técnicas de intrusión mas comunes que afectan a una rede de área local inalámbrica son:

4.3.4.1 Sniffing y eavesdropping (escuchas - interceptación)

El programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son. Se utiliza una tarjeta de red que actúa en “modo adulterado”.

4.3.4.2 Spoofing (burla) y hijacking (secuestro)

El atacante falsifica información, ya sea un identificador de usuario o una contraseña permitidos por el sistema atacado. El funcionamiento de esta técnica se basa en redefinir la dirección física o MAC de nuestra tarjeta inalámbrica por una válida y se le asocia una dirección IP válida del sistema atacado.

4.3.4.3 Denegación de Servicio (DoS) o ataques por inundación

La denegación de servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica e Impide a los usuarios legítimos de esta, disponer de dichos servicios o recursos.

4.3.4 Otros ataques

4.3.4.1 Espionaje (surveillance)

Este ataque consiste simplemente en observar todo el entorno de la red inalámbrica, antenas, puntos de acceso, cables de red y todos los dispositivos conectados a la red, con el fin de recopilar información y combinar con otros tipos de ataques. Para la realización de este ataque no se necesita ningún tipo de “hardware” o “software” especial.

4.3.4.2 Interceptar una señal

En este ataque el atacante intenta identificar el origen y el destino que posee la información, tras haber interceptado la señal, el atacante intentará recopilar información sensible del sistema

4.3.4.3 Suplantar una fuente real

Esta técnica de ataque se engloba dentro de los ataques activos, donde un intruso pretende ser la fuente real u original.[8]

4.4 Herramientas el para monitoreo de redes inalámbricas

En la siguiente tabla se encuentran citadas las mas comunes herramientas para la identificación y el monitoreo de las redes inalámbricas.

Herramienta	Descripciones
NetStumbler	Identificador de APs, escucha los SSID y manda señales buscando APs
Kismet	Sniffer y monitor de WLANs de forma pasiva monitorea el trafico inalámbrico, orden la información para identificar SSIDs, direcciones MAC, canales y velocidades de conexión.
Wellenreiter	Herramienta para descubrir WLANs, Usa la fuerza bruta para identificar APS de bajo tráfico, oculta su verdadera MAC y se integra con GPS.
THC-RUT	Herramienta para descubrir WLANs, Usa la fuerza bruta para identificar APS de bajo tráfico- Su primera herramienta en una red desconocida.
Ethereal	Analiza WLANs, permite surfear de forma interactiva la información capturada, observando información detallada de todo el tráfico inalámbrico.
WepCrack	Rompe la encriptación. Hace un crack de WEP utilizando las vulnerabilidades en la programación de RC4.
AirSnort	Rompe la encriptación, monitorea de forma pasiva las transmisiones, computando la llave de encriptación cuando se han capturado suficientes paquetes.
HostAP	Convierte una estación WLAN para funcionar como un AP.

Tabla 3. Herramientas para el monitoreo de redes inalámbricas[9]

[8] HUERTAS GRAFIA, José Luís. Tecnologías de Red, “Seguridad en redes inalámbricas”.

[9] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas.

5. MÉTODOS DE SEGURIDAD

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. 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 una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Con estos métodos se buscan dos objetivos principales para alcanzar la anhelada seguridad, estos son: la autenticación y la privacidad.

La autenticación: El objetivo es evitar el uso de la red (tanto en la WLAN como la LAN a la que conecta el Access Point) por cualquier persona no autorizada. Para

ello, el Punto de Acceso solo debe aceptar paquetes de estaciones previamente autentificadas.

La privacidad: Consiste en encriptar las transmisiones a través del canal radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.

Teniendo en cuenta estos dos objetivos se definen los métodos de seguridad de 802.11, los cuales se han ido desarrollando e innovando mediante el surgimiento de nuevas necesidades.

Dependiendo su complejidad y características se han clasificado los métodos de seguridad para las redes inalámbricas en métodos básicos y métodos avanzados.

5.1 Métodos de seguridad Básicos

5.1.1 Medidas de Seguridad Física

La seguridad física en las WLANS es muy importante, es lo primero que se debe tener en cuenta al momento de la instalación de este tipo de redes, aunque no es una medida total y robusta de seguridad no se debe obviar por ningún motivo.

Lo primero que se recomienda es efectuar un reconocimiento del entorno físico para determinar el emplazamiento más apropiado de antenas exteriores e interiores, y de Puntos de Acceso de redes inalámbricas. Una vez que se hayan colocado las antenas y los Puntos de Acceso, y antes de conectar la red

inalámbrica, se debe evaluar el alcance de su transmisión de radio y su cobertura. Hay que direccionar la antena y ajustar la potencia del transmisor para restringir la emisión al área o a las áreas específicas para las cuales se quiere ofrecer el servicio de la WLAN (una planta del edificio, el edificio entero, complejo, etc.) Un emplazamiento y direccionamiento de la antena bien planeados puedes ayudar a reducir el riesgo de exposición de su emisión. Pero la cobertura adecuada para su edificio bien puede necesitar una transmisión de radio que, al menos, sobrepase en cierta medida los muros del mismo. Por otra parte, hackers provistos de antenas extremadamente potentes pueden acceder a señales que no son recibidas por tarjetas WLAN normales para laptops o para ordenadores de sobremesa. Por tanto, limitar la cobertura reduce su riesgo – pero esta medida no elimina el riesgo por sí sola.

Se debe realizar una auditoria centrada en la seguridad física de la WLAN. Existen muchos productos shareware y comerciales para la detección y análisis del tráfico, que pueden utilizarse para detectar toda la actividad de la WLAN dentro del área a la que pretende dar cobertura. También se debe Identificar y hacer un inventario de todos los Puntos de Acceso WLAN e interfaces de red autorizados, no autorizados (“rogue”), y vecinos. La instalación no autorizada de Puntos de Acceso es particularmente problemática. Los empleados que instalan un Punto de Acceso WLAN pueden, al igual que tantas características convenientes, anular involuntariamente medidas de seguridad existentes esenciales como, por ejemplo, cortafuegos y sistemas de detección de intrusos, mediante la apertura de puertas traseras a intranets, proporcionando a los atacantes acceso directo a servidores

con misiones críticas. Un buen administrador debe definir una estrategia para incorporar de manera segura a su topología aprobada, cualquier Punto de Acceso no autorizado descubierto o para anularlo y también determinar cómo coexistirá su WLAN con dispositivos inalámbricos vecinos (o visitantes) que están fuera de su control físico.

Otras medidas de seguridad que pueden ser adoptadas en el diseño de las WLAN son: la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio deshabilitando al máximo las señales emitidas hacia el exterior, además se podría utilizar cobertura metálica en las paredes exteriores y colocar los dispositivos WLAN lejos de las paredes exteriores. Estas medidas son un poco exageradas pero así podemos reducir aun más el riesgo de una WLAN[10]

5.1.2 WEP

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

5.1.2.1 Principales características de WEP

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática

[10] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas.

de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización (IV) más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización, en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).

2. Se concatena la clave secreta a continuación del IV formando el *seed*.
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed,* de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

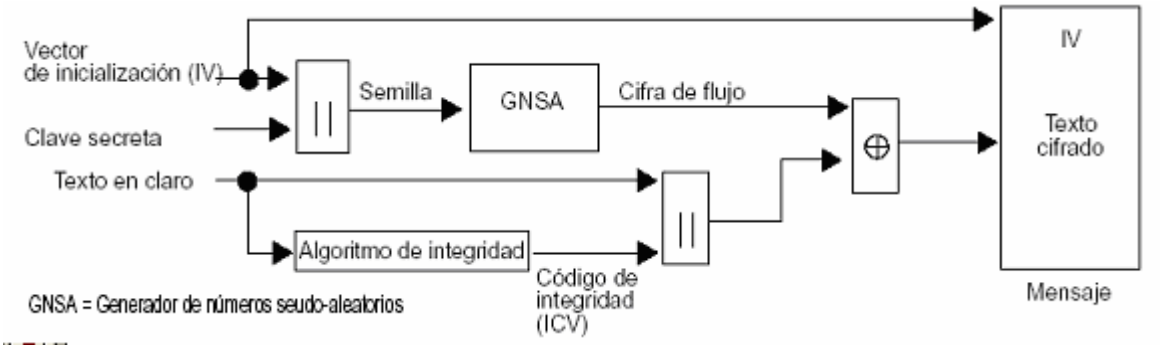

Figura 4. Algoritmo de encriptación de WEP

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

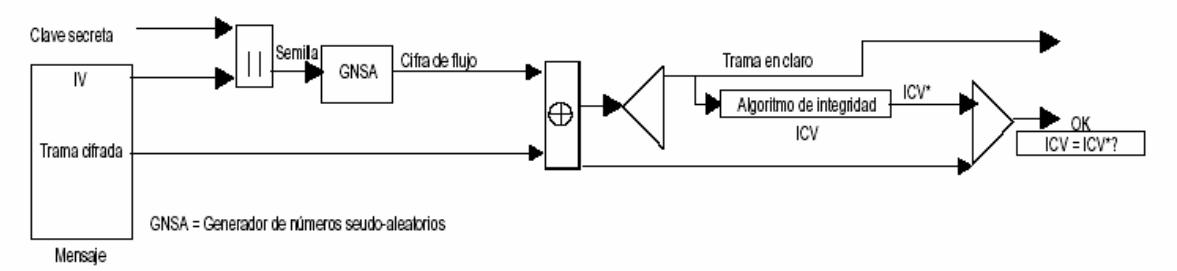

Figura 5. Algoritmo de desencriptación de WEP

5.1.2.2 Debilidades del WEP

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (*seed*) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según, este estándar indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^24=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u

horas. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual *keystream*? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.).

