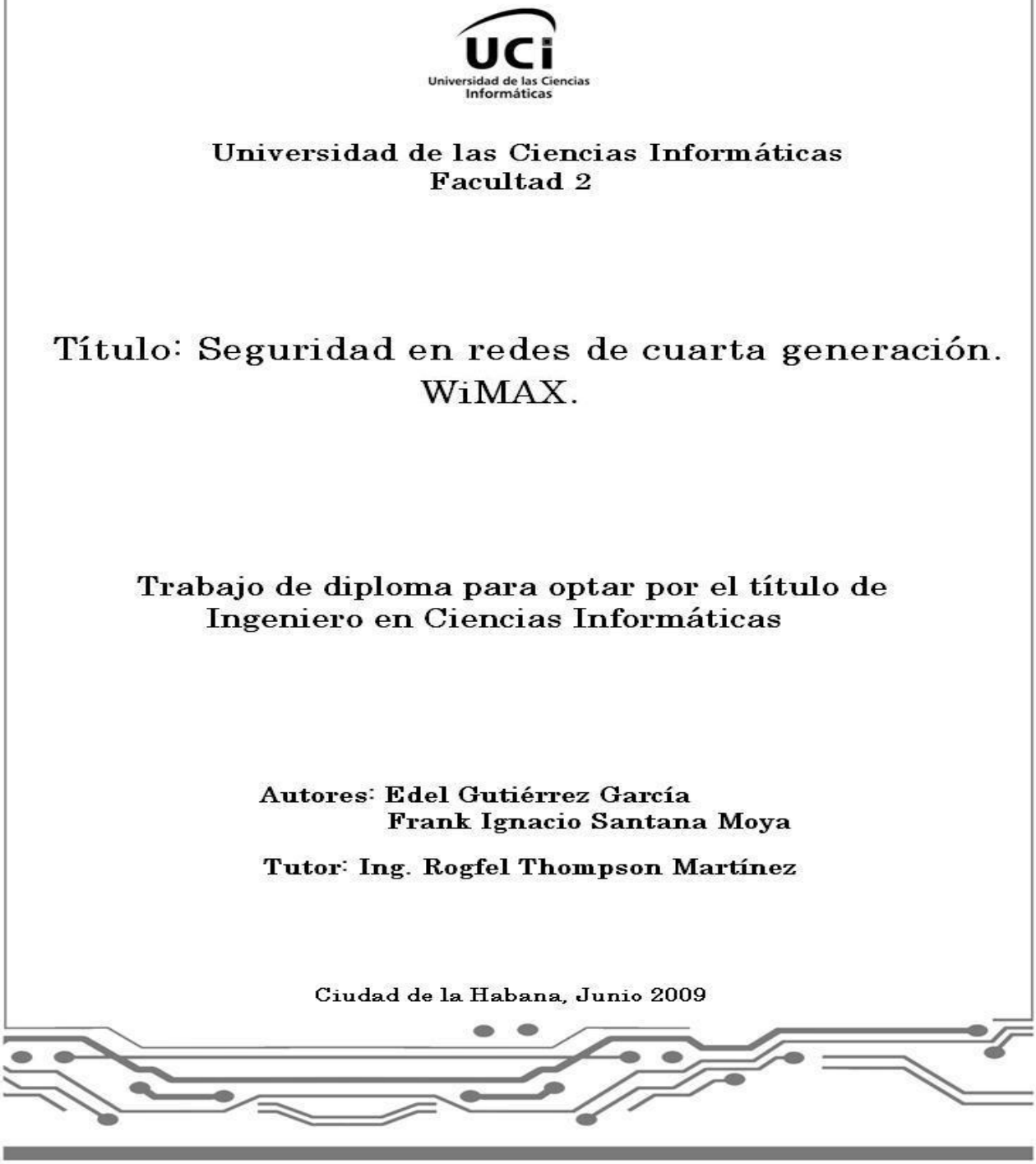


Universidad de las Ciencias Informáticas
Facultad 2

Título: Seguridad en redes de cuarta generación. WiMAX.

Trabajo de diploma para optar por el título de Ingeniero en Ciencias Informáticas

Autores: Edel Gutiérrez García
Frank Ignacio Santana Moya

Tutor: Ing. Rogfel Thompson Martínez

Ciudad de la Habana, Junio 2009

Declaración de autoría

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

_____ _____

Autor Autor

Edel Gutiérrez García Frank Ignacio Santana Moya

_____

Tutor

Ing. Rogfel Thompson Martínez

Agradecimientos

De Edel:

A mis padres agradecerle toda la paciencia que han tenido, por el apoyo y la fuerza que me han brindado. A mis hermanos por confiar tanto en mí y ayudarme cada vez que los necesitaba. A mis abuelos por su cariño y apoyo, gracias por creer en mí. A mis amigos que han cargado estos 5 años conmigo y me han aguantado y ayudado tanto, y a mi compañero de tesis y mejor amigo. Gracias!!

De Frank:

A mis padres agradecerle toda la paciencia que han tenido, por el apoyo y la fuerza que me han brindado. A mis hermanos por confiar tanto en mí y ayudarme cada vez que los necesitaba. A mis abuelos por su cariño y apoyo, gracias por creer en mí. A mis amigos que han cargado estos 5 años conmigo y me han aguantado y ayudado tanto, y a mi compañero de tesis y mejor amigo. Gracias!!

Dedicatoria

A nuestras familias y amigos.

Resumen

Las redes inalámbricas se han ido desarrollando a una velocidad vertiginosa, al igual que las tecnologías para estas redes. WiMAX es una de estas tecnologías, siendo también la especificación para redes metropolitanas inalámbricas. Esta será la base de las redes de acceso a Internet y servirá de apoyo para facilitar las conexiones en zonas rurales. Se utilizará además en el mundo empresarial para implementar las comunicaciones internas. El presente trabajo de diploma tiene como objetivo investigar la seguridad en la tecnología de redes inalámbricas WiMAX enfocándose en la cuarta generación de redes. De modo que constituya la fuente de información fundamental a la hora de implementar las políticas de seguridad de la tecnología. En el trabajo se realizará un profundo análisis de los protocolos, certificados y demás aspectos en torno a la seguridad en esta tecnología. Se llegará a una propuesta de seguridad, que será evaluada y validada por expertos en el tema, garantizando así que esta investigación siente las bases de un anteproyecto para ofrecer las mejores alternativas en la toma de decisiones de seguridad cuando se implante la nueva infraestructura.

Palabras claves: WiMAX, redes, seguridad, protocolo.

Índice de contenidos

Introducción

En la actualidad Internet ha experimentado un desarrollo acelerado que ha creado necesidades de acceso crecientes y cada vez más exigentes por parte de los usuarios. Muchos han hecho del acceso a Internet parte de su vida cotidiana para el desarrollo de muchas de sus actividades, realizar compras a través de la web, revisar su correo electrónico, buscar información para completar sus trabajos o simplemente para la descarga de música o películas, por solo mencionar unos pocos ejemplos.

Las redes inalámbricas surgen como una imperiosa necesidad para aquellos usuarios que por sus actividades requieren desplazarse de un lugar a otro y necesitan conectarse a internet de una forma fácil y segura. Esta movilidad que tanto se necesita solo es posible si las computadoras móviles se comunican a través de señales de radio, ya no es necesario estar atados a un cable para conectarse. No hay muchas novedades en las redes inalámbricas, pero la conexión de los distintos aspectos de la informática con los de la transmisión las convierte en una opción atractiva, e incluso insinúa la raíz de una nueva revolución social, pues las personas pueden comunicarse de formas nuevas y más flexibles. La tecnología inalámbrica en la actualidad se ha hecho posible en muchos de los lugares públicos como cafeterías, hoteles, aeropuertos y universidades.

Las primeras redes inalámbricas propietarias surgen a mediados de los 90 y en la actualidad su desarrollo esta normado para que la tecnología pueda ser utilizada independientemente de cuál sea fabricante de los equipos. Las normas han surgido a base de estándares regulados por la IEEE (Institute of of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos), una institución sin fines de lucro que cuenta con miembros en más de 175 países y con más de 360.000 trabajadores.

Por su parte las empresas telefónicas celulares también se han unido al mercado de las redes de dato, teniéndolas como un enfoque adicional a su servicio principal que es la comunicación de voz. Las redes de telefonía celular se dedicaran cada vez más al los datos mejorando para ello el ancho de banda disponible.

Se han realizado muchos intentos para desarrollar redes inalámbricas con diferentes tecnologías. Una de ellas es la basada en la llamada tecnología de infrarrojo que se ha utilizado con mucho éxito en la comunicación de dispositivos entre si, como la comunicación de una computadora (PC) con otros equipos como impresoras, agendas electrónicas, y no tanto para acceder a redes. Dado a que por las frecuencias

que utilizan su alcance es limitado en distancia, ya que las ondas infrarrojas no pueden pasar objetos opacos.

Otra tecnología inalámbrica exitosa es Bluetooth, creado para comunicar una PC con micrófonos, mouse, celulares entre otros, es también de poco alcance pero como una de sus principales ventajas tiene que utiliza muy poca energía eléctrica por lo que es muy popular en los audífonos de celulares.

Una tecnología que inicialmente se creó para acceder a redes LAN (Local Area Network, Red de Área Local) de forma inalámbrica es WI-FI (Wireless Fidelity, Fidelidad Inalámbrica), hoy se utiliza mayormente para acceder a internet. Recientemente han surgido los llamados "Hot-Spots" o redes públicas inalámbricas con el fin de acceder a Internet en determinados lugares basados en WI-FI, que corresponde al estándar IEEE 802.11. Estos lugares son de uso público en donde se puede acceder a Internet de forma inalámbrica y muchos de ellos son gratuitos.

Pero sin duda una de las aplicaciones más importantes del denominado WI-FI es el hogar donde puede establecerse fácilmente una red inalámbrica de bajo costo, mediante la cual se puede compartir la impresora o el acceso a Internet desde cualquier ubicación de su casa o departamento y sin tener que romper murallas o desplegar cables. Esta tecnología permite conectarse a una distancia de unos 100 metros o más.

El acelerado proceso de desarrollo que lleva el mundo tecnológico y el aumento de los dispositivos que necesitan conexión, lleva consigo la evolución constante de las redes de informáticas, ya sean por cable o inalámbricas.

Actualmente está comenzando una cuarta generación de redes, siendo esta muy superior a las tres anteriores. Se puede decir que esta cuarta generación no es un estándar ni una tecnología definida como las anteriores, sino una colección de tecnologías y protocolos que permite el máximo rendimiento de procesamiento de una red inalámbrica más adecuada en cada momento.

La convergencia de dichas tecnologías surge de la necesidad de agrupar los diferentes estándares en uso con el fin de delimitar el ámbito de funcionamiento de cada uno de ellos y con el fin también de integrar todas las posibilidades de comunicación en un solo dispositivo de forma transparente al usuario. Esta nueva generación donde más será utilizada es en el campo de la telefonía móvil, para mayor beneficio de los usuarios.

A la cuarta generación de redes o 4G (Cuarta Generación), WWRF (Wireless World Research Forum, Fórum Mundial de Investigación Inalámbrica) la define como una red que funciona con la tecnología de Internet combinándola con otros usos y tecnologías tales como Wi-Fi, WiMAX, LTE y EVDO.

La comunicación alcanzaría una velocidad de 100Mbps que puede aumentar hasta 1 Gbps, en aquellas situaciones en las que sea posible utilizar una red de área local como Wi-Fi para establecer dicha comunicación. El objetivo de esta nueva generación es por tanto el de garantizar una calidad de servicio y el cumplimiento de los requisitos mínimos para la transmisión de servicios de mensajería multimedia, video chat, TV móvil o servicios de voz y datos en cualquier momento y en cualquier lugar utilizando siempre el sistema que mejor servicio proporcione.

En esta cuarta generación las infraestructuras y los terminales implementaron todos los estándares desde el 2G hasta el 3G, aunque la estructura se basará sólo en paquetes IP.

Una de las tecnologías que más se ha desarrollado en esta cuarta generación de redes es WiMAX (Worlwide Interoperability for Microwave Access), cuyo significado en es español es Interoperabilidad Mundial para Acceso por Microondas. WiMAX es una tecnología de telecomunicaciones que provee comunicaciones inalámbricas de punto a punto y está basada en el estándar IEEE 802.16, totalmente IP, optimizada para altas velocidades y aplicaciones de datos en tiempo real. Esta tecnología está orientada a proveer acceso de banda ancha a nivel metropolitano en forma inalámbrica. La idea es permitir acceso inalámbrico a Internet desde un lugar fijo, compitiendo con ADSL (Asymmetric Digital Subscriber Line Línea de Abonado Digital Asimétrica) o cable MODEM o para usuarios móviles. Así, mientras Wi-Fi soporta transmisión en el rango de unos cientos de metros, los sistemas WiMAX soportan usuarios en el rango de 30 a 50 km.

Desde su lanzamiento y como cualquiera otra tecnología de redes, ha sido objeto de estudio por parte de grupos dedicados a la seguridad de estos estándares y no han tardado en aparecer sus vulnerabilidades. Pero la seguridad y la integridad de la información que se transmite a través de las redes inalámbricas han traído bastantes críticas porque, según apuntaban algunos expertos, podía interferir en otras redes de comunicación o exponerse a robo de datos. Sin embargo, este campo ha avanzado muy rápidamente y, actualmente, se puede decir que las redes inalámbricas alcanzan unos niveles de seguridad muy similares a las de cable.

Debido al avance tecnológico que existe en la Universidad de las Ciencias Informáticas, esta es la abanderada en nuestro país a realizar las pruebas para implantar la tecnología inalámbrica WiMAX [1]. Por lo que nuestra **Situación Problémica** es: no se conoce como asegurar la tecnología de redes inalámbricas WiMAX. Siendo el **problema científico** ¿Cómo proporcionar seguridad de las redes de WiMAX en la Universidad de las Ciencias Informáticas?

Teniendo como **campo de acción** la seguridad en la tecnología de redes WiMAX.

Nuestro **Objetivo principal** seria: investigar acerca de la seguridad en la tecnología WiMAX, para su implantación en la Universidad de las Ciencias Informáticas. Teniendo como **objetivos específicos:**

1. Investigar y profundizar sobre la seguridad en la tecnología WiMAX.
2. Investigar acerca de todos los aspectos de la seguridad y realizar comparaciones.
3. Realizar una propuesta de seguridad y validar esta propuesta.

Las **tareas a desarrollar** serian:

1. Investigar del desarrollo de las redes de cuarta generación en el mundo.
2. Investigar acerca de la seguridad en WiMAX.
3. Evaluar los protocolos de seguridad más usados en el mundo para esta tecnología.
4. Realizar comparaciones entre estos protocolos y llegar a una propuesta final de los más factibles para la implantación de la tecnología en la universidad.
5. Validar la propuesta.

Con este trabajo de diploma se pretende realizar una investigación detallada de la seguridad en las tecnologías de redes de cuarta generación, principalmente la tecnología WiMAX. Por lo que constara de tres capítulos el **Capítulo 1** abarcará el desarrollo de las redes de cuarta generación, su implantación en el mundo y se comentará acerca de otras tecnologías que son utilizadas en esta generación de redes. En el **Capítulo 2** se profundizará en la seguridad de la tecnología WiMAX y en el **Capítulo 3** se propondrán certificados, estándares y protocolos para la seguridad en la tecnología WiMAX que se desea implantar en la Universidad de las Ciencias Informáticas.

Capítulo 1 Fundamentación Teórica

1.1. Introducción

En este capítulo se realiza un estudio del estado del arte de las redes de cuarta generación y la tecnología WiMAX, el problema planteado y el marco teórico en el que se desarrolla. Se hace una descripción detallada de todos los conceptos y definiciones para un mejor entendimiento de este trabajo de diploma.