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su *keystream*, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP es que permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus *keystreams* asociados obtenidos por el procedimiento anterior.

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC.

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación *de secreto compartido* tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una *autentificación de sistema abierto*, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (*replay*). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

Dentro de estudios mas profundos se explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

5.1.2.3 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como *WEP2*. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es *WEP dinámico*. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios. Este mecanismo requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red, un servidor RADIUS (Remote Authentication Dial-In User Service, servicio de marcado de autenticación remota para usuarios) es el que se encarga de verificar si el login y password que se introduce es correcto y si es así asigna el perfil y permite la conexión. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una

trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPAy WPA2 (IEEE 802.11i). El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.[11]

5.1.3 Nombre de la red inalambrica (SSID, ESSID, IBSSID)

Todos los dispositivos que pertenecen a una WLAN (Adaptadores de Red y Puntos de Acceso) utilizan un nombre de red (SSID, ESSID, IBSSID) para identificarse. Todos los dispositivos que quieren pertenecer a la misma WLAN deben utilizar el mismo nombre, y solo se podrá establecer comunicación con aquellos dispositivos que tengan asignado este mismo nombre o pertenezcan a la misma WLAN.

El SSID (Service Set Identifiers), es el único nombre de red asignado para identificar una WLAN. Los clientes WLAN asocian el SSID que se les asigna con el

[11] BARAJAS, Saulo. Protocolos de seguridad en redes inalámbricas. Articulo

Punto de Acceso (AP). El SSID es un nombre de red que identifica el área cubierta por uno o más APs. En un modo comúnmente usado, el AP periódicamente transmite su SSID. Una estación inalámbrica que desee asociarse con un AP puede escuchar estas transmisiones y puede escoger un AP al que desee asociarse basándose en su SSID.

En otro modo de operación, el SSID puede ser usado como una medida de seguridad configurando el AP para que no transmita su SSID. En este modo, la estación inalámbrica que desee asociarse con un AP debe tener ya configurado el SSID para ser el mismo que el del AP. Si los SSIDs son diferentes, las tramas administrativas (management frames) enviadas al AP desde el estación inalámbrica serán rechazados porque ellos contienen un SSID incorrecto y la asociación no se llevará a cabo.

Desafortunadamente, debido a que las tramas de administración en las WLAN's 802.11 son siempre enviados de forma abierta, este modo de operación no provee seguridad adecuada. Un atacante fácilmente puede escuchar en el medio inalámbrico buscando las tramas de administración y descubrir la SSID del AP. Muchas organizaciones confían en el SSID para obtener seguridad sin considerar sus limitaciones. Esto es por lo menos parcialmente responsable de la facilidad con la que las WLAN's son comprometidas.

Tanto el ESSID como el BSSID son SSID (Service Set Identifier) que identifican y controlan el acceso del cliente inalámbrico a una WLAN específica.

Un ESSID (Extended Service Set Identifier) es utilizado para identificar los clientes inalámbricos y los puntos de acceso en una WLAN. Todos los clientes inalámbricos y los puntos de acceso de la WLAN deben utilizar el mismo ESSID, este puede tener un máximo de 32 caracteres, y distingue entre mayúsculas y minúsculas. Un BSSID (Basic Service Set Identifier) define de manera única cada cliente inalámbrico y punto de acceso.

Hay recomendaciones comunes para aminorar las vulnerabilidades de los nombres de red tales como Nunca se deben usar valores por defecto de fábrica o SSID en blanco, y no se debe permitir a los clientes que simplemente escuchen a "cualquier" SSID. Se deben utilizar SSIDs largos, difíciles de adivinar. Esta medida no impide que su SSID pueda ser capturado por intrusos a la WLAN, pero minimizará el número de clientes WLAN errantes (roaming) o adyacentes que pueden accidentalmente asociarse a su Punto de Acceso.

5.1.4 Filtrado de direcciones MAC

Este método consiste 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 (Media Access Control) 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.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

Este método no escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

Una de los grandes atractivos de las redes inalámbricas es facilitar la movilidad de los usuarios. En este caso, si la organización cuenta con varios Puntos de Accesos significa que la lista de direcciones debe mantenerse cargada y actualizada en cada uno de ellos.

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.

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 AirJack6 o WellenReiter, entre otros, que simulan temporalmente el numero de la dirección MAC. De este modo, el atacante puede hacerse pasar por un cliente válido.

En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, a que no prevé ningún mecanismo de cifrado.

Por tanto, este método simplemente puede proporcionar una cierta dificultad adicional a un atacante, pero en ningún momento constituye una solución de seguridad por si misma.[12]

5.1.5 Sistemas adicionales de seguridad.

5.1.5.1 Firewalls o Cortafuegos

El firewall o Cortafuegos es la herramienta cuya función es proporcionar determinado nivel de seguridad a la conexión de una red de datos con otras redes o con Internet y para ello combina elementos de software y hardware, el propósito principal del firewall es mantener a los intrusos fuera del alcance de la WLAN.

Conceptualmente, hay dos tipos de firewalls: firewall de Nivel de red y firewall de Nivel de aplicación, No hay tantas diferencias entre los dos tipos como se podría pensar. Además las últimas tecnologías no aportan claridad para distinguirlas hasta el punto que no está claro cual es mejor y cual es peor.

5.1.5.1.1 Los firewalls a nivel de red

Generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" firewall a nivel de red, particularmente, desde el momento que no puede tomar decisiones sofisticadas en relación con quién está hablando un paquete ahora o desde donde está llegando en este momento. Los firewall a nivel

---

[12] DELL COMPUTER CORPORATION, WIRELESS SECURITY IN 802.11 (WI-FI®) NETWORKS. Whitepaper, 2003.

de red se han sofisticado ampliamente, y ahora mantienen información interna sobre el estado de las conexiones que están pasando a través de ellos, los contenidos de algunos datagramas y más cosas. Un aspecto importante que distingue a los firewall a nivel de red es que ellos enrutan el tráfico directamente a través de ellos, de forma que un usuario cualquiera necesita tener un bloque válido de dirección IP asignado. Los firewalls a nivel de red tienden a ser más veloces y más transparentes a los usuarios.

5.1.5.1.2 Los Firewalls a nivel de aplicación

Son generalmente, hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellos. Los firewall a nivel de aplicación se pueden usar como traductores de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeros firewalls a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos firewalls a nivel de aplicación son bastante transparentes. Los firewalls a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad. Esto las hace diferenciarse de los firewalls a nivel de red.

Con la ubicación de un Cortafuegos entre los perímetros externo e interno, se asegura que tanto el tráfico hacia adentro como hacia fuera, sea aquel que esté definido en la política de seguridad de la red.

5.1.5.2 Defensa a través de DMZ (Demilitarized Zone)

Este método básico plantea simplemente la creación de una pequeña y aislada red situada entre la red inalámbrica y otras redes o Internet, esta red esta configurada de modo que Los sistemas de las redes externas o Internet pueden acceder a un número limitado de sistemas de la red DMZ y La transmisión directa de tráfico a través de la red DMZ está prohibido.

En esta zona, DMZ, es indispensable colocar los puntos de acceso de la WLAN para que estos no sean accedidos por aquellos usuarios no autorizados.

Como vemos este método es solo parte de la solución ya que solo provee seguridad a los elementos de nuestra red que se encuentran dentro de la DMZ.[13]

5.1.5.3 VPN (Virtual Private Network, VPN)

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los

[13] HUERTAS GRAFIA, José Luís. Tecnologías de Red, “Seguridad en redes inalámbricas”.

puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.[14]

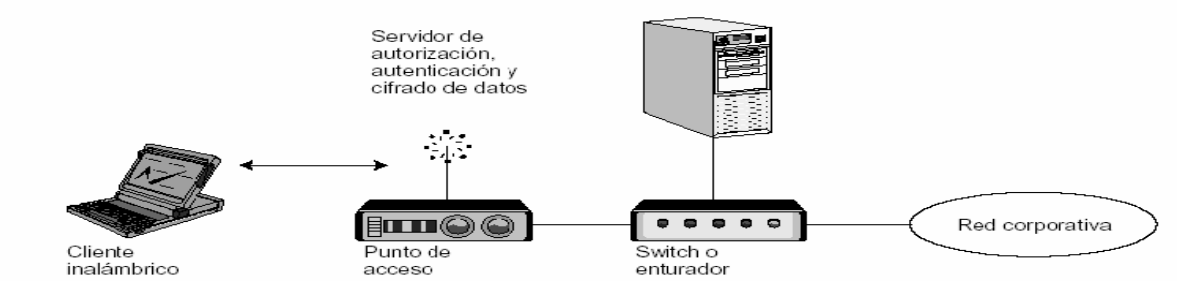

Figura 6. Red privada virtual inalámbrica

5.2 Métodos de seguridad avanzados

5.2.1 Protocolo de integridad de clave temporal (TKIP, Temporal Key Integrity Protocol)

Temporal Key Integrity Protocol (TKIP) amplía y mejora a WEP, solucionando sus vulnerabilidades. TKIP amplía la longitud de la clave de 40 a 128 bits y pasa de

[14] MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis, Universidad ICESI, Valle del Cauca, Colombia, 2004

ser única y estática a ser generada de forma dinámica, para cada usuario, para cada sesión (teniendo una duración limitada) y por cada paquete enviado.

El protocolo TKIP esta compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. esta medida protege contra los ataques de falsificación.
- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.
- Utilización de un vector de inicialización (IV) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

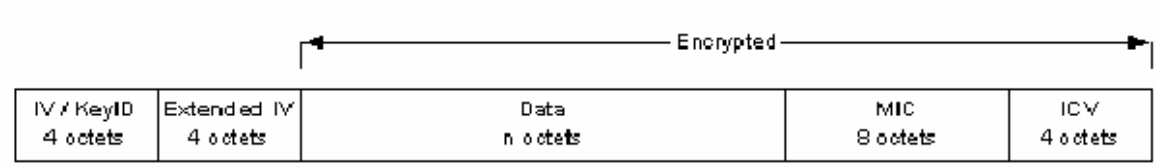

Figura 7. Estructura de encriptación TKIP

la utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 2^{48} paquetes utilizando una sola llave temporal antes de ser rehusada.

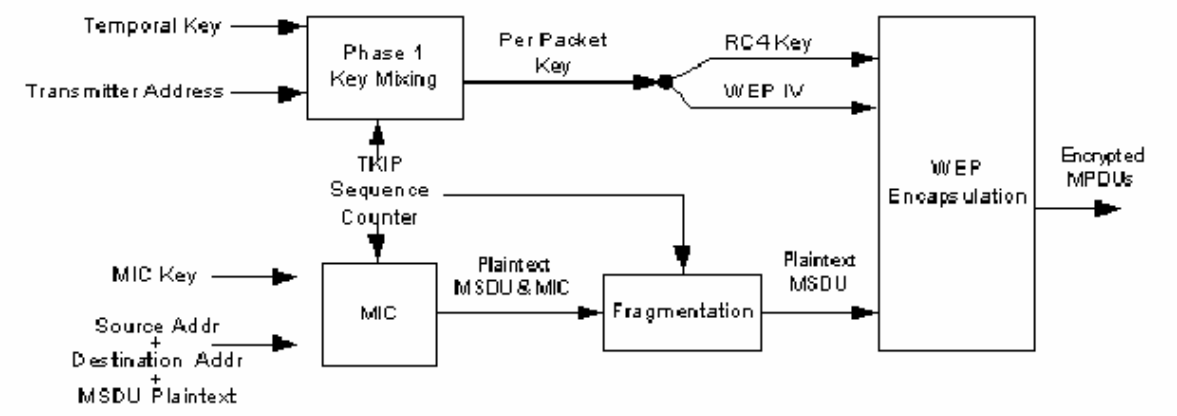

Figura 8. Proceso de encapsulamiento TKIP

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y un IV de 24 bits para su posterior encapulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función Hash unidimensional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior, sino, el paquete se descartara para prevenir posibles ataques por repetición. Después de que el valor MIC sea calculado basado n el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.[15]

[15] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas.

5.2.2 CCMP (Counter-Mode/CBC-MAC Protocol)

Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado, este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Advanced Encryption Standar), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se esta utilizando 802.11i.

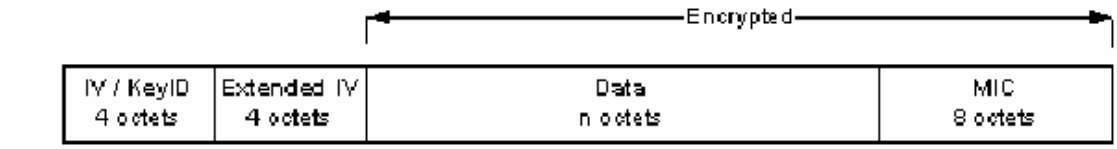

Figura 9. Estructura de la encriptación CCMP

CCMP utiliza IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

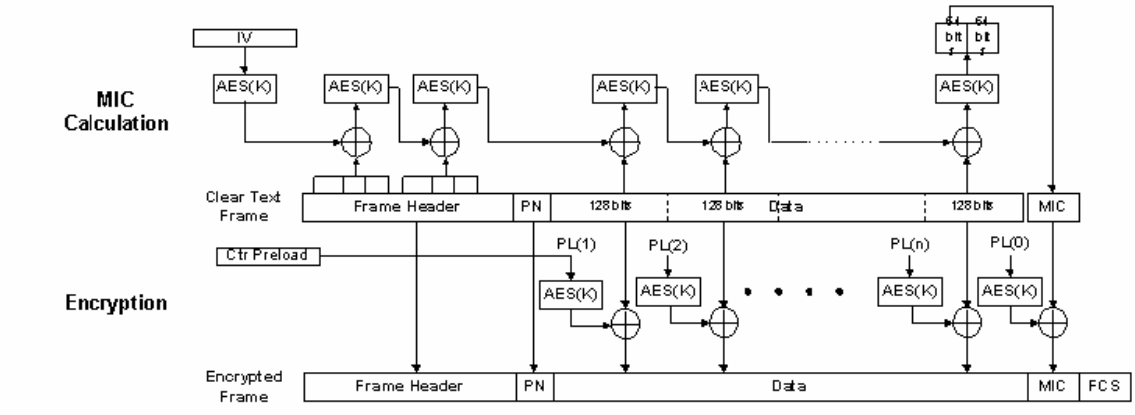

Figura 10. Proceso de Encriptación de CCMP

En el proceso de encriptación CCMP, la encriptación de los boques utiliza la misma clave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, a clave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. El cálculo del MIC y la encriptación se realizan de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.[16]

5.2.3 Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol).

El Protocolo de autenticación extensible (EAP) es una extensión del Protocolo punto a punto (PPP), que es un protocolo que proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto estableciendo una conexión de par evitando que intrusos entren en la comunicación.

Es un protocolo punto a punto que soporta métodos de autenticación múltiples. Este protocolo se desarrolló como respuesta al aumento de la demanda de autenticación de usuarios de acceso remoto que utilice otros dispositivos de seguridad.

---

[16] ALAPONT M, Vincent. Seguridad en Redes Inalámbricas.

EAP proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros.

EAP, junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

5.2.3.1 EAP-TLS: Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate). Su ventaja fundamental es que en este caso tanto el servidor como el cliente se autentican mutuamente y se evita que, debido a la mala política de compartir claves, unos usuarios se puedan hacer pasar por otros. Además obtenemos un elevado nivel de seguridad desde el inicio mismo de la conexión.

5.2.3.2 EAP-TTLS: Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2 que son solo protocolos de autenticación de usuarios remotos.

5.2.3.3 PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.

El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).

La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas. Las variantes de EAP que utilizan contraseñas son las siguientes:

5.2.3.4 EAP-MD5: Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

5.2.3.5 LEAP: Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

5.2.3.6 EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña)

a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

5.2.3.7 EAPOL: EAP over LAN, Esta variante provee autenticación efectiva sin tener en cuenta la forma como se implementan las claves WEP o si hay o no encriptación. Si el protocolo es configurado para implementar intercambio de claves dinámicas, el servidor podrá retornar claves de sesión a lo AP con el mensaje de aceptación, luego los AP usan estas claves de sesión para construir, firmar y encriptar los mensaje de claves EAP que son inmediatamente enviados a los suplicantes los cuales podrán después enviar y recibir mensajes exitosamente.[17]

5.2.4 AES (Advanced Encryption Standard)

Actualmente el algoritmo DES está obsoleto y, para sustituirlo, el NIST (National Institute of Standards and Technology) propuso una competición para desarrollar el estándar AES, hasta cuya resolución ha adoptado el sistema Triple-DES como una solución temporal.