1.2. Conceptos vinculados al campo de acción.

Con el estudio de las redes de cuarta generación y la tecnología WiMAX se han encontrado algunos elementos y conceptos que se deben conocer sus características o significado para entender lo que se trata en el trabajo. En los siguientes puntos se situaran los más importantes para un mejor entendimiento de las tecnologías y redes de cuarta generación.

1.2.1. Redes de cuarta generación.

La 4G estará basada en el protocolo IP(Internet Protocol, Protocolo de Internet) siendo un sistema de sistemas y una red de redes, alcanzándose después de la convergencia entre las redes de cables e inalámbricas así como en ordenadores, dispositivos eléctricos y en tecnologías de la información así como con otras convergencias para proveer velocidades de acceso entre 100 Mbps en movimiento y 1 Gbps en reposo, manteniendo una calidad de servicio (QoS) de punta a punta (end-to-end) de alta seguridad para permitir ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible.

La cuarta generación estaría basada en IP con el objetivo de juntar todos los protocolos de nivel de transmisión en una única arquitectura de protocolos estandarizada, que puede ser utilizada por las aplicaciones para diferentes propósitos de comunicación. Como resultado cualquier aplicación que soporte TCP/IP también podrá comunicar sobre cualquier red basada en IP. En esta nueva generación se lograría una convergencia de todos estos servicios sobre el protocolo IP. Por ejemplo: en una empresa se lograrían que la televisión digital, telefonía e Internet lograrían sus transferencias a través de este protocolo (Siguiente figura).

Convergencia de servicios basados en IP

El WWRF define 4G como una red que funcione en la tecnología de Internet, combinándola con otros usos y tecnologías tales como Wi-Fi y WiMAX. La 4G es una colección de tecnologías y protocolos para permitir el máximo rendimiento de procesamiento con la red inalámbrica más barata. El IEEE aún no se ha pronunciado designando a la 4G como “más allá de la 3G”, debido que los pasos a la cuarta generación no han sido muy grandes sino que han sido versiones de la tercera generación. Ejemplo: 3.5, 3.9.

1.2.2. WiMAX

WiMAX son las siglas de 'Worldwide Interoperability for Microwave Access' (Interoperabilidad Mundial para Acceso por Microondas), y es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico 'IEEE 802.16'. Estos estándares permitirán conexiones de velocidades similares al ADSL o al cable módem, sin cables, y hasta una distancia de 50-60 km. Este nuevo estándar será compatible con otros anteriores, como el de Wi-Fi (IEEE 802.11). [2]

El impacto de esta nueva tecnología inalámbrica puede ser extraordinario ya que contiene una serie de elementos que van a favorecer su expansión: relativo bajo coste de implantación; gran alcance, de hasta 50 Km; velocidades de transmisión que pueden alcanzar los 75 Mbps; no necesita visión directa; disponible con criterios para voz como para video; y tecnología IP extremo a extremo. Además, dependiendo del ancho de banda del canal utilizado, una estación base puede soportar miles de usuarios, netamente superior al WLAN.

La tecnología WiMAX será la base de las Redes Metropolitanas de acceso a Internet, servirá de apoyo para facilitar las conexiones en zonas rurales, y se utilizará en el mundo empresarial para implementar las comunicaciones internas. Además, su popularización supondrá el despegue definitivo de otras tecnologías, como VoIP (llamadas de voz sobre el protocolo IP).

WiMAX funcionaría similar a Wi-Fi pero a velocidades más altas, mayores distancias y para un mayor número de usuarios. WiMAX podría solventar la carencia de acceso de banda ancha a las áreas suburbanas y rurales que las compañías del teléfono y cable todavía no ofrecen.

1.2.3. Wi-Fi

Wi-Fi, es la sigla para Wireless Fidelity (Wi-Fi), que literalmente significa Fidelidad inalámbrica. Es un conjunto de redes que no requieren de cables y que funcionan en base a ciertos protocolos previamente establecidos. Si bien fue creado para acceder a redes locales inalámbricas, hoy es muy frecuente que sea utilizado para establecer conexiones a Internet.

Wi-Fi es una marca de la compañía Wi-Fi Alliance que está a cargo de certificar que los equipos cumplan con la normativa vigente (que en el caso de esta tecnología es la IEEE 802.11). [3]

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuera compatible entre los distintos aparatos. En busca de esa compatibilidad fue que en 1999 las empresas 3com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se reunieron para crear la Wireless Ethernet Compability Aliance (WECA), actualmente llamada Wi-Fi Alliance.

Al año siguiente de su creación la WECA certificó que todos los aparatos que tengan el sello Wi-Fi serán compatibles entre sí ya que están de acuerdo con los criterios estipulados en el protocolo que establece la norma IEEE 802.11.

En concreto, esta tecnología permite a los usuarios establecer conexiones a Internet sin ningún tipo de cables y puede encontrarse en cualquier lugar que se haya establecido un "punto caliente" o hotspot Wi-Fi.

1.2.3.1. IEEE (Institute of Electrical and Electronics Engineers)

El Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática e ingenieros en telecomunicación. [4]

1.2.4. LTE (Long Term Evolution)

Es un nuevo estándar de la norma 3GPP (3rd Generation Partnership Project). Definida para unos como una evolución de la norma 3GPP UMTS (3G) para otros un nuevo concepto de arquitectura evolutiva (4G). De hecho LTE será la clave para el despegue del internet móvil, servicios como la transmisión de datos a más de 300M y videos de alta definición, gracias a la tecnología OFDMA (Orthogonal Frecuency Division Multiple Access, Acceso Múltiple por División de Frecuencia Ortogonal), serán de uso corriente en la fase madura del sistema.

La novedad de LTE es la interfaz radioeléctrica basada en OFDMA para el enlace descendente (DL) y SC-FDMA para el enlace ascendente (UL). La modulación elegida por el estándar 3GPP hace que las diferentes tecnologías de antenas (MIMO) tengan una facilidad de implementación, esto favorece según el medio de hasta cuadruplicar la eficacidad de transmisión de datos. [5]

Las mejoras a investigar son, por ejemplo, el aumento de la eficiencia, la reducción los costes, la ampliación y mejora de los servicios ya prestados y una mayor integración con los ya protocolos existentes.

1.2.4.1. OFDMA (Orthogonal Frecuency Division Multiple Access)

Es una versión multiusuario de la conocida multiplexación por división de frecuencias ortogonales. Se utiliza para conseguir que un conjunto de usuarios de un sistema de telecomunicaciones puedan compartir el espectro de un cierto canal para aplicaciones de baja velocidad. El acceso múltiple se

consigue dividiendo el canal en un conjunto de subportadoras que se reparten en grupos en función de la necesidad de cada uno de los usuarios. [6]

1.2.4.2. MIMO (Multiple-input Multiple-output)

En español, Múltiple entrada múltiple salida. Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores. En el formato de transmisión inalámbrica tradicional la señal se ve afectada por reflexiones, lo que ocasiona degradación o corrupción de la misma y por lo tanto pérdida de datos.

MIMO aprovecha fenómenos físicos como la propagación multicamino para incrementar la tasa de transmisión y reducir la tasa de error. En breves palabras MIMO aumenta la eficiencia espectral de un sistema de comunicación inalámbrica por medio de la utilización del dominio espacial.

Durante los últimos años la tecnología MIMO ha sido aclamada en las comunicaciones inalámbricas ya que aumenta significativamente la tasa de transferencia de información utilizando diferentes canales en la transmisión de datos o la multiplexación espacial por tener las antenas físicamente separadas.[7]

1.2.5. EVDO (Evolution Data Optimized)

EVDO es un acrónimo de "Evolution Data Optimized" o "Evolución de Datos Optimizados", que es un estándar para redes inalámbricas de alta velocidad utilizado para la conexión a Internet de banda ancha. EVDO permite a los usuarios de computadoras de alta velocidad de acceso a Internet sin la ayuda de un hotspot. Sólo mediante la inserción de una tarjeta EVDO en el ordenador, los usuarios conectarse a Internet en cuestión de segundos y tener velocidades de acceso a la red comparables con DSL.

Mientras que las redes inalámbricas tradicionales de asignar una ruta dedicada entre el origen y el destino para toda la duración de la llamada muy similar a la de línea fija redes telefónicas, EVDO transmite varios usuarios de datos a través de un único canal usando Code Division Multiple Access (CDMA), así como acceso múltiple por división de tiempo (TDMA) para lograr un mayor rendimiento y mejor utilización de ancho de banda de red.

La norma se sometió a numerosas revisiones denominado Rev. 0, Rev. A, Rev. B y así sucesivamente. Rev. 0 apoya adelante vínculo velocidades de hasta 2,4 Mbit / s. Rev. A, mientras que puede ir hasta

3,1 Mbit / s. EVDO es parte de la familia de normas CDMA2000 y ha sido adoptado por muchos proveedores de servicios ofrecer conectividad de banda ancha de alta velocidad para los usuarios de telefonía móvil a través de redes CDMA. Ha sido desarrollado por Qualcomm durante finales de los años 90. Dado que la norma era una evolución directa de la norma que llevó 1xRTT sólo los datos, en un principio se llama Evolución de datos solamente. Más tarde, ya que la palabra "sólo" parecía agregar una connotación negativa para el nombre, el nombre fue cambiado a la evolución de datos optimizada. Dado que el nuevo nombre era más comercial y sonaba más alta tecnología, que atascado.

EVDO utiliza la actual emisión de las frecuencias de las redes CDMA, que es una gran ventaja en comparación con las tecnologías competidoras, que a menudo exigen costosos equipos y programas informáticos a los cambios o actualizaciones de la red.

EvDO Rev B es la evolución progresiva de la especificación Rev A. Mantiene las capacidades de Rev A y provee las siguientes mejoras:

- Más velocidad en los enlaces de bajada (hasta 4.9 Mbit/s por operador). Implementaciones típicas incluyen tres operadores para un pico teórico máximo de 14.7 Mbit/s.
- Provee mayores tasas de transferencia compactando múltiples canales, mejora la experiencia de usuario y provee nuevos servicios como streaming para video de alta definición.
- Aprovecha más eficazmente el uso de la batería incrementando el tiempo de uso y de espera del terminal.
- Menos interferencias entre el usuario y la celda mediante la Reutilización Híbrida de la Frecuencia.
- Aumenta la eficiencia del soporte para servicios que tienen requerimientos asimétricos de transmisión como intercambio de archivos, navegación web y entrega de archivos multimedia por banda ancha.

1.2.6. Bluetooth

Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANS) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz). Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos.
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales.

Los dispositivos que con mayor intensidad utilizan esta tecnología son los de los sectores de las telecomunicaciones y la informática personal, como PDA´s, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras y cámaras digitales. [8]

1.3. Evolución de las redes inalámbricas.

Las primeras experiencias con redes inalámbricas datan de 1979 cuando científicos de IBM en Suiza despliegan la primera red de importancia con tecnología infrarroja. No es hasta 1985 cuando se comienzan los desarrollos comerciales de redes con esta filosofía, momento en el que el órgano regulador del espectro radioeléctrico americano, la FCC (Federal Communications Commission**,** Comisión Federal de las Comunicaciones), asigna un conjunto de estrechas bandas de frecuencia para libre uso en las bandas de los 2,4 y los 5 gigahercios. Inmediatamente, la asociación de ingenieros electrónicos, IEEE, designa una comisión de trabajo para desarrollar una tecnología de red en dichas bandas: la 802.11. A partir de ese momento se liberan una serie de estándares, el más reciente de los cuales es el IEEE 802.11g.

Las ventajas de las redes en estos rangos de frecuencias son claras: no requieren licencias, permisos ni necesidad de comunicación para su despliegue y pueden ser implantadas en cualquier ubicación. Como contrapartida surgen una serie de importantes inconvenientes: interferencias impredecibles con redes próximas por selección de frecuencias iguales o parcialmente solapadas, espectro empleado por otras aplicaciones (redes Bluetooth, usos domésticos como teléfonos inalámbricos, emisores de vídeo, mandos de control remoto...), potencia de emisión muy limitada que restringe mucho la cobertura y una banda de uso muy estrecha que permite delimitar muy pocos canales no interferentes.

Es evidente que la tecnología inalámbrica está suscitando no sólo el interés teórico de mercado, por las novedades tecnológicas que aporta, sino también interés práctico, ya que se le suponen crecimientos y cifras de negocio a los que la industria de Tecnologías de la Información ya no está acostumbrada.

Las redes inalámbricas están adquiriendo un éxito sin precedentes debido a una combinación de factores: una tecnología eficaz con el uso del espectro, muy orientada al despliegue de redes locales de pequeño tamaño, un entorno regulatorio que permite su libre uso, una lógica fácilmente integrable y de muy bajo coste, y una interoperabilidad de equipos generalmente exitosa. Sin embargo, la tecnología subyacente no es trivial, sino que ha requerido un estudio profundo de cómo obtener un uso muy eficiente de un rango escaso de frecuencias, cómo conseguir una amplia cobertura con potencias de emisión muy bajas, y todos los aspectos relacionados con la seguridad de las comunicaciones. Es importante entender las bases sobre las que se sustenta para entender sus grandes ventajas y sus inconvenientes. Aunque fue lenta su evolución al principio las redes inalámbricas avanzan rápidamente, a continuación se verá la evolución de una de estas tecnologías inalámbricas.

1.4. Creación de Wi-Fi.

Cualquier red inalámbrica se basa en la transmisión de datos mediante ondas electromagnéticas, según la capacidad de la red y del tipo de onda utilizada se habla de una u otra red inalámbrica.

Wi-Fi es una de ellas, en este caso el alcance de la red es bastante limitado por lo que se utiliza a nivel doméstico y oficina. Por eso mismo es la más popular ya que muchos usuarios se han decidido por eliminar los cables que le permiten la conexión Internet. De manera que es posible conectarse a la red desde cualquier lugar de la casa.

Los inicios de cualquier descubriendo suelen ser difíciles y uno de los principales problemas a los que se enfrenta es la implantación de un estándar. Por ello los principales fabricantes de redes inalámbricas decidieron asociarse para definir los estándares y facilitar la integración en el mercado de las redes inalámbricas.

Nokia, 3com, Airones, Intersil, Lucent Technologies y Symbol Technologies eran los principales vendedores de soluciones inalámbricas en los años 90. En 1999 se asociaron bajo el nombre de WECA, Wireles Ethernet Compability Aliance, Alianza de Compatibilidad Ethernet Inalámbrica. Desde el 2003 el nombre de esta asociación es Wí-Fi Alliance y ahora comprende más de 150 empresas.

Wí-Fi Alliance se encarga de adoptar, probar y certificar que los equipos cumplen con los estándares que han fijado. Su objetivo siempre ha sido crear una marca que fomentase la tecnología inalámbrica y que asegurase la compatibilidad entre equipos.

En el 2000, tan solo un año después de su formación, la que aun se denominaba WECA acepta como estándar la norma IEEE 802.11b. El nombre era muy poco comercial así que la asociación contrata a la empresa de publicidad Interbrand para que cree un nombre mucho más fácil de recordar, algo corto y simple. Las propuestas son varias: “Prozac”, “Compaq”, “Oneworld”, “Imation” y, evidentemente, “Wi-Fi” la abreviación de Wíreles Fidelity.

Wi-Fi (802.11) fue creado para sustituir a las capas físicas y MAC de Ethernet (802.3). En otras palabras, Wi-Fi y Ethernet son redes iguales que se diferencian en el modo en que el ordenador o terminal accede a la red, Ethernet mediante cable y Wi-Fi mediante ondas electromagnéticas. Esta característica las hace compatibles.