Los cinco algoritmos finalistas para AES, elegidos entre un total de quince, fueron MARS, RC6, Rijndael, Serpent y Twofish. Así, Rijndael es un cifrador en bloque

[17] MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis

diseñado por John Daemen y Vincent Rijmen como algoritmo candidato al AES (Advanced Encryption Standard). Su diseño estuvo fuertemente influenciado por el de un cifrador (block cipher Square), que también fue creado por John Daemen y Vincent Rijmen y se centraba en el estudio de la resistencia al criptoanálisis diferencial y lineal. El nombre del algoritmo es una combinación de los nombres de sus dos creadores

El cifrador tiene longitudes de bloque y de clave variables y puede ser implementado de forma muy eficiente en una amplia gama de procesadores y mediante hardware. Como todos los candidatos del AES es muy seguro y hasta la fecha no se le han encontrado puntos débiles.

La longitud de la clave de Rijndael, si bien es variable, debe ser de 128, 192 o 256 bits, según los requisitos establecidos para el AES. Asimismo, la longitud del bloque puede variar entre 128, 192 o 256 bits. Todas las posibles combinaciones (nueve en total) entre longitudes de clave y bloque son válidas, aunque la longitud oficial de bloque para AES es de 128 bits. Las longitudes de la clave y el bloque pueden ser fácilmente ampliadas a múltiplos de 32 bits. El número de iteraciones del algoritmo principal puede variar de 10 a 14 y depende del tamaño del bloque y de la longitud de la clave. Una de las críticas más habituales de Rijndael es el escaso número de iteraciones, pero esto no supone un problema, pues el coste operacional puede aumentarse sin más que incrementar el tamaño del bloque y la longitud de la clave.

La implementación Stealth de Rijndael usa una clave de 256 bits y un bloque de 128 bits de tamaño. Usando la mayor longitud posible de clave conseguimos la máxima seguridad para el usuario. La filosofía de este diseño concedería pues mayor importancia a la seguridad que a la velocidad. Si el usuario proporciona una clave de menor longitud Stealth la transforma de una forma especial, casi aleatoriamente, para hacerla de 256 bits. Y aunque acepta tamaños de bloque mayores que 128 bits, no existe ninguna razón para usarlos siendo que este número de bits ha sido elegido como tamaño estándar.

5.2.5 MIC (Message Integrity Check)

Message Integrity Check o chequeo de integridad del mensaje ha sido diseñado para prevenir que intrusos capturen paquetes, los alteren y los re-envíen. La función MIC, la cual se le conoce como "Michael", es un hash criptográfico de un solo sentido, el cual re-emplaza el Checksum CRC-32 utilizado en WEP. Michael provee una función matemática de alta fortaleza en la cual el receptor y transmisor deben computar, y luego comparar, si no coinciden la data se asume como corrupta y se desecha el paquete.

5.2.6 Estándar IEEE 802.1x

Especifica los mecanismos necesarios para llevar a cabo un control de acceso por puerto en redes 802. Este estándar, ha tenido una gran aceptación, y su implementación está disponible en varias formas por parte de los fabricantes.

802.1x define el control de acceso por puerto. Para ello, cuando un dispositivo quiere acceder a una red a través de un AP, este solicita unas credenciales al mismo. Esta solicitud se realiza usando EAP (*Extensible Authentication Protocol*). Una vez recibidas las credenciales por parte de la estación, el AP reenvía las mismas a un servidor de autentificación RADIUS, que realiza la autentificación del usuario y autoriza su acceso.

Debido a que EAP es un protocolo genérico, puede transportar diferentes tipos de autentificación, con diferentes prestaciones cada uno de ellos una debilidad que presenta este estándar es que fue diseñado para redes cableadas y aun así podemos utilizar sus principios para la transmisión de datos en una red inalámbrica.

El siguiente esquema representa la forma el funcionamiento de este estándar y como este permite la transmisión de datos en una red inalámbrica de área local.[18]

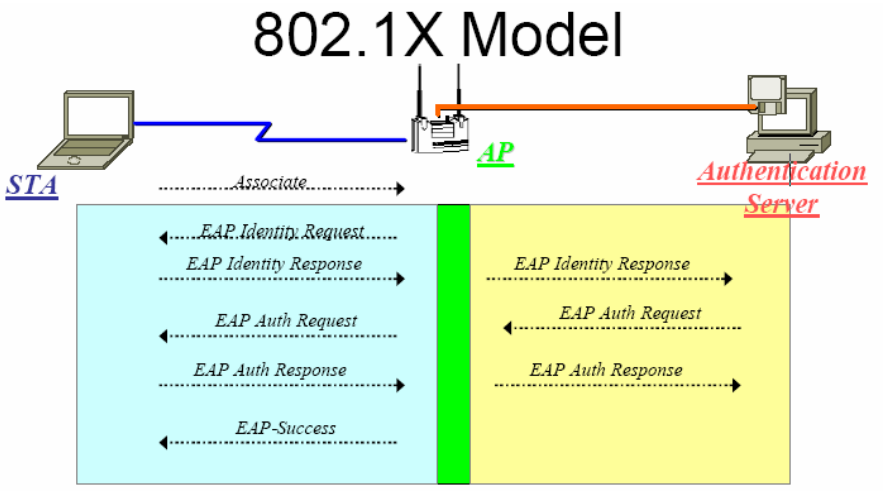

Figura 11. Funcionamiento del estándar IEEE 802.1x

[18] CHEN, Jyh-Cheng; JIANG, Ming-Chia y LIU, Yi-Wen. Wireless LAN Security and IEEE 802.11i*.

5.2.7 WPA

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que es IEEE 802.11i.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i.

5.2.7.1 Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X**. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el

usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros). Cuenta

- **EAP**. EAP, es el *protocolo de autentificación extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*).
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- **MIC** (*Message Integrity Check*) o Michael. Código que verifica la integridad de los datos de las tramas.

5.2.7.2 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número

suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes, se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X/EAP/RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

5.2.7.3 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

5.2.7.3.1 WPA con servidor AAA, RADIUS normalmente

Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

5.2.7.3.2 WPA con clave inicial compartida

Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.[19]

[19] BARAJAS, Saulo. Protocolos de seguridad en redes inalámbricas. Articulo
Wi-Fi Alliance, Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks

6. LAS MEJORAS DE SEGURIDAD

IEEE, la organización que creó los estándares 802.11, es responsable de mantener estos estándares actualizados, es decir, trabajan en estos según las nuevas necesidades. Los miembros de IEEE incluyen a muchos vendedores que deben seguir un proceso de estándar-fabricación estricto y deben hacer los compromisos para estar de acuerdo en cualquier estándar final. Este proceso toma un tiempo largo. Para enfocar los requisitos del mercado más rápidamente, la Alianza de Wi-Fi ha creado que una norma del mercado llamada Wi-Fi Protected Access que se llevará a cabo delante de el estándar 802.11i.

6.1 Estándar IEEE 802.11i

El estándar IEEE 802.11i es una nueva norma de seguridad desarrollada por el IEEE Taskgroup i (TGi). Una de las principales misiones de este grupo es definir una red de seguridad robusta (RSN, Robust Security Network). Esta RSN, de acuerdo con el proyecto 802.11i, es básicamente una red segura que solo permita la creación de asociaciones de redes de seguridad robustas, RSNA (Robust Security Network Associations), es decir, en una RSN las asociaciones de todas las estaciones incluyendo los puntos de acceso (APs, Access Points), son creados en una fuerte relación autenticación/asociación llamada RSNA. RSNA es también descrita por el TGi como una asociación de redes que depende del estándar 802.1x para transportar sus servicios de autenticaciones y para manejar el servicio

de entrega de claves. Una asociación de seguridad se refiere al contexto (claves criptográficas, contadores, etc.) que proporciona el estado necesario para la operación correcta para el cifrado y descifrado de solicitudes en IEEE 802.11, es decir, solo aquellas estaciones con esta capacidad pueden acceder a la RSN. RSNA incluye un moderno mecanismo, el 4-way handshake, un sistema de comunicación entre estaciones en 4 vías, para proveer un manejo robusto de contraseñas de sesión. Con el mejoramiento del 802.1x, el mecanismo de 4-way handshake y el mejoramiento del algoritmo criptográfico, los enlaces inalámbricos de las comunicaciones en el estándar IEEE 802.11 son protegidos seguramente.