Es importante resaltar que Wi-Fi no es una marca, es el nombre de un estándar. Esto quiere decir que todos los equipos con el sello Wi-Fi pueden trabajar juntos independientemente del fabricante que haya creado la red o el ordenador. Así pues si una oficina posee computadores de diferentes marcas pero todos ellos disponen de Wi-Fi se podrá conectar entre sí sin problemas.

Actualmente Wi-Fi es, sobre todo, conocido como herramienta para acceder a Internet pero lo cierto es que se diseñó como red inalámbrica local, para conectar a corta distancia varios dispositivos entre sí. Conviene no olvidar esta utilidad, pues aunque esté menos difundida puede aportar al usuario muchas facilidades y posibilidades.

1.5. Cuarta Generación en el mundo.

Basándose en el éxito de las pruebas realizadas con la tecnología WiMAX en todo el mundo, las operadoras han comenzado a realizar despliegues comerciales de este tipo de redes, tanto en ciudades como en zonas suburbanas y rurales, para permitir a las operadoras ofrecer servicios de banda ancha a través de redes inalámbricas en lugares donde, hasta ahora, resultaba imposible o muy caro para las operadoras ofrecer este tipo de servicio.

En colaboración con Intel, y utilizando equipos basados en la interfaz de banda ancha Intel® PRO/Wireless 5116, han instalado ya redes comerciales operadoras como: Altitude Telecom* (Francia), AXTEL* (México), BEC Telecom, S.A.* (República Dominicana), Dedicado* (Uruguay), Globe/Innove* (Filipinas), Iberbanda (España), Irish Broadband* (Irlanda), SferaNET* (Polonia), Mikkelin Puhelin Oyj* y

Savonlinnan Puhelin Oy* (Finlandia), Telgua* (Guatemala), Ukrainian High Technologies* (Ucrania), y WiMAX Telecom* (Austria y Eslovaquia).

Estas instalaciones ofrecen soporte a diversos servicios, que van desde el acceso básico de alta velocidad para los hogares, a la telefonía por Internet, la conectividad empresarial y el apoyo a escuelas y oficinas gubernamentales. De esta forma, y como ejemplo:

- BEC Telecom va a ofrecer servicios de Voz sobre IP (VoIP) en la República Dominicana, comenzando en Santo Domingo, y ampliándolos posteriormente al resto del país, mientras que WiMAX Telecom va a ofrecer servicios de VoIP a los usuarios domésticos de Burganland, Austria.

- Los usuarios de pequeñas empresas y áreas residenciales tienen ahora acceso a Internet de alta velocidad gracias a los servicios que les ofrecen AXTEL en Monterey, México; y Dedicado en Montevideo, Uruguay, o los que proporcionan Globe/Innove en Cavite, Filipinas, e Iberbanda en Andalucía y Cataluña, España.

- Los colegios y las oficinas gubernamentales se pueden beneficiar ahora del acceso rentable y de alta velocidad en zonas como, por ejemplo, Dublín, en Irlanda, que cuenta con un contrato con Irish Broadband, o el Sur de Polonia, en donde SferaNet ofrece servicios WiMAX a oficinas gubernamentales locales, agencias públicas para seguridad y colegios.

Otras operadora que han instalado redes WIMAX son: Americatel Perú S.A.* (Perú), Call Plus* (Nueva Zelanda), Chunghwa Telecom Co. Ltd.* (Taiwán), DBD Deutsched Breitband Dienste GmbH* (Alemania), Digicel* (El Caribe), Entel* (Chile), Ertach* (Argentina), Integrated Telecom Company* (Arabia Saudí), Next Mobile* (Filipinas), Taiwan Fixed Networks* (Taiwán) y VeloCom* (Argentina).

Según las estimaciones el número de los suscriptores a servicios Móviles WIMAX será de 80 millones en todo el mundo en 2013. Japón, Corea del Sur y Estados Unidos serán los líderes del sector, aunque cerca de 40 millones de esos suscriptores se encontrarán en la región asiática.

Se señala que a tecnología WiMAX está preparada para una implementación rápida en zonas como India, Corea, Paquistán o Australia. Además, los programas gubernamentales de países como Taiwán impulsarán este crecimiento, que llevará el segmento a unas ventas de 23.000 millones de dólares en 2013,

Analista estiman que “el uso del WiMAX Móvil se desarrollará después de la demanda inicial de servicios fijos y portátiles. 802.16e es una plataforma flexible que puede operar en tres modelos de uso.”

Los 80 millones de usuarios que se esperan en 2013 podrían ser más si la plataforma es integrada en dispositivos como portátiles de bajo coste, reproductores de música y consolas de videojuegos. La disponibilidad de estos dispositivos y la adjudicación de licencias son dos factores fundamentales en la expansión de la tecnología WiMAX.

El continente africano no se ha quedado al margen de las tecnologías de cuarta generación pues existen convenios para implantar redes WiMAX en varios países como son los casos de:

En África Oriental se anunció que se va a poner en marcha una red WiMAX. Hay una gran necesidad insatisfecha de muy alta velocidad de acceso a Internet y WiMAX es una solución avanzada, diseñada para satisfacer esta necesidad, y hacerlo en un bajo costo y flexible. El caso de Uganda que el gobierno ha proporcionado presupuesto para poder llevar a cabo la implantación de WiMAX.

Hay tres zonas del mundo en las que está prosperando el WiMAX: Corea (avanzada de todo lo que tiene que ver con banda ancha), África del Sur (porque es un medio barato de crear infraestructuras allí donde no las había) y América Latina. En este último caso, se mezclan la carencia de buenas conexiones con la ambición de los operadores. Así como en Europa y EE.UU. el uso del WiMAX se reduce por ahora a las zonas rurales, en América Latina ya hay compañías dispuestas a extender el servicio a núcleos urbanos como vía de entrada en el negocio de la banda ancha. Y es que el ADSL o el cable, aunque disponibles en las grandes ciudades, son demasiado caros para el ciudadano medio de estos países. Así que las consultoras ya andan haciendo estudios. Una de ellas, Maravedis, calcula que este año habrá 273.460 usuarios de WiMAX en América Latina, por 2,5 millones para 2012. El país más desarrollado será, sin duda, Brasil, donde apenas el 12% de la población usa Internet. Pese a que su población es casi tres veces superior a la española, el país carioca tiene menos clientes de banda ancha.

Los mercados de banda ancha en América Latina están entrando en una etapa madura en cuanto a la tecnología WiMAX, con casi 12 millones de suscriptores en los cinco principales mercados - Argentina, Brasil, Chile, Colombia, y México. En comparación, el número de suscriptores de WiMAX en la región no superan unos pocos miles. En vista de esto, se espera que WiMAX crezca a una tasa muy atractiva.

Según el análisis de Frost & Sullivan revela que este mercado se compuso de 20.700 suscriptores en el año 2006 y las estimaciones para el año 2012 estarían aproximadamente en unos 1.234.900 suscriptores.

“Los operadores cada vez recurren al WiMAX, ya que reduce significativamente el costo del despliegue de una red de banda ancha, ya sea para ampliar su capacidad o para llegar a las zonas más alejadas”, señala Ignacio Perrone, Jefe de Equipo de Servicios para el grupo Telecom.

Para los operadores, WiMAX puede ser una gran oportunidad para superar los problemas de distribución, que es la barrera de entrada al mercado. WiMAX ofrece la posibilidad de llegar a un gran número de clientes sin tener que invertir en costosas infraestructuras.

WiMAX implica una visión a largo plazo para los operadores de telefonía móvil y la principal razón para un operador móvil en interesarse en esta tecnología es prepararse para ofrecer Voz sobre Protocolo de Internet (VoIP), que es una tendencia inevitable.

En Brasil, el órgano regulador Anatel probablemente abra un proceso de licitación para distribuir las nuevas frecuencias de WiMAX para empresas de telecomunicaciones. Argentina es el país que cuenta con los elementos más favorables para el despliegue del WiMAX. Este mercado se divide en dos proveedores; Telecom Argentina (propiedad de Telecom Italia), que es responsable de la parte norte del país, y Telefónica, del sur. Actualmente, el reglamento de telecomunicaciones del país no permite la desagregación, lo que hace la entrada de nuevos competidores sea muy costosa.

En nuestro país también se quiere implementar WiMAX y esto lo posibilitara la empresa china Huawei con una tecnología que proporciona velocidades de hasta tres megabits por segundo a si uno se encuentra a distancias de hasta 5 Km de la radio base y además consume muy poca energía eléctrica, esta tecnología permite hasta 6000 usuarios en una radio base lo cual podría impulsar el proceso de expansión telefónica que se ejecuta en Cuba a partir de la instalación de al menos uno de estos equipamientos por provincia en el futuro inmediato. En nuestra universidad existe un proyecto aprobado para implantar estas tecnologías de 4G que no se ha podido llevar a cabo por falta de presupuesto.

1.6. Conclusiones del capítulo

Dentro del amplio mundo de las comunicaciones inalámbricas y la tecnología móvil las redes inalámbricas van ganando terreno demostrando ser una tecnología capaz de resolver muchos de los

inconvenientes que tiene el cable como medio físico de enlace en las comunicaciones, muchas de ellas de vital importancia en nuestra vida cotidiana. En este capítulo se examinó la mayoría de los conceptos relacionados con las redes inalámbricas de la tercera y cuarta generación de redes. Se observa el porqué se escoge la tecnología WiMAX para su implantación en la Universidad de las Ciencias Informáticas. En este capítulo se ilustraron además los logros a nivel mundial que ha tenido la tecnología WiMAX.

Capítulo 2 Seguridad en WiMAX

2.1. WiMAX

WiMAX es una especificación para redes metropolitanas inalámbrica (WMAN) de banda ancha, cuyos dos miembros más representativos son Intel y Nokia. Como sucedió con la marca Wi-Fi, que garantiza la interoperabilidad entre distintos equipos la etiqueta WiMAX es asociado globalmente con el propio nombre del estándar.

WiMAX es la próxima generación de tecnología inalámbrica diseñada para permitir que generalizada, de alta velocidad móvil de acceso a Internet a la más amplia gama de dispositivos portátiles incluidos, teléfonos móviles, smartphones, y la electrónica de consumo, como dispositivos de juego, cámaras, videocámaras, reproductores de música, y más. En la cuarta generación (4G) de la tecnología inalámbrica, WiMAX ofrece a bajo costo, las redes abiertas y es la primera solución de Internet móvil de propiedad intelectual que permite eficiente y escalable de redes de datos, vídeo y voz. Como uno de los principales impulsores en el apoyo y el desarrollo de WiMAX, Intel ha diseñado soluciones WiMAX incorporados para una variedad de dispositivos móviles apoyar el futuro de la banda ancha de alta velocidad On-The-Go. Por ser una tecnología inalámbrica no se confía mucho en su seguridad, en el próximo epígrafe se demostrara que no hay de que temer.

En la tabla de a continuación le presentamos una tabla con las características de esta tecnología.

Características	Descripción
Sin Línea de Vista (NLOS)	No necesita línea de visión entre la antena y el equipo del suscriptor.
Modulación OFDM (*Orthogonal Frequency Division Multiplexing*)	Permite la transmisión simultánea de múltiples señales a través de cable o aire en diversas frecuencias; usa espaciamiento ortogonal de las frecuencias para prevenir interferencias.
Antenas inteligentes	Soporta mecanismos de mejora de eficacia espectral en redes inalámbricas y diversidad de antenas
Topología punto-multipunto y de malla (*mesh*)	Soporta dos topologías de red, servicio de distribución multipunto y la malla para comunicación entre suscriptores.
Calidad de Servicio (QoS)	Califica la operación NLOS sin que la señal se distorsione severamente por la existencia de edificios,

	por las condiciones climáticas ni el movimiento vehicular.
FDM (*Frequency Division Multiplexing*) y TDM (*Time Division Multiplexing*)	Tipos de multiplexaje que soporta para propiciar la interoperabilidad con sistemas celulares (FDM) e inalámbricos (TDM).
Seguridad	Incluye medidas de privacidad y criptografía inherentes en el protocolo. El estándar 802.16 agrega autenticación de instrumentos con certificados x.509 usando DES en modo CBC (*CipherBlockChaining*).
Bandas bajo licencia	Opera en banda licenciada en 2.4 GHz y 3.5 GHz para transmisiones externas en largas distancias
Bandas libres (sin licencia)	Opera en banda libre en 5.8, 8 y 10.5 GHz (con variaciones según espectro libre de cada país)
Canalización	De 5 y 10 MHz
Codificación	Adaptiva
Modulación	Adaptiva
Ecualización	Adaptiva
Potencia de Transmisión	Controla la potencia de transmisión
Acceso al Medio	Mediante TDMA dinámico
Corrección de errores	ARQ (retransmisión inalámbrica)
Tamaño del paquete	Ajuste dinámico del tamaño del paquete
Aprovisionamiento	Aprovisionamiento dinámico de usuarios mediante DHCP y TFTP
Tasa de transmisión	Hasta 75 Mbps
Espectro de frecuencia	• IEEE 802.16a entre 2-11 GHz (LOS) para comunicación entre antenas • IEEE 802.16b entre 5-6 GHz con QoS • IEEE 802.16c entre 10-66 GHz • IEEE 802.16e entre 2-6 GHz (NLOS) para distribución a suscriptores, móvil.
Alcance	• 50 Km con Linea de vista • 20 Km sin Línea de Vista

	• 4- 6 Km en áreas de alta densidad demográfica
Aplicaciones	Voz, video y datos

2.2. Seguridad en WiMAX.

La seguridad es un aspecto que cobra especial relevancia cuando se habla 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 se tienen que tener en cuenta para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Las dudas sobre la seguridad han sido el principal freno tanto para los operadores como para los usuarios empresariales a la hora de realizar mayores inversiones y acometer proyectos Wi-Fi o de radio de gran envergadura. Tanto si se trata de algo real o percibido, lo que sí es un hecho es que los riesgos de seguridad de las soluciones wireless LAN están todavía lastrando los despliegues de las mismas. Hay que ser consciente y darse cuenta del punto de estancamiento que la seguridad ha sido en la adopción general tanto de los servicios inalámbricos de banda ancha propietarios como de los de Wi-Fi, lo que ha llevado a que el IEEE y el WiMAX Forum estén trabajando en la definición de un entorno de seguridad robusto y consolidado, que ofrezca plena confianza a los usuarios.

La tecnología WiMAX está diseñada teniendo en cuenta las cuestiones relacionadas con la seguridad, y ofrece una protección más sólida mediante la encriptación basada en certificados.

Desde que los sistemas WiMAX utilizan el interface radio como medio de transmisión, la pregunta que conviene hacerse es cómo prevenir que los intrusos no intercepten información sensible y confidencial transmitida por ondas hertzianas (electromagnéticas) ya sea en banda libre o banda licenciada.

La tecnología WiMAX requiere de las mejores características de seguridad en su clase, lograda gracias a la adopción de las mejores tecnologías disponibles actualmente. Las características de seguridad son independientes al tipo de operador y a la topología de la red de acceso. En este sentido, el estándar aborda las cuatro áreas principales a tener en cuenta.

2.2.1. Evitar el uso clandestino de la conexión wireless.

Esto se logra a través del cifrado, ofreciendo una protección sólida mediante la implementación de los protocolos 3DES de 128 bits, AES de 192 bits y RSA de 1024 bits, estableciendo la autenticación de usuarios y el cifrado de datos.