6.2 Estructura del estándar IEEE 802.11i

El estándar IEEE 802.11i define dos clases de estructuras para las WLANs IEEE 802.11: RSN y pre-RSN.

Una estación se puede describir como un equipo apto RSN si tiene la capacidad de crear RSNAs.

Si una red solo permite RSNA en asociaciones con equipos aptos RSN es conocida como una estructura de seguridad RSN y si una red permite asociaciones pre-RSNA entre estaciones es conocida como una estructura de seguridad pre-RSN. La principal diferencia entre RSNA y pre-RSNA esta en el handshake de cuatro vías, si este handshake no esta incluido en el procedimiento autenticación/asociación se dice que la estación usa pre-RSNA.

6.2.1 Pre-RSN

La seguridad pre-RSN consiste en dos subsistemas de seguridad: Autenticación de entidad IEEE 802.11 y WEP. La autenticación de entidad IEEE 802.11 incluye una autenticación de sistema abierto y una autenticación de clave compartida. En el sistema de autenticación abierto no hay algoritmos de autenticación. Una estación es autenticada simplemente basándose en su identidad. La autenticación de claves compartida, por el contrario, autentica una estación basado en una clave secreta conocida tanto para el solicitante como por el que responde la autenticación. Esto requiere el mecanismo de privacidad implementado en WEP.

6.2.2 RSN

Con el objetivo de mejorar la seguridad en la estructura pre-RSN, la seguridad RSN define procedimientos de manejo de claves para las redes 802.11. Esto también refuerza la autenticación y la encriptación en pre-RSN.

- **Mejora de la autenticación**: IEEE 802.11i utiliza IEEE 802.1x para sus servicios de autenticación y manejo de claves. Esto incorpora dos componentes en la arquitectura de IEEE 802.11: Un puerto IEEE 802.1x y un servidor de autenticación (AS, Authentication Server). El puerto IEEE 802.1x representa la asociación entre dos pares, es decir, hay una asignación uno-a-uno entre el puerto IEEE 802.11 y la asociación. El puerto IEEE 802.1x permite el trafico general de datos solo cuando la autenticación es completamente exitosa. El AS puede ser un servidor individual e independiente o puede estar

integrado dentro del AP. A pesar de que el protocolo entre AS y AP no es recomendado por IEEE 802.11i, debe haber un canal seguro como TLS o IPsec (los cuales se utilizan como protocolos de ciframientos para asegurar el canal), entre el AP y el AS. Un Protocolo de autenticación extensible EAP que soporta autenticación mutua debe ser usado en RSN, es decir, el solicitante y el que responde deben ser capaces de autenticarse entre si.

- **Manejo y establecimiento de claves**: Dos maneras para soportar la distribución de claves son introducidas por el IEEE 802.11i: manejo manual de claves y manejo automático de claves. El manejo manual de claves requiere que el administrador configure manualmente las claves. El manejo automático de claves esta disponible solo en RSNA. Este cuenta con el IEEE 802.1x para soportar el servicio de manejo de claves, mas específicamente, el handshake en 4 vías es usado para establecer cada clave temporal para transmisión de paquetes.
- **Mejoramiento de la encriptación:** Con el fin de mejorar la confidencialidad, se han desarrollado dos algoritmos criptográficos avanzados: Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (CCMP, Counter-Mode/CBC-MAC Protocol) y el Protocolo de integridad de clave temporal (TKIP, Temporal Key Integrity Protocol). En RSN, el algoritmo CCMP es obligatorio mientras que el TKIP es opcional y es recomendado solo para optimizar el equipo pre-RSNA

6.2.3 RSN IE (RSN information Element)

El estándar IEEE 802.11i especifica un elemento de información RSN (RSN IE, RSN information Element) que transportan información de seguridad RSN incluyendo las capacidades RSN, autenticación y selector de clave cifrada. RSN IE puede ser usado para distinguir estaciones pre-RSN y estaciones RSN. Las estaciones RSN incluirán en sus mensajes el RSN IE, por el contrario, las estaciones pre-RSN no contienen el RSN IE en sus mensajes. El RSN IE contiene una lista de campos de autenticación y selector de cifrado para las comunicaciones. El primer campo, identificador del elemento, debe tener un valor siempre 48 en decimal. El campo longitud indica el numero de octetos en el campo de información excluyendo el identificador del elemento y el campo longitud. El campo versión muestra la versión del protocolo RSNA. El campo contador de paridad de solicitud de clave cifrada indica el número de paridad de solicitud de clave que esta contenido en el campo lista de paridad de solicitud de clave. La paridad se refiere a dos entidades que están asociadas entre si. La paridad de solicitud de clave es la solicitud cifrada que esta siendo o es asociada entre pares que se están comunicando. Similarmente el contador de autenticación y de solicitud de manejo de claves indican el número de autenticación y de solicitudes de manejo de claves contenido en el campo de las listas de autenticación y solicitud de manejo de claves. En el campo capacidades RSN, se coloca la capacidad solicitada o informada. Usando este campo el receptor podría conocer los mecanismos de seguridad que soporta el remitente o los que esta solicitando.

Element ID	Length	Version	Group Key Cipher Suite	Pairwise Key Cipher Suite Count	Pairwise Key Cipher Suite List	Authentication and Key Management Suite Count	Authentication and Key Management Suite List	RSN Capabilities

Figura 12. Formato del RSN IE

Generalmente hablando el RSN IE transporta la información de seguridad robusta que indica la autenticación o el algoritmo de cifrado usado en la comunicación. Las estaciones y los APs pueden aprender las capacidades de seguridad de las comunicaciones y negociar con los RSN IE de cada uno entre si. Luego de esto los procedimientos de seguridad correspondiente se ejecutaran.

Si el suplicante y el servidor de autenticación se autentican entre si, ambos generan independientemente una clave de paridad maestra (PMK, Pairwise Master Key). Luego el servidor de autenticación envía el PMK hasta el autenticador por un canal seguro (por Ej. TLS, IPsec). Luego el handshake de 4 vías usa el PMK para deducir y verificar la clave de paridad temporal (PTK, Pairwise Transient Key), de esta manera se garantiza que la sesión establecida entre el suplicante y el autenticador sea confiable. Luego la clave de grupo del handshake es usado para generar grupos de claves actualizadas, las cuales son compartidas entre el grupo de estaciones y los APs. Con el uso de estas claves se pueden intercambiar seguramente mensajes de broadcast y multicast por el aire.

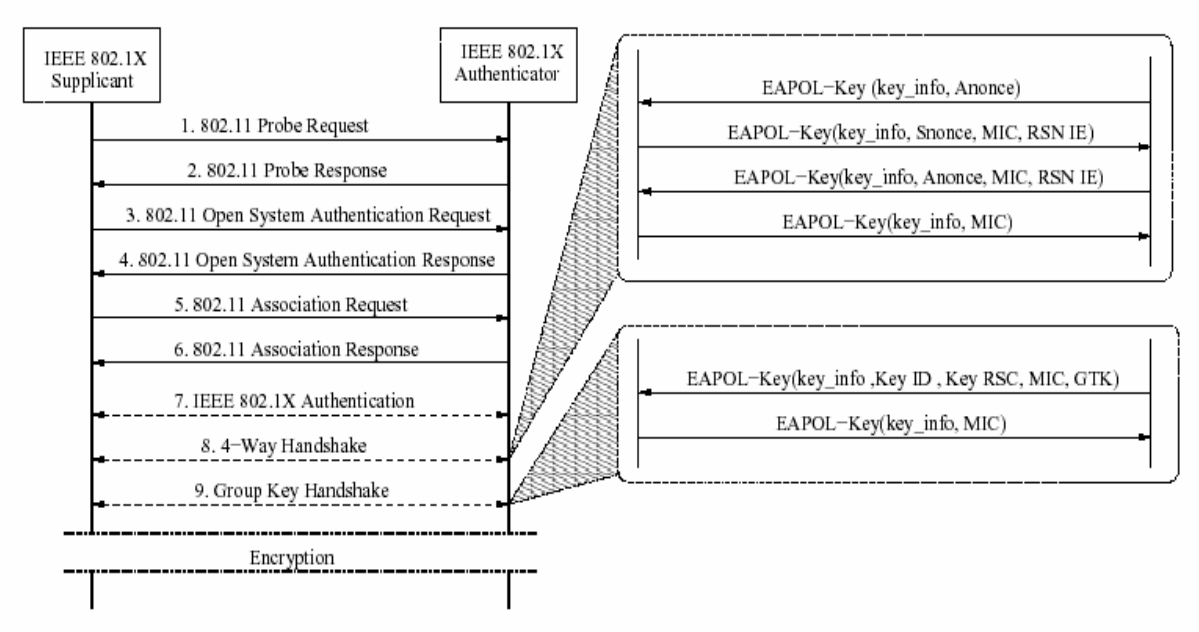

Figura 13. Flujo para el establecimiento del RSNA

6.3 Mejora de la autenticación

En el estándar original IEEE 802.11, una estación primero debe asociarse con un AP IEEE 802.11, de esta manera la estación esta habilitada para acceder a los servicios de la WLAN. Luego de encontrar el AP tras el recibimiento de la respuesta de prueba, la estación móvil necesita seguir los siguientes dos pasos: la autenticación y asociación de la entidad. Antes de la asociación con el AP, la estación necesita llevar a cabo la autenticación como entidad IEEE 802.11. Como discutimos anteriormente, hay dos maneras de realizar esta autenticación: Autenticación de sistema abierto y la autenticación de clave compartida. La autenticación de sistema abierto permite que una estación sea autenticada sin tener una clave WEP correcta. En este caso hay un intercambio de dos mensajes,