2.2.1.1. Protocolo TDES ó 3DES (Triple Digital Encryption Standard, Estándar de cifrado digital triple)

- **Algoritmo**

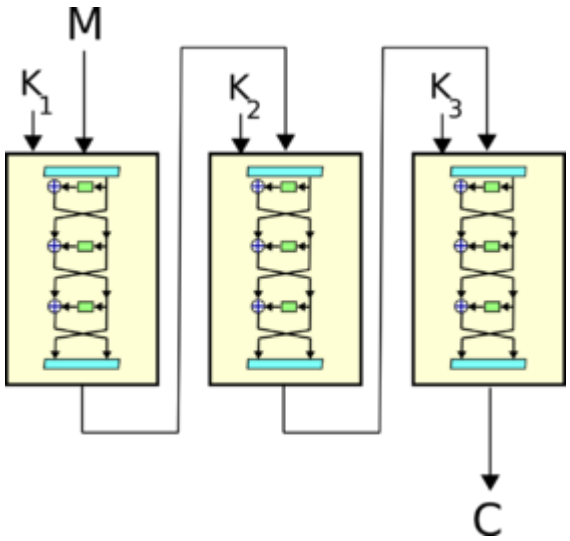


Figura 1 Como trabaja 3DES

No llega a ser un cifrado múltiple, porque no son independientes todas las subclases. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos claves diferentes se aumenta el tamaño efectivo de la clave. [9]

La variante más simple del Triple DES funciona de la siguiente manera:

$$C = E_{DES}^{k_3}\left(D_{DES}^{k_2}\left(E_{DES}^{k_1}(M)\right)\right)$$

Donde *M* es el mensaje a cifrar y k_1, k_2 y k_3 las respectivas claves DES.

- **Seguridad**

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, TDES fue elegido como forma de agrandar el largo de la clave sin necesidad de cambiar de algoritmo de cifrado. Este método de cifrado es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave (112 bits), pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES. Por tanto, la longitud de la clave usada será de 192 bits, aunque como se ha dicho su eficacia solo sea de 112 bits.

- **Usos**

El Triple DES está desapareciendo lentamente, siendo reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjeta de crédito y otros medios de pago electrónico tienen como estándar el algoritmo Triple DES (anteriormente usaban el DES). Por el diseño DES y por lo tanto TDES son algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y hasta el día de la fecha no se encontró ninguna vulnerabilidad.

2.2.1.2. Protocolo AES (Advanced Encryption Estándar, Estándar de cifrado avanzado)

El algoritmo Rijndael fue elegido por el NIST (National Institute of Standards and Technology), para ser el estándar en los próximos 20 años y es llamado AES (Advanced Encryption Standar). Rijndael fue elegido después de pasar un periodo de análisis durante aproximadamente 3 años, Rijndael fue elegido como la mejor opción dentro de 15 candidatos, sus principales características fueron su fácil diseño, su

versatilidad en ser implementado en diferentes dispositivos, así como ser inmune a los ataques conocidos hasta la fecha, soportar bloques de datos de 128 bits y claves de 128, 192, y 256 bits. La idea básica general es tener un estándar que mejore el “performance” de TDES y sea resistente a los ataques conocidos. [10]

El aspecto más importante de un algoritmo es su seguridad, sin embargo, la seguridad no es algo fácil de manejar. Un algoritmo es seguro si éste está diseñado para soportar todos los ataques conocidos hasta el momento y da la suficiente evidencia de su fortaleza. Aunque es claro que siempre existe la posibilidad de que el algoritmo pueda ser roto por recientes y novedosos ataques, es decir, es imposible diseñar un algoritmo inmune a taques no conocidos.

Las principales características que un algoritmo criptográfico simétrico debe tener son:

1. La no linealidad entre las entradas y las salidas, o la correlación de las entradas con las salidas.
2. La propagación de las diferencias de los bits, o el medir la probabilidad de que tanto se confunden los bits.

Particularmente las anteriores características son las más requeridas en un algoritmo simétrico, en el diseño las dos se mezclan y se miden en cada una de las rondas que consiste el algoritmo, es decir, en términos muy generales y básicos si un algoritmo tiene esas dos propiedades y se realizan las suficientes rondas, entonces el algoritmo será inmune a los análisis lineal y diferencial.

A continuación se explican las dos características anteriores de la forma más sencilla posible:

1. Linealidad

En términos elementales por ejemplo si las entradas de nuestro algoritmo son 1, 2, 3, 4, y 5 y se tiene como salidas 2, 4, 6, 8, y 10, claramente hay una dependencia lineal entre las entradas y las salidas, es decir $f(x)=2g(x)$ donde f, g son las funciones de entrada y salida correspondientemente. El método conocido como correlación es el que se aplica a dos conjuntos de datos A, B y determina que tanto puede haber uno del otro una dependencia lineal. De tal modo que si existe una relación lineal entre las entradas de las salidas, no es nada difícil conocer la información de los textos originales o de la clave de cifrado. Claramente la linealidad no es una propiedad que se quiera en un algoritmo criptográfico.

El mecanismo que impide que haya correlación es el alternar las claves, es decir que para cada ronda de nuestro algoritmo se aplique una clave diferente, esto se logra en términos generales implementado un programa de claves que proporciona una clave diferente para cada ronda. Esto permite disminuir la linealidad en la mayoría de las modalidades que pueda pensarse como una debilidad de nuestro algoritmo, y es aprovechada principalmente por el criptoanálisis lineal.

2. Propagación

El otro concepto muy trabajado en una algoritmo simétrico es la propagación, este concepto hay que trabajarlo de la manera más cuidadosa, el que el algoritmo tenga buena "propagación" impide que sea aplicado principalmente el criptoanálisis diferencial que es un ataque del tipo "Chosen Plaintext Attack" y permite derivar información de la clave a partir de conocer las probabilidades de las diferencias de la propagación, por lo que estas probabilidades deben de ser lo más pequeño posible. La propagación se obtiene con el programa de claves, con la propagación de la función no lineal del algoritmo (S-Box) y el número de rondas.

Por otra parte otro tipo de ataques o conceptos de debilidad que han sido propuestos, Rijndael los evita, como "Square Attack", "Six Round Attack", "Herds Attack", "Gilbert-Minier Attack", "Interpolation attack", "Related- Key Attack", "Timing Attack", "Imposible Differential attack", "Collision attack", últimamente se han propuesto los llamados ataques algebraicos que en general explotan las propiedades algebraicas del algoritmo. Sin embargo por el momento no se ha podido montar un ataque a la versión completa de Rijndael, lo que lo hace tan seguro como una búsqueda exhaustiva.

- **Como opera AES**

El proceso consiste en una serie de cuatro transformaciones matemáticas, las cuales se repiten 10, 12 o 14 veces, dependiendo de la longitud del bloque y de la longitud de la clave. Modifica bloques de 128 bits representados en una matriz de 4×4 bytes, que llama *estado.* Cada ronda (excepto la última) consiste en cuatro pasos:

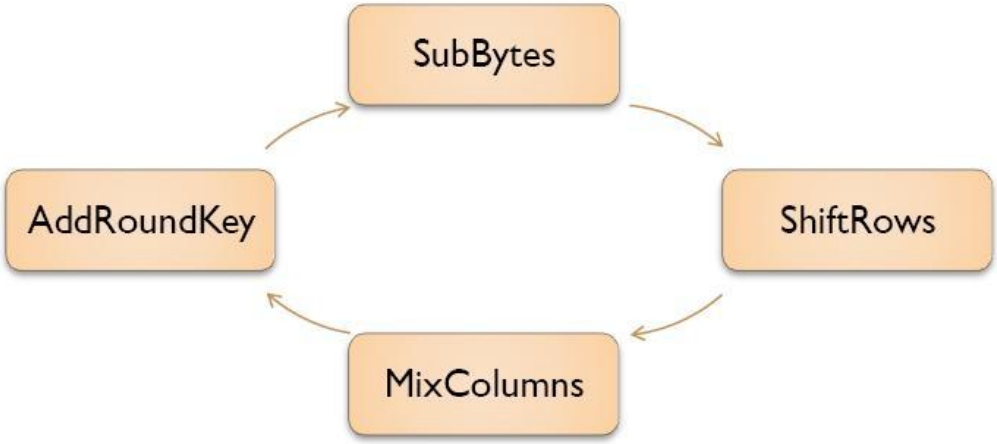


Figura 2 Funcionamiento de AES

SubBytes = Sustitución de bits.

ShiftRows = Desplazamiento de filas.

MixColumns = Mezcla de columnas.

AddRoundKey = Calculo de subclaves.

La ronda final reemplaza la fase MixColumnspor otra instancia de AddRoundKey.

1. SubBytes-Sustitución de bits: Sustitución no lineal donde cada byte del estado es reemplazado con otro según una tabla:

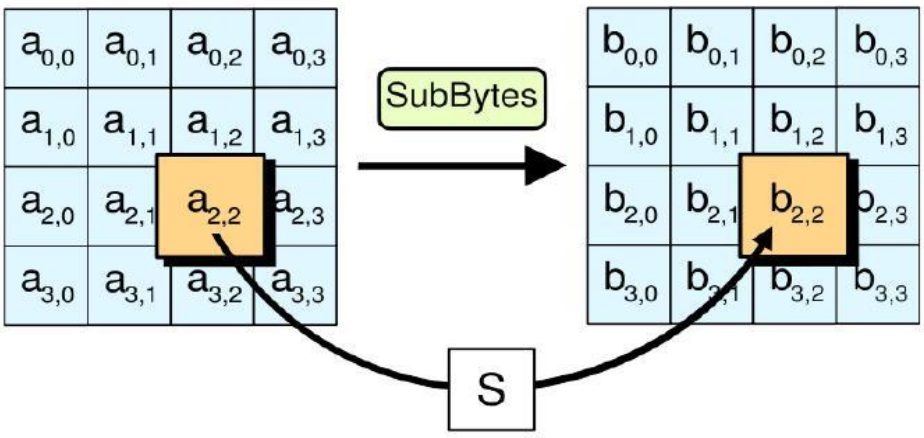


Figura 3 Sustitución de bits

2. ShiftRows–Desplazamiento de filas: Los bytes de cada fila del estado se rotan de manera cíclica hacia la izquierda un número de lugares diferente para cada fila.

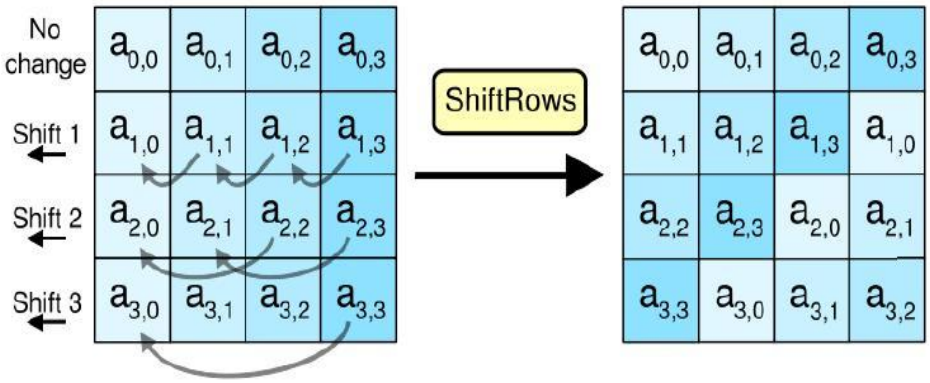


Figura 4 Desplazamiento de filas

3. MixColumns–Mezcla de columnas: Cada columna del estado se multiplica por un polinomio constante c(x). Así se mezclan los 4 bytes de la columna con una transformación lineal.

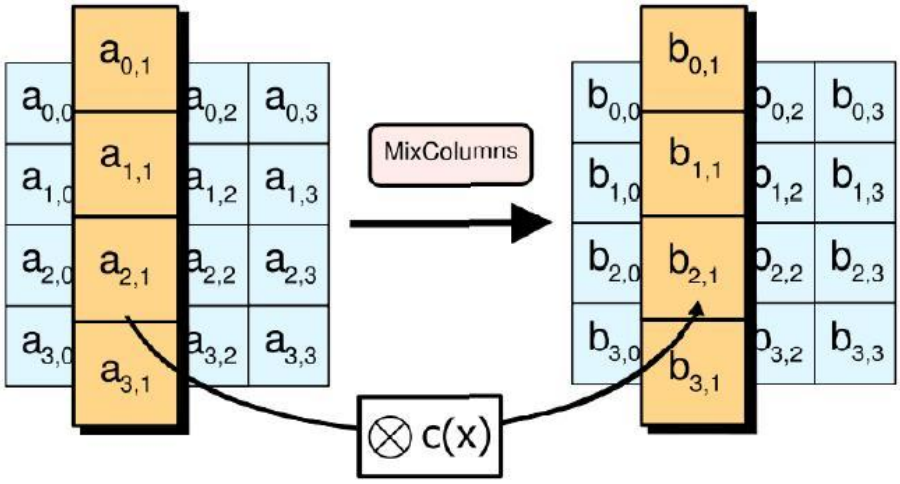


Figura 5 Mezcla de columnas

4. AddRoundKey-Cálculo de las subclaves: Cada byte del estado se combina mediante XOR con una subclave. Las subclaves se derivan de la clave de cifrado usando un proceso iterativo.

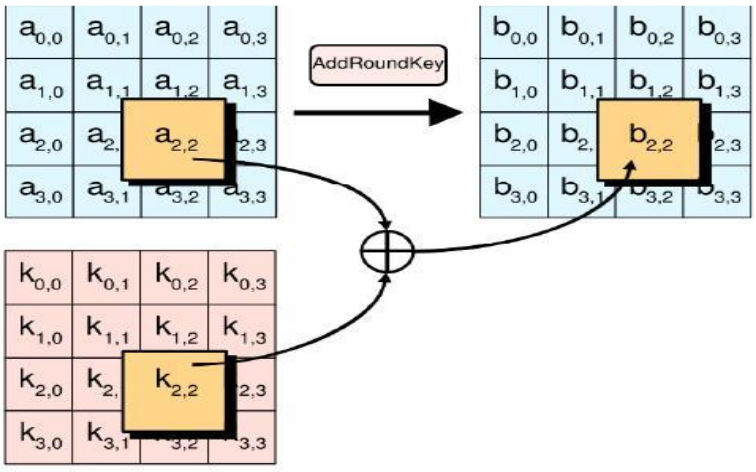


Figura 6 Cálculo de las subclaves

2.2.1.3. Protocolo RSA

- **Historia**

El algoritmo fue descrito en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT; las letras RSA son las iniciales de sus apellidos. Fue inventado en Schenectady (estado de Nueva York). Clifford Cocks, un matemático británico trabajando para la agencia de inteligencia británica GCHQ describió un sistema equivalente en un documento interno en 1973. Debido a la lentitud de la implementación en las computadoras de la época, se lo consideró una curiosidad. Su descubrimiento sin embargo no fue revelado hasta 1997 ya que era confidencial.

El algoritmo fue patentado por el MIT en 1983 en Estados Unidos con el número 4.405.829. Esta patente expiró el 21 de septiembre de 2000. Como el algoritmo fue publicado antes de patentar la aplicación, esto impidió que se pudiera patentar en otros lugares del mundo. Como Cocks trabajó en un organismo gubernamental, una patente en Estados Unidos tampoco habría sido posible.

- **Cifrado de mensajes**

Ejemplo rápido: B quiere enviar a A un mensaje secreto que solo A pueda leer.

A envía a B una caja con una cerradura abierta, de la que solo A tiene la llave. B recibe la caja, escribe el mensaje, lo pone en la caja y la cierra con su cerradura (ahora B no puede leer el mensaje). B envía

la caja a A y ella la abre con su llave. En este ejemplo, la caja con la cerradura es la clave pública de A, y la llave de la cerradura es su clave privada.