el primer mensaje enviado desde el suplicante (estación móvil) al autenticador (AP) es usado para exponer la identidad de la estación, basándose en esta, el resultado de la autenticación es enviado desde el autenticador de regreso a la estación, aquí no hay algoritmo de autenticación. En la autenticación de clave compartida hay un intercambio de 4 mensajes, el primer mensaje contiene la identificación de la estación, este es enviado de la estación hasta el AP. Luego el AP enviara al suplicante un paquete el cual debe ser encriptado por este (estación móvil) usando la clave compartida WEP y reenviar el paquete hasta el AP. Si el paquete es encriptado correctamente, el suplicante es autenticado exitosamente. El resultado de la autenticación es enviada a la estación en el cuarto mensaje. Si la estación es autenticada exitosamente, se procede con la asociación IEEE 802.11. La estación móvil debe transmitir una solicitud de asociación al AP y el AP le envía una respuesta de asociación a la estación.

La autenticación de clave compartida en IEEE 802.11 no es adoptada por IEEE 802.11i, en cambio este incorpora el estándar IEEE 802.1x para realizar el proceso de autenticación para la RSN. IEEE 802.1x es realizado después de la autenticación y la asociación de sistema abierto. IEEE 802.1x provee un mecanismo de acceso a la red basado en puerto para proteger de los accesos no autorizados.

El estándar IEEE 802.11i también específica una estructura más robusta utilizando el estándar IEEE 802.1x, el handshake en cuatro vías y una clave de grupo del handshake para autorizar y autenticar la estaciones. Después que las estaciones son autenticadas exitosamente, las claves criptográficas también son

configuradas, por consiguiente la estación esta habilitada para enviar y recibir de manera segura tramas unicast y broadcast. Además, el estándar IEEE 802.11i también soporta la pre-autenticación. Una estación puede ser pre-autenticada con un AP antes de hacer el proceso de roaming (saltar de celda en celda). En consecuencia la latencia de handoff (buscar la estación base con menos congestión) será reducida.

6.4 Manejo y establecimiento de claves

El estándar IEEE 802.11i utiliza un sistema de handshake en cuatro vías para el manejo y el establecimiento de claves además de una clave de grupo del handshake.

6.4.1 4-way handshake o handshake en cuatro vías

RSNA propone un handshake en cuatro vías para mejorar algunas funciones como lo es la confirmación del estado de las estaciones en comunicación, garantizando la actualización de las claves de sesión, la inicialización de las claves criptográficas y la confirmación de la instalación de las claves. El handshake en cuatro vías es llevado a cabo por la utilización del estándar 802.1x. Específicamente, los mensajes intercambiados en este handshake están en el formato de clave EAPOL, el estándar IEEE 802.1x determina que este formato puede ser usado para el intercambio de claves criptográficas.

En el handshake de cuatro vías el autenticador envía primero un mensaje al suplicante. El primer mensaje contiene la información de la clave y una clave

material generada por el autenticador llamada *anonce*, esta clave es esencialmente valor aleatorio o seudo-aleatorio el cual no debe ser rehusado. Después que se recibe el primer mensaje el suplicante lo valida chequeando el campo de contador de respuesta en el mensaje, el contador de respuesta es una secuencia de números que van incrementando cada vez que hay un mensaje de clave EAPOL, si este contador es menor o igual al valor que tiene el suplicante, este descarta el mensaje, sino el suplicante genera una nueva clave llamada *snonce* usando el algoritmo de función seudo-aleatoria (PRF, Pseudo-Ramdom Function) con la clave *anonce*. Con la clave *snonce,* la clave maestra de paridad (PMK) y otra información como las entradas, el suplicante deduce la clave temporal de paridad (PTK). Luego el suplicante envía de regreso al autenticador el segundo mensaje el cual contiene la información de clave, la clave *snonce,* el RSN IE del suplicante y el código de integridad de mensaje (MIC), el MIC es una compilación criptográfica usada para proveer el servicio de integridad. Cuando el autenticador recibe el segundo mensaje lo valida chequeando el contador de respuesta. Este proceso es similar que el que se realiza cuando se recibe el primer mensaje. Luego deduce el PTK, como el autenticador usa el mismo algoritmo y las mismas entradas, el PTK deducido por el autenticador debe ser el mismo que el del suplicante. El autenticador también verifica el MIC. El paquete es descartado si el MIC no es valido. además el autenticador compara el RSN IE con el que esta contenido en la solicitud Asociación/reasociación recibida anteriormente del suplicante, si esta no es exactamente idéntica la asociación es terminada, sino el autenticador envía el tercer mensaje al suplicante, el tercer

mensaje incluye la información de clave, la clave *anonce*, el MIC y el RSN IE del autenticador. Cuando el suplicante recibe el tercer mensaje, primero verifica el mensaje chequeando el contador de respuesta y el campo de la clave *anonce,* después compara el RSN IE con el recibido previamente en la respuesta de prueba, el suplicante se desasociara del AP si el RSN IE es diferente, si este es correcto el suplicante chequea el MIC, si el MIC es valido, el suplicante envía el cuarto mensaje al autenticador. Cuando el cuarto mensaje es recibido por el autenticador, este chequea el contador de respuesta, si este es valido, verifica el MIC, si el MIC es valido entonces el handshake en cuatro vías esta completo. El cuarto mensaje por el autenticador para saber que el suplicante ha instalado correctamente una clave temporal, PTK, esta clave solo es conocida por el autenticador, el suplicante y el servidor de autenticación y es usada como clave para la encriptación de datos.

6.4.2 Clave de grupo del handshake

RSNA define también una clave de grupo del handshake por autenticador para entregar la clave de grupo temporal (GTK) a los suplicantes para que estos puedan recibir mensajes de broadcast. Este intercambio de la clave de grupo de handshake al igual que el handshake en cuatro vías también utiliza el formato de clave EAPOL.

El grupo de claves de handshake es realizado después del handshake de cuatro vías, el autenticador envía primero al suplicante un mensaje el cual incluye la información de la clave, el MIC, y el GTK. El GTK es encriptado usando la clave

de encriptación de EAPOL (KEK), y el MIC es computado con el cuerpo del mensaje de la clave EAPOL usando la clave de confirmación de EAPOL (KCK), tanto el KEK y el KCK hacen parte del PTK. Cuando el suplicante recibe el mensaje chequea el contador de respuesta, luego usa el KCK para verificar el MIC, el suplicante solo puede desencriptar el GTK con el KEK el contador de respuesta y el MIC son validos. Luego el suplicante contigua el GTK en su dirección MAC IEEE 802.11, además también responde un mensaje al autenticador, el cual incluye la información de la clave y el MIC, similarmente el autenticador valida el contador de respuesta y el MIC.

6.5 Mejoramiento de la encriptación

El algoritmo WEP se usa primordialmente para proteger las comunicaciones inalámbricas de los ataques de intrusión además puede prevenir accesos no autorizados. De esta forma, WEP proporciona servicios de confidencialidad e integridad. WEP se basa en la clave secreta compartida entre la estación móvil y el AP. WEP usa el algoritmo de encriptación RC4. Antes de enviar un dato, el remitente necesita calcular el Valor de Comprobación de Integridad (ICV) con un algoritmo CRC-32. Luego encripta la trama de datos y el ICV. El texto cifrado consiste en los datos encriptados y su ICV. Además, debe colocarse a uno el bit WEP del encabezado MAC. Cuando el destinatario recibe un una trama MAC con el bit WEP en uno, entonces usará la clave WEP compartida para desencriptar la carga útil.