Se supone que B desea enviar un mensaje M a A. Él cambia M en un número m<n, usando un protocolo reversible conocido como padding scheme.

$$c \equiv m^e \pmod{n}$$

B ahora tiene m, y conoce n y e, mientras A fue avisado. B entonces calcula el texto cifrado c correspondiente a m: Esto puede ser rápido usando el método de exponenciación binaria (exponentiation by squaring). B transmite c a A.

1. Cada usuario elige n = p·q

2. Los valores p y q NO se hacen públicos

3. Cada usuario calcula ϕ(n) = (p-1) (q-1)

4. Cada usuario elige una clave pública e de forma que 1 < e < ϕ(n) y que cumpla con la condición: mcd [e, ϕ(n)] = 1

5. Cada usuario calcula la clave privada d = inv [e, ϕ(n)]

6. Se hace público el grupo n y la clave e

7. Se guarda en secreto la clave d

Cifra: C = NeR mod nR

Firma: C = h (M) dE mod nE

- **Ejemplo**

Aquí se muestra un ejemplo de cifrado/descifrado con RSA. Los parámetros usados aquí son pequeños y orientativos con respecto a los que maneja el algoritmo, pero se puede usar también OpenSSL para generar y examinar una par de claves reales.

p=61 1º nº primo Privado

q=53 2º nº primo Privado

n=pq=3233 producto p*q

e=17 exponente Público

d=2753 exponente Privado

La clave pública (e, n). La clave privada es d. La función de cifrado es:

encrypt(m) = m^e(mod n) = m^{17}(mod 3233)

Donde m es el texto sin cifrar La función de descifrado es:

decrypt(c) = c^d(mod n) = c^{2753}(mod 3233)

Donde c es el texto cifrado. Para cifrar el valor del texto sin cifrar 123, se calculó:

encrypt(123) = 123^{17}(mod 3233) = 855

Para descifrar el valor del texto cifrado, se calculó:

decrypt (855) = 855^{2753}(mod 3233) = 123

Ambos de estos cálculos pueden ser eficientemente usados por el algoritmo de multiplicación cuadrática para exponenciación modular.

- **Padding schemes (Esquema de relleno)**

RSA debe ser combinado con alguna versión del padding scheme, ya que si no el valor de M puede llevar a textos cifrados inseguros. RSA usado sin padding scheme podría sufrir muchos problemas.

- El valor m=0 o m=1 siempre produce textos cifrados iguales para 0 o 1 respectivamente, debido a propiedades de los exponentes.
- Cuando se cifra con exponentes pequeños (e=3) y valores pequeños de m, el resultado de m podría ser estrictamente menor que el módulo de n. En este caso, el texto cifrado podría ser fácilmente descifrado, tomando la raíz e-ésima del texto cifrado sin tener en cuenta el módulo.

- Dado que el cifrado RSA es un algoritmo determinista (no tiene componentes aleatorios) un atacante puede lanzar con éxito un ataque de texto elegido contra el criptosistema, construyendo un diccionario de textos probables con la llave pública, y almacenando el resultado cifrado. Observando los textos cifrados en un canal de comunicación, el atacante puede usar este diccionario para descifrar el contenido del mensaje.

En la práctica, el primero de los dos problemas podría presentarse cuando se envía pequeños mensajes ASCII donde m es la concatenación de uno o más carácter/es ASCII codificado/s. Un mensaje consiste en un solo carácter ASCII NUL (cuyo valor es 0) se codificaría como m=0, produciendo un texto cifrado de 0 sin importar qué valores de e y N son usados. Probablemente, un solo ASCII SOH (cuyo valor es 1) produciría siempre un texto cifrado de 1. Para sistemas convencionales al usar valores pequeños de e, como 3, un solo carácter ASCII mensaje codificado usando este esquema sería inseguro, ya que el máximo valor de m sería 255, y 255^3 es menor que cualquier módulo razonable. De esta manera los textos sin cifrar podrían ser recuperados simplemente tomando la raíz cúbica del texto cifrado. Para evitar estos problemas, la implementación práctica del RSA se ayuda de algunas estructuras, uso del randomized padding dentro del valor de m antes del cifrado. Esta técnica asegura que m no caerá en el rango de textos sin cifrar inseguros, y que dado un mensaje, una vez que este rellenado, cifrará uno de los números grandes de los posibles textos cifrados. La última característica es la incrementación del diccionario haciendo este intratable a la hora de realizar un ataque.

Estándares como PKCS han sido cuidadosamente diseñados para la seguridad de los de mensajes importantes con el cifrado RSA. Porque el pad scheme rellena el texto sin cifrar m con algunos números adicionales (bits); el tamaño del mensaje un-padded M debe ser algo más pequeño. RSA-padding scheme debe ser cuidadosamente diseñado así como para prevenir ataques sofisticados los cuales podrían ser facilitados por la predictibilidad de la estructura del mensaje. Versiones más recientes del PKCS Standard usando construcciones ad-hoc, las cuales fueron encontradas vulnerabilidades más tarde en la práctica adaptativa de elección de ataques de textos cifrados. Las construcciones modernas usan técnicas seguras como Optimal Asymetric Encryption Padding (OAEP) para proteger los mensajes mientras previenen estos ataques. El PKCS estándar también incorpora procesado de esquemas diseñados para proveer adicionalmente la seguridad de autentificaciones RSA. Por ejemplo: la Probabilistic Signature Scheme para RSA (RSA-PSS).

- **Autenticación de mensajes**

RSA puede también ser usado para autenticar un mensaje. Se supone que A desea enviar un mensaje autentificado a B. Ella produce un valor hash del mensaje, aumenta la potencia de d≡ mod n (como ella hace cuando descifra mensajes), y marca con una "firma" el mensaje. Cuando B recibe el mensaje autentificado, él aumenta la autentificación para aumentar e≡ mod n (como hace él cuando cifra menajes), y compara el resultado hash con el actual valor hash del mensaje. Si es el resultado, el conoce que el autor del mensaje estaba en posesión de la clave secreta de A, y que el mensaje no ha sido tratado de forzar entonces (no ha sufrido ataques).

Observar que la seguridad de padding-scheme como RSA-PSS es esencial para la seguridad del mensaje cifrado, y que la misma clave nunca debería ser usada para ambos cifrados ni los propósitos de autentificación.

- **Seguridad**

La seguridad del criptosistema RSA está basado en dos problemas matemáticos: el problema de factorizar números grandes y el problema RSA. El descifrado completo de un texto cifrado con RSA es computacionalmente intratable, no se ha encontrado un algoritmo eficiente todavía para ambos problemas. Proveyendo la seguridad contra el descifrado parcial podría requerir la adición de una seguridad padding scheme.

El problema del RSA se define como la tarea de tomar raíces eth módulo a componer n: recuperando un valor m tal que me=c ≡mod n, donde (e, n) es una clave pública RSA y c es el texto cifrado con RSA. Actualmente la aproximación para solventar el problema del RSA es el factor del módulo n. Con la capacidad para recuperar factores primos, un atacante puede computar el exponente secreto d desde una clave pública (e, n), entonces descifra c usando el procedimiento standard. Para conseguir esto, un atacante factoriza n en p y q, y computa (p-1) (q-1) con lo que le permite determinar d y e. No se ha encontrado ningún método en tiempo polémico para la factorización de enteros largos.

La factorización de números grandes por lo general propone métodos teniendo 663 bits de longitud usando métodos distribuidos avanzados. Las claves RSA son normalmente entre 1024-2048 bits de longitud. Algunos expertos creen que las claves de 1024 bits podrían comenzar a ser débiles en poco tiempo; con claves de 4096 bits podrían ser rotas en un futuro. Por lo tanto, si n es suficientemente grande el algoritmo RSA es seguro. Si n tiene 256 bits o menos, puede ser factorizado en pocas horas

con un computador personal, usando software libre. Si n tiene 512 bits o menos, puede ser factorizado por varios cientos de computadoras como en 1999. Un dispositivo hardware teórico llamado TWIRL descrito por Shamir y Tromer en el 2003 cuestionó a la seguridad de claves de 1024 bits. Es actualmente recomendado que n sea como mínimo de 2048 bits de longitud.

En 1993, Peter Shor publicó su algoritmo, mostrando que una computadora cuántica podría en principio mejorar la factorización en tiempo polinomial, mostrando RSA como un algoritmo obsoleto. Sin embargo, las computadoras cuánticas no se esperan que acaben su desarrollo hasta dentro de muchos años.

- **Consideraciones prácticas**

1. Generación de claves

Buscando números primos grandes p y q por el test de aleatoriedad y realizando test probabilísticos de primalidad los cuales eliminan virtualmente todos los no-primos (eficientemente).

Los números p y q no deberían ser suficientemente cercanos para que la factorización de Fermat para n sea exitosa. Además, si cualquier p-1 o q-1 tiene sólo factores primos pequeños, n puede ser factorizado rápidamente, con lo que estos valores de p o q deben ser descartados.

Uno no debería emplear un método de búsqueda de primos con el cual dar alguna información cualquiera sobre los primos al atacante. En particular, un buen generador aleatorio de números primos para el comienzo del valor empleado. Observar que el requerimiento esta en ambos ‘aleatorios’ e ‘impredecibles’. Esto no son los mismos criterios; un número podría haber sido elegido por un proceso aleatorio, pero si éste es predecible de cualquier forma (o parcialmente predecible), el método usado resultara una seguridad baja. Por ejemplo: la tabla de números aleatorios de Rand Corp en 1950 podría muy bien ser verdaderamente aleatoria, pero ha sido publicada y a ésta puede acceder el atacante. Si el atacante puede conjeturar la mitad de los dígitos de p o q, ellos podrían rápidamente computar la otra mitad. (Ver Coppersmith en 1997).

Es importante que la clave secreta d sea muy grande. Wiener mostró en 1990 que si p está entre q y 2q (es típico) y d<n1/4/3, entonces d puede ser computado eficientemente de n y e. Aunque valores de e son bajos como 3 han sido usados en el pasado, los exponentes pequeños en RSA está actualmente en desuso, por razones incluyendo el unpadded del texto sin cifrar, vulnerabilidad listada sobre 65537

es normalmente usado para el valor de e, considerado demasiado grande para evitar ataques de exponenciación pequeños, de hecho tiene un peso de hamming suficiente para facilitar una exponenciación eficiente

2. Velocidad

RSA es mucho más lento que DES y que otros criptosistemas simétricos. En la práctica, B normalmente cifra mensajes con algoritmos simétricos, cifra la clave simétrica con RSA, y transmite a ambos la clave simétrica RSA-cifrada y el mensaje simétricamente-cifrado a A.

Esto plantea además problemas adicionales de seguridad, por ejemplo, es de gran importancia usar un generador aleatorio fuerte para claves simétricas, porque de otra forma E (un atacante que quiera averiguar el contenido del mensaje) podría puentear la clave simétrica de RSA mediante la adivinación de la clave simétrica.

3. Distribución de claves

Como todos los cifrados, es importante como se distribuyan las claves públicas del RSA. La distribución de la clave debe ser segura contra un atacante que se disponga a espiar el canal para hacer un ataque de replay. Se supone E (atacante) tiene alguna forma de dar a B arbitrariamente claves y hacerle creer que provienen de A. Se supone que E puede interceptar transmisiones entre A y B. E envía a B su propia clave pública, como B cree que es de A. E puede entonces interceptar cualquier texto cifrado enviado por B, descifrarlo con su propia clave secreta, guardar una copia del mensaje, cifrar el mensaje con la clave pública de A, y enviar el nuevo texto cifrado a A. En principio, ni A ni B han detectado la presencia de E. Contra la defensa de ataques algunos están basados en certificados digitales u otros componentes de infraestructuras de la clave pública.

2.2.2. Suministrar servicios sólo a los usuarios finales específicos.

A través de autenticación, basada en certificados digitales X.509, incluida en la capa de control de acceso a los medios, dando a cada usuario WiMAX receptor su propio certificado, más otro para el fabricante, permitiendo a la estación base autorizar al usuario final.

2.2.2.1. Certificado X.509

- **Certificados**

El Certificado Digital es un documento firmado por una Autoridad Certificadora (AC). El documento contiene:

- Versión
- Número de serie
- Nombre de la entidad o persona a la que pertenece la clave pública
- Clave pública de la entidad o persona nombrada
- Fecha de expiración del certificado
- Nombre de la entidad emisora
- Firma digital de la entidad emisora

Si el Certificado es auténtico y se confía en la AC, entonces, se puede confiar en que el sujeto identificado en el Certificado Digital posee la llave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la AC podrá autenticar el documento.

- **Estructura de un certificado digital**

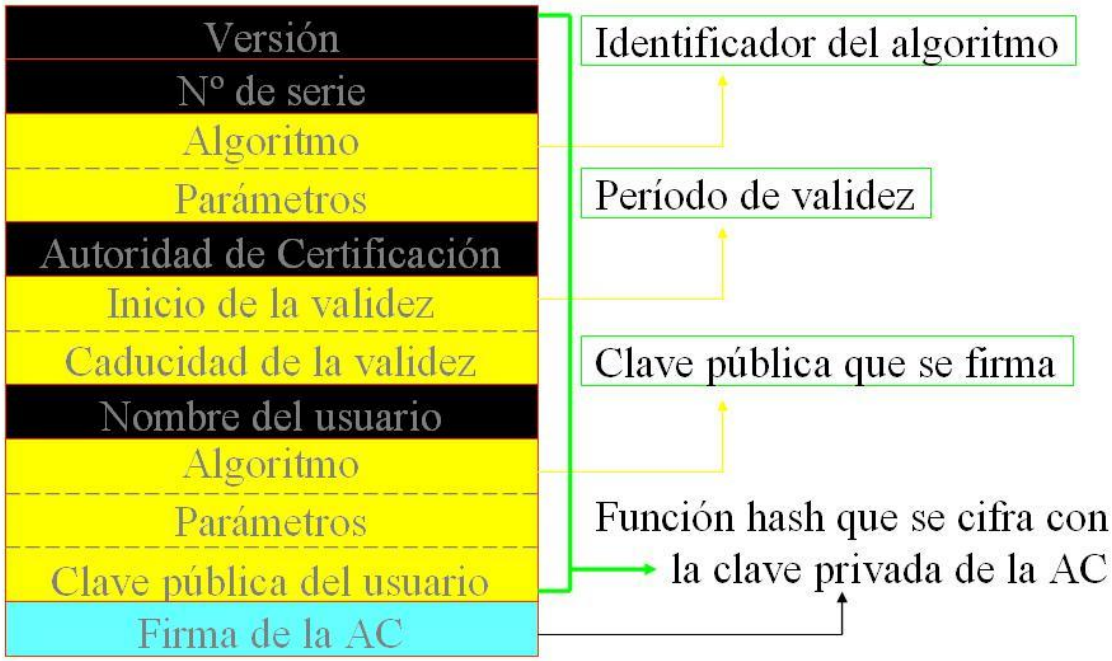


Figura 7 Estructura de un certificado digital

- **Autoridad de Certificación (CA)**

La Autoridad de Certificación es la organización responsable del mantenimiento final de los certificados. Suele representar en el esquema PKI (Public Key Infrastructure, Infraestructura de Clave Pública), la "Tercera Parte Confiable", en la cual los participantes confían al momento de confirmar la autenticidad del otro extremo.

En pocas palabras, las funciones básicas provistas por la Autoridad de Certificación son:

- Emitir certificados
- Revocar certificados y emitir CRLs (Listas de Certificados Revocados)
- Suspender certificados
- Renovar certificados

- **En la red**

  - Un certificado digital también establece la identidad de un usuario en una red.
  - Los servidores pueden ser configurados para permitir el acceso a usuarios con ciertos certificados.
  - Los clientes pueden ser configurados para confiar en servidores que presentan ciertos certificados.

- **X.509**

La primera versión apareció en 1988 y fue publicada como el formato X.509v1, siendo la propuesta más antigua para una infraestructura de clave pública (PKI) a nivel mundial. Esto junto con su origen ISO/ITU han hecho de X.509 el PKI más ampliamente utilizado. Más tarde fue ampliada en 1993 por la versión 2 únicamente en dos campos, identificando de forma única el emisor y usuario del certificado. [11] La versión 3 de X.509 amplia la funcionalidad del estándar X.509.

1. **Campos**

V: Versión del certificado.
SN: Número de serie. (Para los CRL).
AI: identificador del algoritmo de firma que sirve única y exclusivamente para identificar el algoritmo usado para firmar el paquete X.509.
CA: Autoridad certificadora (nombre en formato X.500).
TA: Periodo de validez.
A: Propietario de la clave pública que se está firmando.
P: Clave pública más identificador de algoritmo utilizado y más parámetros si son necesarios.
Y {I}: Firma digital de Y por I (con clave privada de una unidad certificadora).
CA<<A>> = CA {V, SN, AI, CA, T_A, A, AP} Donde Y<<X>> es el certificado del usuario X expedido por Y, siendo Y la autoridad certificadora. De esta forma se puede obtener cualquier X certificado por cualquier Y.

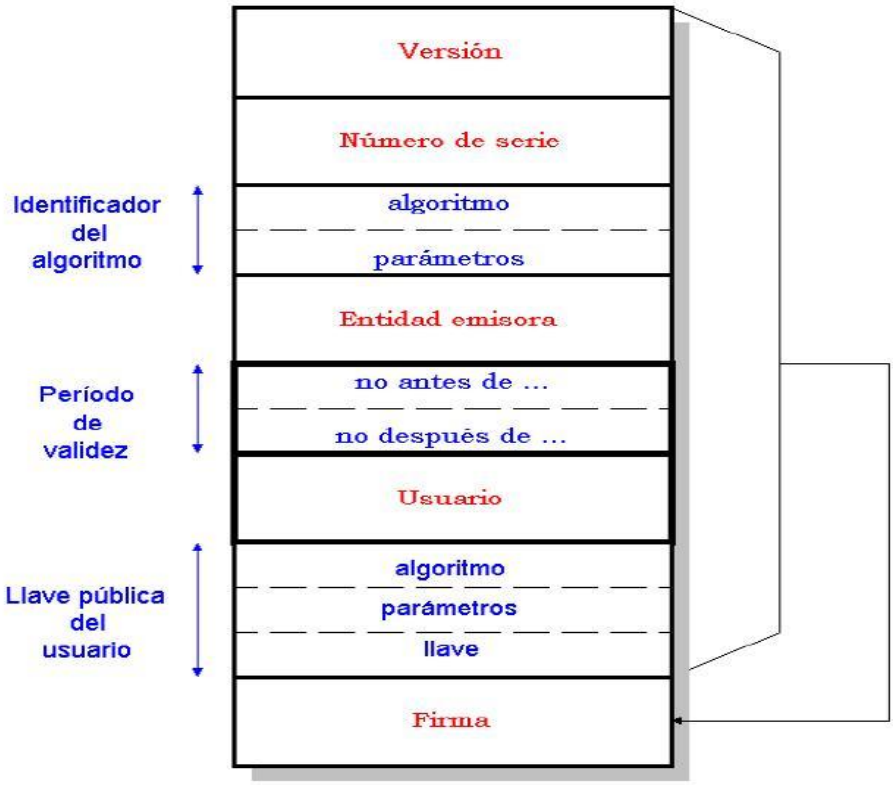


Figura 8 Campos X.509

- **X.509, Versión 3**

El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509, en su versión 3. Contiene datos del sujeto, como su nombre, dirección, correo electrónico, y otros. Con la versión 3 de X.509, sucesora de la versión 2, no hace falta aplicar restricciones sobre la estructura de las CAs gracias a la definición de las extensiones de certificados. Se permite que una organización pueda definir sus propias extensiones para contener información específica dentro de su entorno de operación. Este tipo de certificados es el que usa el protocolo de comercio electrónico SET.

X.509 y X.500 fueron originalmente diseñados a mediados de los años 80, antes del enorme crecimiento de usuarios en Internet. Es por esto por lo que se diseñaron para operar en un ambiente donde sólo los computadores se interconectaban intermitentemente entre ellos. Por eso en las versiones 1 y 2 de X.509 se utilizan CRLs muy simples que no solucionan el problema de la granularidad de tiempo.

La versión 3 introduce cambios significativos en el estándar. El cambio fundamental es el hacer el formato de los certificados y los CRLs extensible. Ahora los que implementen X.509 pueden definir el contenido de los certificados como crean conveniente. Además se han definido extensiones estándares para proveer una funcionalidad mejorada.

1. **Campos del X.509v3**

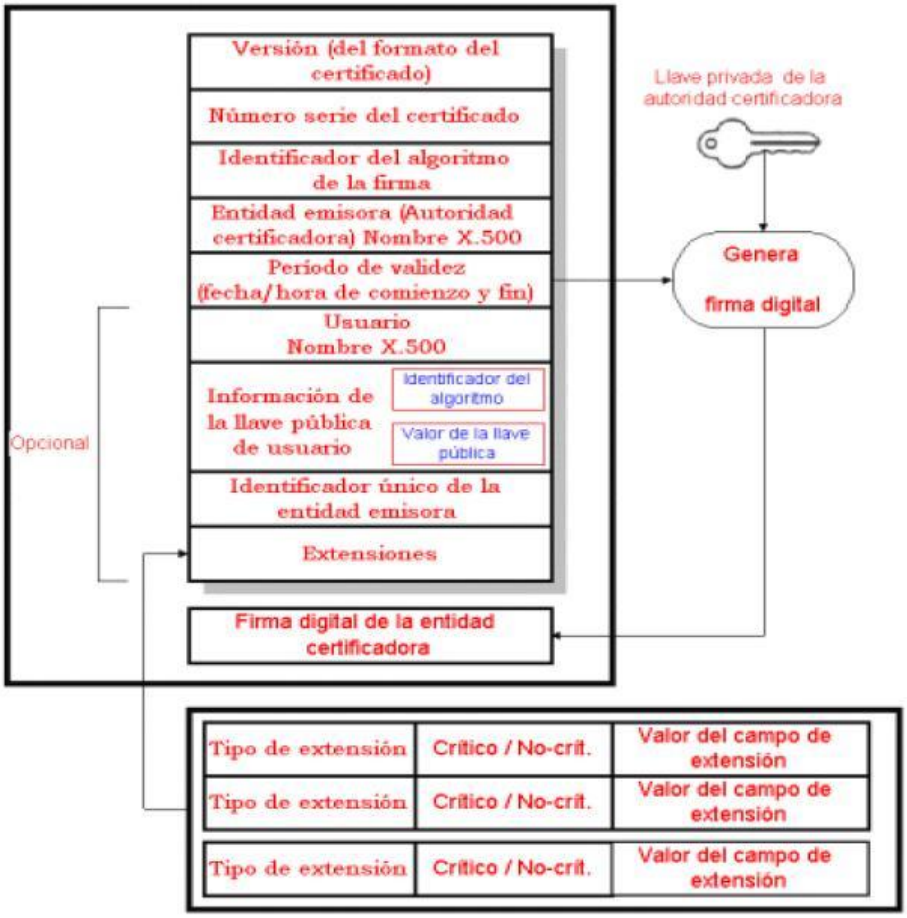


Figura 9 CAMPOS DEL X.509v3

- **Procedimientos de autenticación en una red**

X.509 da tres procedimientos alternativos para la autenticación en peticiones de servicio, mensajes o envío de información.

- Autenticación a una vía (una transmisión).
- Autenticación a dos vías (una transmisión + respuesta).
- Autenticación a tres vías (una transmisión + respuesta + acuse de recepción).

KUB Clave Pública de B.

KRB Clave Privada de B.

KAB Clave simétrica de sesión entre A y B.

EKXX [...] Encriptación con la clave EKXX.

DKXX [...] Encriptación con la clave DKXX.

A {X} Firma por A de X.

tA Marca de tiempo.

rA Testigo (número aleatorio único que A no repetirá durante la vida del mensaje).

En todos estos procedimientos, se supone que las dos partes conocen la clave pública de la otra, bien porque la han obtenido de un directorio, o bien porque en el mensaje inicial va incluida.

1. **Autentificación en una vía**

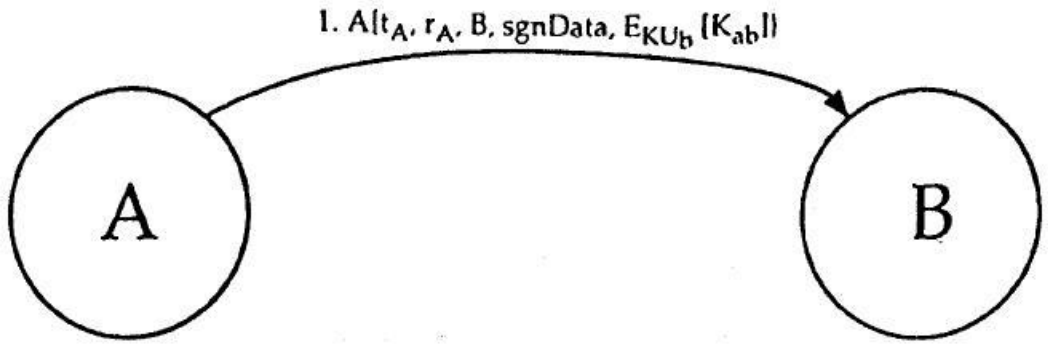


Figura 10 Autentificación en una vía

El mensaje mínimo está formado por el testigo y la marca de tiempo. Puede además contener una clave de cesión temporal entre A y B.

El envío de información de A a B, define:

- La identidad de A y que el mensaje fue generado por A.
- Que el mensaje estaba dirigido a B.
- La integridad y unicidad del mensaje.

2. Autentificación en dos vías

Consiste en el envío de información de A a B, y a continuación de B a A.

Define además de los anteriores:

- La identidad de B, y que el mensaje fue generado por B.
- Que el mensaje estaba dirigido a A.
- La integridad y unicidad del segundo mensaje.

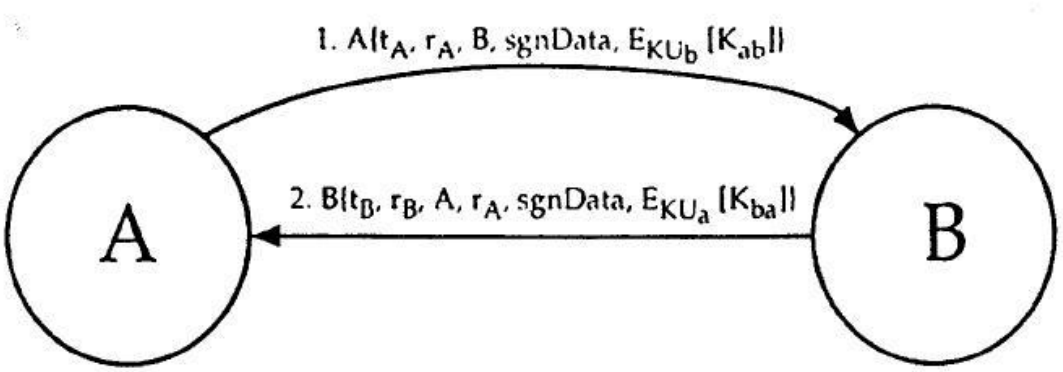


Figura 11 Autentificación en dos vías

3. Autentificación en tres vías

La autentificación de tres vías se emplea cuando el destino y el iniciador no tienen relojes sincronizados o no desean confiar en los relojes. Además de pasar por la autentificación de dos vías, el iniciador envía entonces una respuesta a la respuesta del destino incluyendo el nuevo testigo contenido en la respuesta original, como se muestra en la siguiente figura. Después de verificar que los valores del testigo son idénticos, ya no hay necesidad de verificar las marcas de tiempo.

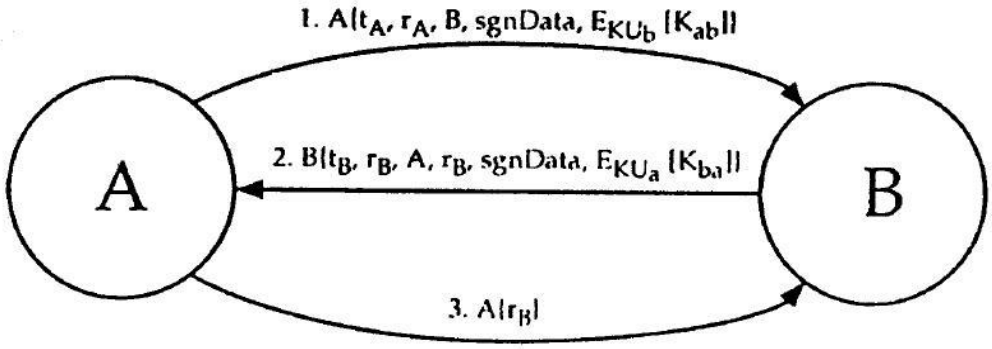


Figura 12 Autentificación en tres vías

2.2.3. Cumplir con la gestión de acceso seguro.

El acceso seguro bajo privacidad de conexión es implementada como parte de un subnivel MAC: la capa de privacidad. Ésta se basa en el protocolo PKM (Privacy Key Management, Administración de Llaves Privadas).

2.2.3.1. Capa MAC

Durante años, la exitosa 802.11x Wi-Fi o LAN inalámbrica la tecnología se ha utilizado en acceso inalámbrico de banda ancha (BWA) las solicitudes junto con una serie de soluciones basadas en la propiedad. Los expertos examinaron la tecnología WLAN de cerca, y se consideró que el diseño global y conjunto de características disponibles, no era muy adecuado para aplicaciones al aire libre BWA. El despliegue se hizo con una capacidad limitada en términos de ancho de banda y los abonados.

La capa MAC de IEEE 802.16 fue diseñada para punto a multipunto inalámbrico de banda ancha a las solicitudes de acceso. La tarea primordial de la capa MAC WiMAX es proporcionar una interfaz entre las capas superiores de transporte y la capa física.

La capa MAC tiene paquetes de la parte superior estos paquetes se denominan servicio de unidades de datos (MSDUs). El protocolo MAC los organiza en unidades de datos (MPDUs) para su transmisión por aire. El diseño de MAC de IEEE 802.16-2004 e IEEE 802.16e-2005 incluye una convergencia en la subcapa que puede interactuar con una variedad de capas superiores y protocolos, como ATM de voz TDM, Ethernet, IP, y cualquier protocolo futuro desconocido.

El 802.16 MAC está diseñada para el punto a multipunto (PMP) y las aplicaciones se basa en colisión sentido de acceso múltiple con la evitación de colisiones (CSMA / CA (Método de acceso múltiple por detección de portadora con anulación de colisiones)).

La MAC incorpora varias características adecuadas para una amplia gama de aplicaciones en diferentes tipos de movilidad, como los siguientes:

- Privacidad de gestión de claves (PKM) para la capa de seguridad MAC. PKM versión 2 incorpora soporte para el protocolo de autenticación extensible (EAP).
- Radio y soporte multicast.