Se sabe que WEP ha sido craqueado. WEP es vulnerable debido a la corta longitud de su Vector de Inicialización (IV) y la clave secreta estática. Los IV son utilizados para concatenar la clave secreta compartida, con el fin de producir diferentes secuencias de claves RC4 para cada paquete. El IV es generado aleatoriamente e incluido en el paquete. Con solo 24 bits de IV, WEP podría eventualmente usar el mismo IV para diferentes paquetes de datos, lo que se conoce como colisión de IV. Cuando se acumulan diferentes paquetes basados en el mismo IV, un atacante podría averiguar el valor compartido, por ejemplo, la secuencia de claves o la clave secreta, entre las partes de la comunicación. La naturaleza estática de la clave compartida causa otro problema de seguridad. Debido a que el original IEEE 802.11 no provee de ningún mecanismo para el manejo de claves, el administrador del sistema y un usuario en general usan la misma clave secreta compartida por un largo período de tiempo. Incluso, la misma clave WEP es compartida por todas las estaciones en un mismo Sistema de Servicios Básicos (BSS) o Sistema de Servicios Extendidos (ESS). Esta naturaleza proporciona suficiente tiempo al atacante para monitorear y hackear en WLAN's con WEP habilitado.

Para enmendar los defectos en WEP, la IEEE 802.11i desarrolla un algoritmo mejor llamado Protocolo de Integridad de Clave Temporal (TKIP) como estándar interino. TKIP, inicialmente conocido como WEP2 también se basa en la encriptación RC4. Sin embargo, se implemente de una forma diferente que evita las vulnerabilidades de WEP. TKIP define una Clave Temporal (TK) que es una

clave secreta de 128 bits compartida por el encriptador y el desencriptador. La TK puede ser común a muchas partes. El encriptador y el desencriptador deben usar la forma de ciframiento RC4. Cada parte debe asegurar que ningún IV sea usado más de una vez con una misma TK. El IV se implementa como un contador de 16 bits comenzando en cero. Las implementaciones deben asegurarse de que la TK sea actualizada antes de que el espacio de 16 bits de IV se agote. TKIP también emplea un contador de secuencia de paquetes para ordenar la Unidad de Datos de Protocolo MAC (MPDU). El destinatario debe desechar las MPDU's que estén fuera de servicio. Por consiguiente, esto podría proteger el ataque de respuesta. Además, TKIP combina la clave temporal con la dirección MAC del cliente y luego agrega un IV de 16 bits relativamente grande para producir la clave para encriptar los datos. Esto asegura que cada computador utilice una clave diferente para la encriptación. TKIP aplica básicamente la misma encriptación que WEP, pero utiliza el protocolo IEEE 802.1X EAPOL, para actualizar las claves temporales y prevenir la reutilización de claves. Esto proporciona una distribución dinámica de claves que mejor significativamente la seguridad proporcionada por WEP. El TKIP puede ser adaptado en los antiguos productos IEEE 802.11 a través de parches de firmware relativamente simples. Esto es favorable especialmente para los vendedores. Y además, los equipos que solamente soporten el antiguo WEP, aún serán capaces de interoperar con dispositivos que tengan TKIP habilitado. TKIP es opcional en 802.11i.

Debido a que TKIP usa encriptación RC4 al igual que WEP, se le considera una solución a corto plazo para la seguridad en WLAN. Además de TKIP, el estándar IEEE 802.11i también define un Protocolo MAC Counter Mode/CBC (CCMP) como una solución a largo plazo. CCMP utiliza una encriptación más fuerte a través del Algoritmo de Encriptación Avanzado (AEA) que usa el modo CCM (IETF RFC 3610) con una clave de 128 bits y un bloque de operación de 128 bits de tamaño. El modo CCM combina Counter-Mode(CMR) y Código de Autenticación de Mensaje de Encadenamiento de Bloques Cifrados (CBC-MAC). El CTR es usado para encriptar la carga útil y el MIC para proveer servicio de confidencialidad. El CBC-MAC calcula el MIC para proporcionar autenticación y servicios de integridad. CCM requiere una nueva Clave Temporal (TK) y necesitas actualizarla cuando el Número de Paquete (PN) está repetido. El número de paquete se incrementa por cada MPDU y puede ser usado para prevenir el ataque de repetición con el Contador de Repeticiones en el destinatario. El número de paquete y el identificador de clave son codificados en el encabezamiento del CCMP. Aunque el CCMP podría proporcionar servicios de seguridad más fuertes, requiere hardware adicional (co-procesador) para mejorar el desempeño de la encriptación. Por consiguiente, el antiguo hardware IEEE 802.11 no será actualizable en muchos casos. CCMP es obligatorio en IEEE 802.11i.[20]

---

[20] DELL COMPUTER CORPORATION, WIRELESS SECURITY IN 802.11 (WI-FI®) NETWORKS. ALAPONT M, Vincent. Seguridad en Redes Inalámbricas: Trabajo Ampliación de Redes. Tesis. CHEN, Jyh-Cheng; JIANG, Ming-Chia y LIU, Yi-Wen. Wireless LAN Security and IEEE 802.11i*.

7. CONCLUSIÓN

La tecnología inalámbrica es la puerta de un mundo de posibilidades de conexión sin la utilización del cableado clásico, proporcionando flexibilidad, movilidad, mejor escalabilidad, facilidad de instalación, menor costo etc., por estas razones esta tecnología esta tomándose gran parte del futuro de los sistemas de comunicación.

Las WLANs como todos los sistemas de comunicación tienen sus desventajas e inconvenientes, uno de ellos y el más importante es la seguridad, uno de sus mayores inconvenientes es su principal ventaja, el no usar cables, Debido a que en estas redes las conexiones se hacen de manera inalámbrica, se corren muchos riesgos al momento de transmitir la información por el aire. Existen muchos riesgos de seguridad cuando estamos trabajando con las redes inalámbricas, estos riesgos tienen en común el lograr el acceso no autorizado y sabotear la red, el ataque más común de hoy en día es la intrusión.

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas. Su implementación depende del uso que se vaya a dar a la red, ya sea que sea una red de una empresa o una red casera, de si es una red que ya existente o la vamos a implementar nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

Conocidas las vulnerabilidades de las redes de área local inalámbrica y sus factores de riego podemos proponer diferentes métodos para la implantación de la seguridad, de los cuales podemos escoger los más adecuados para hacer más robusta la seguridad de nuestra red y así establecer un control tanto físico como lógico del acceso y la transmisión de información por esta.

Finalmente no se recomienda un solo método para preservar la seguridad de una red inalámbrica, lo mejor es utilizar una buena política de seguridad, es decir, implantar normas de seguridad homogéneas y sin fisuras.

Esta política debe constar de un buen método de seguridad física, para lograr una seguridad en el medio donde se va a implementar la WLAN.

Un método de seguridad lógico avanzado, es decir, un método como WPA o el estándar IEEE 802.11i, que son los mas efectivos y por lo tanto los mas usados actualmente y son los recomendados por las empresas competentes. Este método avanzado de seguridad nos va ayudar a conseguir los principales objetivos de la seguridad, la autenticidad y la privacidad de los usuarios de la red y la integridad

de la información que por esta se trasmite, esto hará nuestra comunicación confidencial y confiable.

Se debe utilizar uno o varios sistemas adicionales de seguridad, como firewalls, VPN o DMZ, estos métodos sirven de apoyo a los métodos avanzados de seguridad en el momento que algún intruso quiera acceder a la WLAN.

Además se recomienda realizar auditorias y monitoreos de la red cada cierto tiempo para evaluar el nivel de seguridad de la WLAN, esto evitara que las medidas de solución de problemas de seguridad y recuperación se vuelvan un obstáculo para el trabajo habitual de los sistemas de comunicación.

8. RECOMENDACIONES

La seguridad en redes de área local inalámbricas es muy importante en la implementación de sistemas de comunicación que presentan esta tecnología. Este documento comprende de manera sencilla una investigación acerca de las vulnerabilidades, riesgos, ataques, amenazas y métodos de seguridad de esta tecnología de comunicación, nos referimos a los métodos para brindar y/o mejorar la seguridad en el desarrollo de implementaciones inalámbricas en redes de área local.

El estándar IEEE 802.11i es el método mas reciente que existe en estos momentos, por lo tanto el mas efectivo, esta técnica recoge lo mejor de su antecesor el WPA y realiza mejoras en cuanto a los principales aspectos de la seguridad de las redes, autenticidad, privacidad e integridad de la información. En estos momentos las organizaciones competentes con el tema de la seguridad siguen trabajando con el fin de obtener nuevos y mejores resultados en cuanto a la implementación de este conjunto de técnicas, siempre buscando lograr mejores normas para disminuir las vulnerabilidades y así también las amenazas y ataques.

Por otra parte, como este tema de la seguridad de las redes inalámbricas es muy factible a cambios, ya sea por el crecimiento del auge de esta tecnología o por el desarrollo de mejores técnicas por parte de los atacantes, sabemos que no hemos

dicho todo, es decir, en este preciso momento pueden haber nuevas investigaciones acerca de las fallas de estas redes o muchos atacantes pueden estar aplicando nuevas técnicas para sobrepasar los métodos de seguridad existentes. En un tiempo no muy prolongado este estándar que hoy es el mejor solo será parte de uno nuevo y mejorado.