- Gestionabilidad primitivas.
- Traspaso de alta velocidad de la gestión de la movilidad y primitivas.
- Cinco clases de servicio, servicios de concesión no solicitados (UGS), en tiempo real de votación servicio (rtPS), no en tiempo real de votación servicio (nrtPS), mejor esfuerzo (BE) y la extensión en tiempo real a tipo variable (ERT-VR).

Categoría de QoS	Aplicación	Especificaciones de QoS
UGS Servicios de Concesión no Solicitado	VoIP	- Tasa Máxima soportada - Máxima Tolerancia al Retardo *(Latencia)* - Tolerancia al Jitter
rtPS Servicio de Sondeo en Tiempo Real	Flujo de Video o Audio	- Tasa Máxima Reservada - Tasa Máxima Soportada - Máxima Tolerancia al Retardo - Prioridad de Tráfico
ertPS Servicio de Sondeo en Tiempo Real Extendido	Voz con Detección de Actividad (VoIP)	- Tasa Máxima Reservada - Tasa Máxima Soportada - Máxima Tolerancia al Retardo - Tolerancia al Jitter - Prioridad de Tráfico
nrtPS Servicio de Sondeo en Tiempo no Real	Protocolo de Transferencia de Archivo (FTP)	- Tasa Máxima Reservada - Tasa Máxima Soportada - Prioridad de Tráfico
BE Servicio del Mejor Esfuerzo	Transferencia de Datos, Navegación	- Tasa Máxima Soportada - Prioridad de Tráfico

Estas características combinadas con las ventajas inherentes de OFDMA hacen escalable 802.16 adecuado para la alta velocidad de datos y síncrono de aplicaciones multimedia IP.

Apoyo a la QoS es una parte fundamental de la capa MAC WiMAX-. El diseño WiMAX toma prestadas algunas de las ideas básicas detrás de su diseño de QoS.

El fuerte control de QoS se logra mediante el uso de una conexión orientada a la arquitectura MAC, donde todos los enlaces ascendentes y descendentes de las conexiones están controlados por el cumplimiento BS.

WiMAX también define un concepto de un servicio de flujo. Un servicio es un flujo unidireccional de flujo de paquetes con un conjunto particular de parámetro QoS y se identifica por un servicio de identificación de flujo (SFID).

La capa MAC comprende tres subcapas. La subcapa de convergencia de servicios específicos (CS), la Subcapa de Parte Común MAC (MAC CPS) y la subcapa de seguridad, la cual proporciona autenticación, intercambio de claves de seguridad, y encripción.

- **Subcapa de Convergencia de Servicios Específicos (CS)**

La subcapa de convergencia de servicios específicos (CS), provee transformación de datos de redes externas recibidas a través de un CS SAP (punto de acceso a servicios CS) en SDU MAC que son recibidos por la subcapa de Parte Común (CPS) a través de los MAC SAP.

La subcapa de convergencia (CS), desempeña las siguientes funciones:

- Acepta las unidades de datos de protocolo (PDUs) de las capas superiores.
- Realiza la clasificación de los PDUs de las capas superiores.
- Procesamiento (si se requiere) de los PDUs de las capas superiores, basado en la clasificación.
- Entrega los CS PDUs al MAC SAP apropiado.
- Recibe los CS PDUs desde la entidad par.
- Actualmente, son proporcionadas dos especificaciones CS:

- El ATM CS (Asynchronous Transfer Mode CS).
- El Packet CS.

➢ **Subcapa de Parte Común MAC (MAC CPS)**

La subcapa CPS de la MAC proporciona las funcionalidades básicas para el acceso al sistema, asignación del ancho de banda, establecimiento y mantenimiento de la conexión. Recibe datos de varias subcapas CS a través de MAC SAP, clasificados en conexiones MAC diferentes.

Si se tiene una red que utiliza un medio compartido, ésta debe proporcionar un mecanismo eficiente para su uso. Ejemplos de medio compartido inalámbrico, son las redes inalámbricas Punto-Multipunto (PMP) y Tipo Malla. La tecnología utiliza principalmente el de Punto-Multipunto. En este caso, el medio es el espacio a través del cual las ondas de radio se propagan.

➢ **Punto-Multipunto (PMP)**

El enlace punto a multipunto es un sistema que está conformado por un equipo de comunicaciones o estación base (BS) y de equipos remotos o estaciones remotas o estaciones clientes.

El enlace de bajada, que va desde la estación base a la estación del suscriptor es tipo Punto-Multipunto. El enlace inalámbrico IEEE802.16-2004 opera con una estación base central y una antena sectorizada, que es capaz de manejar varios sectores independientes simultáneamente.

La figura muestra un enlace de bajada tipo Punto-Multipunto:

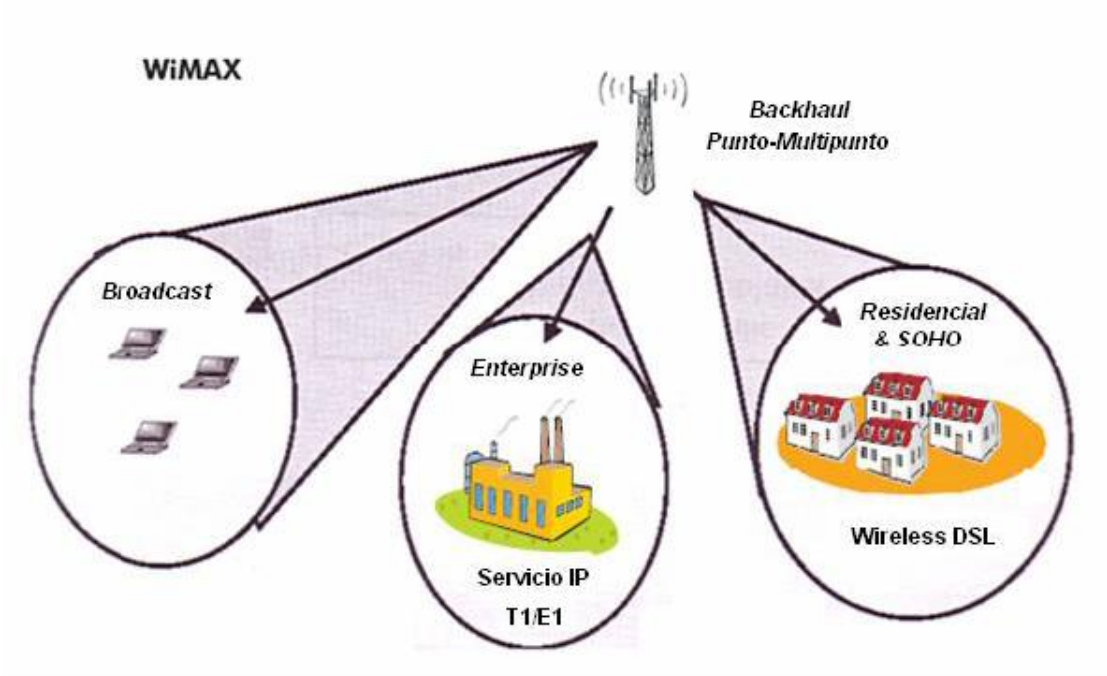


Figura 13 Enlace de Bajada (Downlink) Tipo Punto-Multipunto

La estación base es el único transmisor operando en esa dirección, de modo que no tiene que coordinar con otras estaciones, excepto en el caso que se usa TDD (Time Division Duplexing) el cual divide el tiempo en períodos de transmisión de subida y de bajada.

El enlace de bajada es generalmente un enlace broadcast como se indica en la figura, a menos que se indique que las tramas están dirigidas para un SS específico.

El radio enlace multipunto proporciona soluciones de conectividad para empresas con centros de trabajo múltiples que necesiten de una gran coordinación y trabajo compartido. Este enlace proporciona a la empresa un entorno de intercambio de información de muy alta velocidad.

Los mensajes pueden ser direccionados individualmente o ser enviados sobre conexiones multicast. Efectivamente, todos los centros conectados por el enlace multipunto formarán parte de una única red local, exactamente como si estuvieran en el mismo edificio.

- **Subcapa de Seguridad**

Esta subcapa provee a los abonados de privacidad a través de la red fija inalámbrica de banda ancha. Esto ocurre mediante el encriptado de las conexiones entre las SS y BS.

Adicionalmente, la seguridad provee a los operadores protección contra hurto del servicio. La BS protege en contra de acceso no autorizado a estos servicios de transporte de datos mediante encriptado forzado a los servicios asociados que fluyen a través de la red.

La privacidad emplea un protocolo de autenticación cliente/servidor en el cual la BS, controla la distribución de material clave al cliente SS. Aparte de ello, los mecanismos de privacidad básica son reforzados adicionando al control de protocolo autenticación de SS basada en certificados digitales.

Si durante la negociación de capacidades, la SS especifica que no soporta seguridad 802.16-2004, los pasos de autorización e intercambio de claves deben ser salteados. La BS, si está provisto, debe considerar la SS autenticada, de otra manera la SS no debe ser validada.

- **Arquitectura**

La subcapa de seguridad tiene dos componentes de protocolo:

a. Un protocolo de encapsulación para encriptado de paquetes de datos a través de la red fija BWA. Este protocolo define:

- Un conjunto de suites criptográficas, pares de encriptado de datos y algoritmos de autenticación.
- Reglas para aplicar estos algoritmos a la carga útil de MAC PDU.

b. Un protocolo de manejo principal que proporciona la distribución segura de datos claves desde la BS a la SS. A través de este protocolo de administración de claves, la SS y BS sincronizan los datos clave; además, la BS usa el protocolo para reforzar el acceso condicional a los servicios de la red.

- Encriptado de Paquetes de Datos

Los servicios de encriptado están definidos en un conjunto de capacidades dentro de la subcapa de seguridad MAC. La información específica de encriptado en el encabezado MAC está localizada en el formato de encabezado MAC genérico.

El encriptado también es aplicado a la carga MAC PDU; el encabezado MAC genérico no está encriptado.

- **Protocolo de Administración de Claves (PKM)**

Una SS usa el protocolo PKM para obtener autorización y tráfico de material codificado de la BS, y para soportar reautorizaciones periódicas y refrescos de claves.

El protocolo de administración de claves usa certificados digitales X.509, el algoritmo de encriptado RSA de clave pública, algoritmo de fuerte encriptado para realizar intercambio de clave entre la SS y BS.

2.2.3.2. Protocolo PKM

La Subcapa de Seguridad provee a los suscriptores privacidad, autenticación y confidencialidad a través de la red inalámbrica de banda ancha, aplicando transformaciones criptográficas a los MAC PDUs transportados sobre las conexiones entre SSs (Subscriber station, Estación Cliente) y BSs (Base Station, Estación Base). Emplea un protocolo autenticado cliente/servidor de gestión de claves, en el que la BS controla la distribución de claves a la SS. Adicionalmente los mecanismos de seguridad básica se refuerzan con la combinación de una autenticación digital basada en certificados de equipos de las SSs con el protocolo de gestión de claves (Privacy Key Management, PKM).

El protocolo de gestión de claves PKM permite tanto autenticación mutua (entre BS y SS) como autenticación unilateral (solo la BS autentica a la SS). Soporta además la re autenticación/reautorización periódica y la actualización de claves. El protocolo PKM utiliza EAP (Extensive Authentication Protocol, Protocolo de Autenticación Extensible) o certificados digitales X.509 junto con el algoritmo de encriptación de claves públicas RSA o una secuencia iniciada por autenticación RSA y seguida por una autenticación EAP. Utiliza algoritmos fuertes de encriptación para realizar el intercambio de claves entre la BS y la SS. El protocolo de autenticación PKM establece un shared secret llamado Authorization Key (AK) entre la SS y la BS. La AK es utilizada para asegurar los siguientes intercambios PKM de TEKs (Traffic Encryption Keys).

Una BS autentica a una SS cliente durante el intercambio de autorización inicial.

Cada SS presenta sus credenciales que incluyen un certificado digital único X.509 de fábrica (para autenticación RSA) o una credencial especificada por el operador (para autenticación EAP).

La BS asocia la identidad autenticada de una SS con un suscriptor, asociándola su vez a los servicios de datos a los que el suscriptor tiene autorizado el acceso. [12]

Existen dos protocolos PKM soportados por IEEE 802.16e:

1. PKMv1
2. PKMv2

- **PKMv1**

Una asociación de seguridad (SA) es el conjunto de información de seguridad compartido entre una BS y una o más SS clientes con el fin de soportar comunicaciones seguras a través de la red IEEE802.16. Existen tres tipos de SA:

Primaria, Estática y Dinámica. Cada SS establece una SA primaria durante el proceso de inicialización de la SS. Las SA estáticas son provistas por la BS. Las

SA dinámicas son establecidas y eliminadas conforme a las necesidades, en respuesta al inicio y terminación de service flows específicos. Tanto las SA estáticas como las SA dinámicas pueden ser compartidas por múltiples SSs.
La BS autentica la identidad de la SS cliente al establecer una AK compartida a través de RSA, de la cual se deriva una KEK (key encryption key, clave de cifrado de clave) y las claves de autenticación de mensajes. La BS provee a la SS cliente un identificador de SA (SAID, que identifica la SA Estática) y con propiedades de las SAs primaria y estática para las cuales la SS está autorizada a obtener información de claves.

La SS inicia la autorización al enviar un mensaje de información de autenticación a su BS, el mismo que contiene el certificado X.509, y envía inmediatamente después un mensaje demanda de autorización solicitando un AK y los SAIDs que identifiquen las SAs estáticas en las cuales la SS se encuentra autorizada a participar. En respuesta a este mensaje, la BS valida la identidad de la SS, determina el algoritmo de encriptación y el protocolo soportado compartido con la SS, activa un AK para la SS y lo encripta con la clave publica de la SS, y la envía de regreso a la SS dentro de un mensaje

respuesta de autorización. La SS debe mantener actualizada su AK enviando periódicamente mensajes demanda de autorización. Una vez realizada la autorización, la SS inicia una maquina de estados TEK independiente para cada SAID identificado, la cual es responsable del manejo de las claves asociadas al SAID respectivo. Las maquinas de estados TEK mantiene actualizadas sus claves a través del intercambio periódico de mensajes Key

Request – Key Reply. El TEK es encriptado con una clave KEK derivada de la AK. [12]

- **PKMv2**

PMKv2 utiliza un handshake de tres vías con el fin de optimizar los mecanismos de re autenticación y así soportar fast handoff, además de reforzar la seguridad y evitar el ingreso de usuarios no autorizados.

Existen dos esquemas de autenticación, una autenticación mutua RSA y una autenticación mutua en el ingreso inicial seguida de una autenticación EAP en cada reingreso.

La autenticación RSA inicia cuando la SS envía un mensaje de información de autenticación a su BS inmediatamente después del cual envía un mensaje demanda de autorización solicitando un AK y los SAIDs que identifiquen las SAs estáticas en las cuales la SS se encuentra autorizada a participar. Como respuesta, la BS valida la identidad de la SS, determina el algoritmo de encriptación y el protocolo soportado que comparte con la SS, activa un AK para la SS, lo encripta con la clave publica de la SS y lo envía de regreso a la SS dentro de un mensaje respuesta de autorización. La SS mantiene actualizada su AK enviando periódicamente mensajes demanda de autorización.

Realizada la autorización, la SS inicia una maquina independiente de estados TEK para cada SAID identificado en los mensajes respuesta de autorización o PKMv2.

La máquina de estados TEK es responsable del manejo de las claves asociadas al SAID respectivo, y mantiene actualizadas sus claves a través del intercambio periódico de mensajes Key Request–Key Reply. Para SAs que utilicen DES-CBC para encriptación, el TEK del mensaje Key Reply se encripta con 3-DES (Triple Data Encryption Standard) usando una clave 3-DES KEK derivada de la AK. Para

SAs que utilicen claves de encriptación de 128 bits, como el modo AES-CCM, el TEK se encripta con AES usando una clave de 128 bits derivada de la AK y un bloque de tamaño 128 bits.