Hacemos referencia al TaskGroup i (TGi) de IEEE que es la entidad encargada de realizar las investigaciones con respecto a la seguridad de las redes inalámbricas de área local

9. GLOSARIO

AAA: Abreviatura de Autenticación, Autorización y Accounting, sistema en redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

AES - Advanced Encryption Standard / Estándar de Cifrado Avanzado: También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.

Acceso Remoto: Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

Access Point (AP) - Punto de Acceso (PA): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

Ad Hoc: Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son

comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

Algoritmo de Encriptación: Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños.

Antena: Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia que punto emitan la señal podemos encontrarlas direccionales u omnidireccionable.

Ataque de Fuerza Bruta: Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

Autenticación: Proceso en el que se da fe de la veracidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

Autorización: Proceso por el que se acredita a un sujeto o entidad para realizar una acción determinada.

Bluetooth: Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el término *piconet* . Un *piconet* es un grupo de 2 u 8 aparatos que utilizan "Bluetooth" *que* comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada *piconet* contiene un aparato principal ("master") que es el encargado de coordinar el "Hopping Pattern" del *piconet* para que los demás aparatos ("slaves") sean capaces de recibir información.

Checksum Criptográfico: Checksum calculado mediante la utilización de un algoritmo con base criptográfica. Es imposible cambiar unos datos sin que el checksum criptográfico cambie. Ver también Checksummer.

CheckSum: Herramienta que calcula un único número asociado a determinados archivos que habitualmente no cambian para protegerlos. CheckSummer recalculará periódicamente dicho número y si se detecta que ha cambiado, será un indicio de infección.

Clave de Encriptación: Serie de números utilizados por un algoritmo de encriptación para transformar plaintext (texto sin encriptar que se puede leer directamente) en datos ciphertext (encriptados o cifrados) y viceversa.

Cliente o Usuario Inalámbrico: Toda solución suceptible de integrarse en una red wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc...

Confidencialidad: Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

Cortafuegos o Firewall: Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc...

Denegación de Servicio (DoS) - Denial of Service: Se trata de una ofensiva diseñada específicamente para impedir el funcionamiento normal de un sistema y por consiguiente impedir el acceso legal a los sistemas para usuarios autorizados.

DES: Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

DSSS - Direct Sequence Spread Spectrum / Espectro Amplio mediante Secuencia Directa: A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos .Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.

EAP - Extensible Authentication Protocol / Protocolo de Autenticación Extensible: Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virutla (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

FHSS - Frequency Hopping Spread Spectrum / Espectro Amplio mediante Saltos de Frecuencia: Primer desarrollo de la técnica de transmisión del Espectro

Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar acabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este "Hopping Pattern". El estándar IEEE 802.11 utiliza FHSS, aunque hoy en día la tecnología que sobresale utilizando FHSS es Bluetooth.

HASH: Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

Integridad de Archivos: Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

IPSec - IP Security: Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

MD5: Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, EL PRIMERO SE ENVÍA sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

RADIUS - Remote Authentication Dial-In User Service: Sistema de autenticación y accounting empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

Roaming: En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad

Sniffers: Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los sniffers pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras...

SSID: Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

Tarjeta de Red Inalámbrica: Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

TKIP - Temporal Key Integrity Protocol / Protocolo de Integridad de Clave Temporal: Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security: Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS - situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS handshake Protocol. Y, el protocolo de handshake TLS - permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente. Basado en SSL de Netscape 3.0, TLS supercede y es una extensión de SSL, si bien no son interoperables.

Virus: Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

VPN - Red Privada Virtual / Virtual Private Network: Red privada que se configura dentro de una red pública. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos

sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (*LAN*).

Warchalking: Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

Wardriving: Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc...

WEP - Wired Equivalent Privacy: Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WLAN - Wireless Local Area Network / Red de Área Local Inalámbrica: También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

WPA - Wi-Fi Protected Access / Acceso Wi-Fi Protegido: Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

10. BIBLIOGRAFÍA

STALLINGS, William. Comunicación y Redes de Computadoras. Prentice-Hall, Madrid, 2000.

HALSALL, Fred. Comunicación de Datos, Redes de Computadoras y Sistemas Abiertos. Addison-Wesley iberoamericana, 1998.

RAPPAPORT, Theodore S. Wireless communications: principles and practice. Prentice-Hall, 1996.

FLICKENGER, Rob. Building Wireless Community Networks. O´Reilly, 2002.

FLECK, Bob y POTTER, Bruce. 802.11 Security, O´Reilly, 2002.

CAM-WINGET, Nancy; MOORE, Tim; STANLEY, Dorothy y WALKER, Jesse. 802.11i Overview. Whitepaper.

WI-FI ALLIANCE, Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks

CANARIAS WIRELESS, Vulnerabilidades Inalámbricas. Articulo. Mayo 2003.

3E TECHNOLOGIES INTERNACIONAL. Strengthening 802.11i Implementations with Additional Standards-based Mechanisms. Whitepaper, 2004.

BARAJAS, Saulo. Protocolos de seguridad en redes inalámbricas, Doctorado en Tecnologías de las Comunicaciones, Universidad Carlos III de Madrid. Articulo.

DELL COMPUTER CORPORATION, WIRELESS SECURITY IN 802.11 (WI-FI®) NETWORKS. Whitepaper, 2003.

WATCHGUARD TECHNOLOGIES, Seguridad al Descubierto: Procedimientos de Seguridad por Capas Para Incorporar Redes LAN Inalámbricas a Intranets, Whitepaper, 2002.

CHEN, Jyh-Cheng; JIANG, Ming-Chia y LIU, Yi-Wen. Wireless LAN Security and IEEE 802.11i*. Whitepaper, Nacional Tsing Hua Univesity, Taiwam, 2004.

DIAZ, Tony. Autenticación e integridad en redes wireless, Whitepaper, Madrid 2003.

UNIVERSIDAD POLITÉCNICA DE MADRID, Redes sin cables. Articulo. 2002

ARBAUUGH, William A. y MISHRA, Arunesh. An Initial Security Analysis of the IEEE 802.1X Standard.

ALAPONT M, Vincent. Seguridad en Redes Inalámbricas: Trabajo Ampliación de Redes. Tesis, Universidad de Valencia España.

FRÍAS Javier y CARAMAZANA Alberto. SEGURIDAD EN LA RED Y EN EL COMERCIO ELECTRÓNICO: “Seguridad en redes inalámbricas”. Tesis, Universidad de Salamanca, Madrid.

MADRID M, Juan M. Seguridad en redes inalámbricas 802.11. Tesis, Universidad ICESI, Valle del Cauca, Colombia, 2004

CUELLAR RUIZ, Jaime. Redes Inalámbricas, Estándares y Mecanismos de Seguridad. Articulo

NEWSWEEK. The Future of Wireless: Wireless in the world. Articulo, Junio 2004

GOMEZ CARDENAS, Roberto. Seguridad en la infraestructura de redes inalámbricas. Conferencia. XII CONGRESO NACIONAL DE ESTUDIANTES INGENIERIA DE SISTEMAS XIICNEIS USACA, Cali – Colombia, 2.003.

BULA, Cesar. Wireless Technology, Conferencia. XII CONGRESO NACIONAL DE ESTUDIANTES INGENIERIA DE SISTEMAS XIICNEIS USACA, Cali – Colombia, 2.003.

HUERTAS GRAFIA, José Luís. Tecnologías de Red, “Seguridad en redes inalámbricas”. Presentación de ponencia.

MONTILLA F, Ivan M. Fallos de Seguridad del Estándar IEEE 802.1X, Como convivir con ellos. Ponencia. XII CONGRESO NACIONAL DE ESTUDIANTES INGENIERIA DE SISTEMAS XIICNEIS USACA, Cali – Colombia, 2.003.

Fuentes de información electrónicas

http://www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/default.asp

http://standards.ieee.org/getieee802/portfolio.html?agree=ACCEPT

http://www.goaheadmail.com/tools/web/redir.php

http://www.wl0.org/~sjmudd/wireless/network-structure/article.html#AEN55

http://www.elearningamericalatina.com/edicion/agosto1_2004/it.php

http://www.windowstimag.com/atrasados/2003/80_oct03/articulos/seguridad_1.asp

http://www.edubis.com/pub/magazine/articulos/wsec/wsec.htm

http://www.xombra.com/go_articulo.php?articulo=31

http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_3245.html#1

http://www.wirelesslansecuritysite.htm

http://www.e-advento.com/tecnologia/wlan_intro.php

http://www.wlana.org/learn/educate.htm