La jerarquía de claves de PMKv2 define las claves presentes en el sistema y el modo en el que son generadas. Al existir dos esquemas de autenticación, existen dos fuentes principales de claves. Las claves utilizadas para proteger la integridad de los mensajes de gestión y transportar las claves de encriptación de tráfico se derivan de las claves fuente generadas en los procesos de autenticación y autorización. El proceso de autenticación basado en RSA entrega el AK pre primario (pre-PAK) (utilizado para generar el PAK el cual es utilizado a su vez para general el AK) y el proceso de autenticación basado en EAP entrega el MSK (Master Session Key).

Las claves que protegen el trafico MBS se derivan del MBS AK, cuyo medio de entrega se encuentra fuera del alcance de este estándar. [12]

2.2.4. Denegación de servicios para unidades robadas o utilizadas de forma fraudulenta.

Cuando el certificados del lado de los clientes están alojados en tarjetas inteligentes, esta ofrece la más segura solución de autenticación disponibles porque no hay manera de recuperar del usuario clave privada a partir de una tarjeta inteligente sin robar la tarjeta en sí. Cualquier robo físico de una tarjeta inteligente se nota de inmediato es revocada y una nueva tarjeta inteligente se publicará en breve.
Las causas por las que se revoca un certificado pueden ser varias, pero la más clara aparece cuando se produce la pérdida o captura de la clave privada. Para las CA es muy importante ser capaz detectar los certificados cuya confianza este dudosa ya que compromete el nivel de confianza que se puede tener sobre una CA. Cuando un certificado es revocado, este es pasa a una lista de certificados revocados (CRL) y no se puede tener acceso a los servicios que anteriormente tenía el cliente y de esta forma el intruso no puede acceder a ninguno de ellos.

2.2.5. IPSec

2.2.5.1. La seguridad en el protocolo IP

Como la tecnología WiMAX está basada totalmente en el protocolo IP, esta hereda también su seguridad. La seguridad en IP (IPSec) que se tratará, es la seguridad en la versión 6 de dicho protocolo (IPv6).

Debido al carácter científico que en un principio tuvo INTERNET, la seguridad no fue contemplada históricamente en ninguna de las capas que forman la estructura TCP/IP. Con el auge de las tecnologías de la información y el aumento de personas y empresas conectadas a INTERNET, la necesidad de seguridad se fue convirtiendo en una necesidad. Además la proliferación de noticias sobre personas sin escrúpulos dedicadas a la piratería en INTERNET, creó un gran malestar social debido a la sensación de inseguridad por los ataques que sufrían tanto las empresas (bancos, universidades e incluso instituciones como la NASA) como los usuarios (utilización ilícita de números de tarjetas de crédito...).

La tardía reacción de las instituciones encargadas de la creación y modificación de los protocolos de INTERNET, propició la aparición de diferentes soluciones comerciales (SSL, SET...) para que los usuarios pudieran disfrutar de una seguridad que INTERNET no proporcionaba.

Aprovechando la necesidad de adaptar los diferentes protocolos al crecimiento de INTERNET, se optó por introducir una serie de especificaciones para garantizar la seguridad como parte implícita de las nuevas especificaciones de los protocolos. Estas especificaciones se conocen como IP Security o IPSec.

Una vez que se había consensuado la necesidad de introducir especificaciones de seguridad como parte intrínseca de los protocolos y no como simples extensiones voluntarias para los fabricantes de software, se planteó un duro debate sobre que capa sería la idónea para proporcionar esta seguridad. Esta decisión era crítica, ya que en el mercado ya existían diferentes soluciones comerciales (SSL, SET...) que proporcionaban distintos grados de seguridad en la capa de usuario.

Finalmente para evitar duplicidades y asegurar un sistema seguro y auténtico en todas las capas, se optó por incluir las especificaciones en el nivel más bajo de la pila (Stack) de protocolos, en la especificación del protocolo IP versión 6. [13]

2.2.5.2. Las especificaciones IPSec

La información siguiente ha sido extraída en su mayoría de las referencias [Hui98], [RFC2104], [RFC2401], [RFC2402], [RFC2403], [RFC2404], [RFC2405], [RFC2406], [RFC2407], [RFC2408], [RFC2410], [RFC2410], [RFC2411], [RFC2412], [RFC2451] así como de [WWW16].

Las especificaciones IPSec han sido definidas para trabajar en la capa inferior de la pila (Stack) de protocolos TCP/IP, funcionando por lo tanto en el nivel de datagrama y siendo independientes del resto de protocolos de capas superiores (TCP, UDP...).

La seguridad en IPSec se proporciona mediante dos aspectos de seguridad (Security Payload):

- **Cabecera de autenticación** (Authentication Header, **AH**).

Esta cabecera es la encargada de proporcionar autenticidad a los datos (datagramas) que se reciben en dos aspectos:

  - Los datagramas provienen del origen especificado. Se garantiza la autenticidad del origen de los datos (no pueden ser repudiados).
  - Los datagramas (y por tanto los datos que contienen) no han sido modificados.

- **Cifrado de seguridad** (Encrypted Security Payload, **ESP**).

  - De esta forma se garantiza que tan sólo el destinatario legítimo del datagrama (datos) pueda descifrar el contenido del datagrama.

La autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la **asociación de seguridad** (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

En un ordenador con múltiples conexiones (consultar el correo mientras se baja un fichero por FTP y se consulta el saldo bancario...) se puede tener varias asociaciones de seguridad (como mucho una por conexión). Para poder diferenciar entre ellas utilizare un **índice de parámetros de seguridad** (Security

Parameter Index, SPI) que permitirá al recibir un datagrama saber a qué asociación de seguridad hace referencia, y de esta forma poder autenticarlo y/o descifrarlo.

Al iniciar una comunicación que utilice los servicios IPSec con un único destino (direcciones unicast) este debe comunicar a que índice de parámetros de seguridad (SPI) se debe hacer referencia. Análogamente en una comunicación con varios destinos (direcciones multicast o anycast) todos los destinatarios deben compartir el mismo número de índice (SPI).

- **La cabecera de autenticación (AH)**

La **cabecera de autenticación** (Authentication Header, AH) es una cabecera específica de la versión 6 de IP (ver figura 14). Se suele situar justo antes de los datos, de forma que los proteja de posibles atacantes. No obstante ha sido diseñada de forma muy versátil, pudiendo incluirse antes que otras cabeceras (cabecera de opciones, cabecera de encaminamiento...) para asegurar así que las opciones que acompañan al datagrama son correctas.

De esta forma, la presencia de una cabecera de autenticación no modifica el funcionamiento de los protocolos de nivel superior (TCP, UDP...) ni el de los routers intermedios, que simplemente encaminan el datagrama hacia su destino.

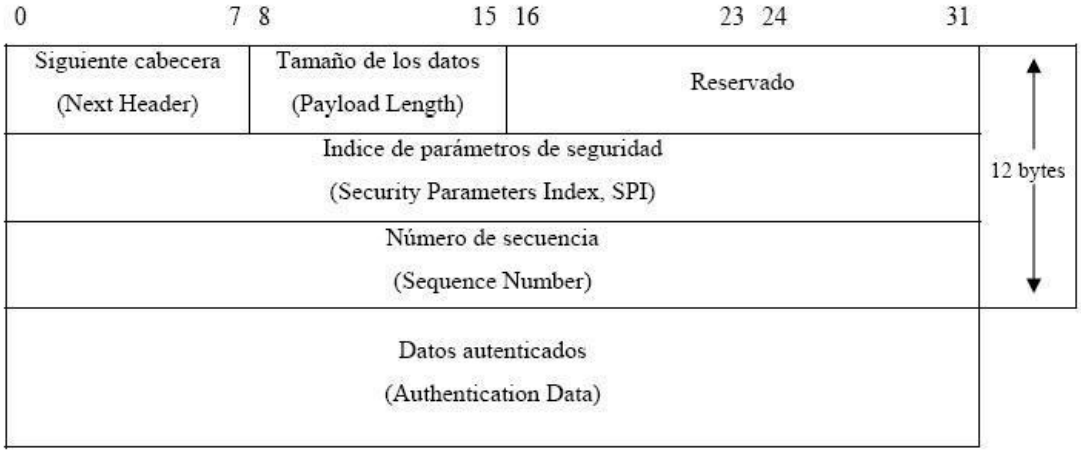


Figura 14 Esquema de cabecera de autenticación

El **tamaño de los datos** (Payload Length) especifica la longitud de los datos en palabras de 32 bits (4 bytes).

El **índice de parámetros de seguridad** (SPI) es un número de 32 bits, lo que permite tener hasta 2^32 conexiones de IPSec activas en un mismo ordenador.

El **número de secuencia** (Sequence Number) identifica en número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas Los **datos autenticados** (Authentication Data) se obtienen realizando operaciones (depende del algoritmo de cifrar escogido) entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.

El principal problema al autenticar un datagrama es que algunos campos son modificados por los routers intermedios (como el alcance del datagrama, que se va decrementando en una unidad cada vez que pasa por un router para evitar bucles infinitos), esto hace imposible poder autenticar todo el datagrama, ya que durante su camino por INTERNET es modificado. El cálculo de los datos autenticados se realiza mediante un algoritmo de Hash (actualmente se sugiere el algoritmo MD5 que calcula un checksum de 128 bits).

- **La cabecera de cifrado de seguridad (ESP)**

La cabecera de autenticación (AH) no modifica los datos que transporta, circulando el texto en claro (Clear Text), simplemente les añade autenticidad (al origen y al contenido). De esta forma, los datos que circulan pueden ser interceptados y visualizados por un eventual atacante. Esto puede sernos útil por ejemplo cuando se consulta un documento oficial (BOE o las bases de unas oposiciones en la universidad...) ya que debe ser público y no tiene sentido cifrarlo, aunque si es básico que sea auténtico.

En el caso de necesitar confidencialidad (por ejemplo en consultas a un banco, no interesa que una tercera persona tenga acceso a nuestro saldo) se debe utilizar la **cabecera de cifrado de seguridad** (Encrypted Security Payload, **ESP**).

La **cabecera de cifrado de seguridad** (ver figuras 15 y 16) es siempre la última en el sistema de cabeceras en cadena (*Daisy Chain*). Esto es debido a que a partir de ella todo los datos vienen cifrados, con lo que los routers intermedios no podrían procesar las cabeceras posteriores.

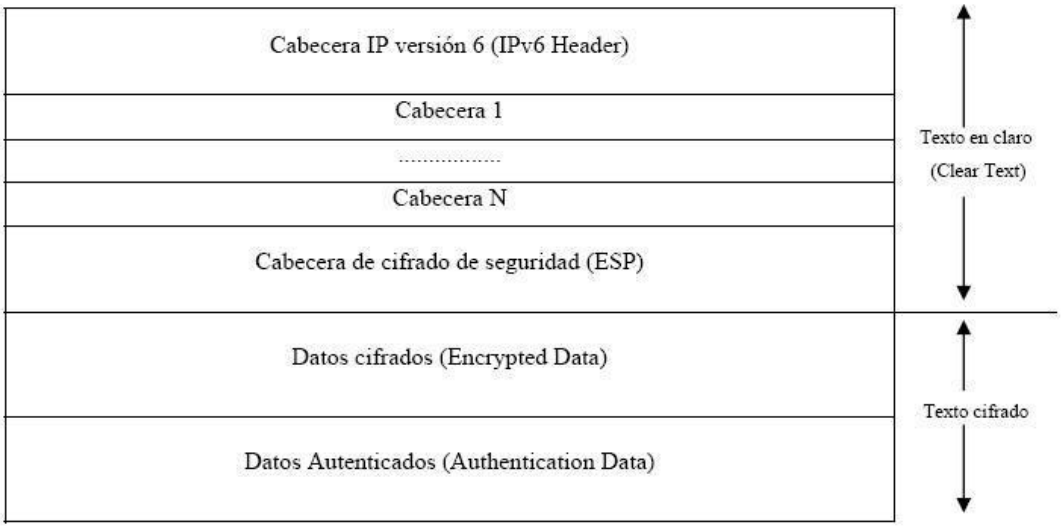


Figura 15 Situación de la cabecera de cifrado de seguridad

Al igual en con la cabecera de autenticación (AH), el algoritmo a utilizar se negocia con el receptor de la información antes de enviar un datagrama cifrado. Actualmente se propone e DES-CBC que es el algoritmo DES funcionado el modo de bloque CBC.

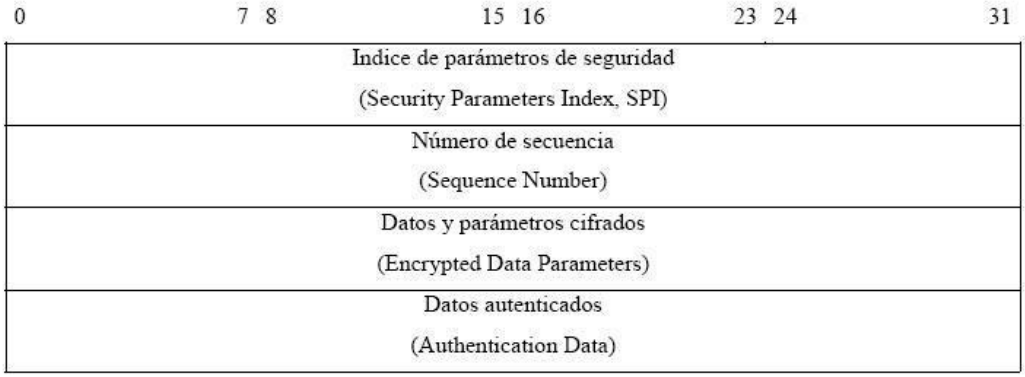


Figura 16 Esquema de la cabecera de cifrado de seguridad

A diferencia de la cabecera de autenticación (AH) no es necesario especificar el tamaño de los datos cifrados, ya que a partir de la cabecera de cifrado hasta el final del datagrama todo está cifrado.

El **índice de parámetros de seguridad** (SPI) y el **número de secuencia** (Sequence Number) tienen el mismo significado que en la cabecera de autenticación (AH).

Los **datos autenticados** (Authentication Data) aseguran que el texto cifrado no ha sido modificado utilizando un algoritmo de Hash (depende del algoritmo de cifrar escogido).

Debido a que tanto la cabecera de autenticación (AH) como la cabecera de cifrado de seguridad (ESP) pueden ser utilizadas independientemente, se recomienda que en el caso de ser necesario tanto la autenticidad como la privacidad se incluya la cabecera de cifrado tras la de autenticación. De esta forma se autentica los datos cifrados.

- **El protocolo ISAKMP**

El protocolo **ISAKMP** (INTERNET Security Association Key Management Protocol) parece ser el escogido para el intercambio de claves y parámetros de seguridad en

IPSec. No obstante, debido a que aún se encuentra en fase experimental, no se puede asegurar que finalmente este sea el elegido, ya que varios algoritmos han sido propuestos durante los últimos años (SKIP, Phouturis, Oakley...).

ISAKMP es un protocolo que proporciona la infraestructura necesaria para la negociación de asociaciones de seguridad (SA) entre dos usuarios cualesquiera (ver figura 17). Se define una **transacción de configuración** (Configuration Transaction) como un doble intercambio dónde el emisor realiza un envío/petición (Set/Request) y el receptor contesta mediante un reconocimiento de petición/respuesta (Acknowledge/Reply).

De esta forma a un envío (Set) le corresponde un reconocimiento de envío (Acknowledge) y a una petición (Request) una respuesta (Reply).

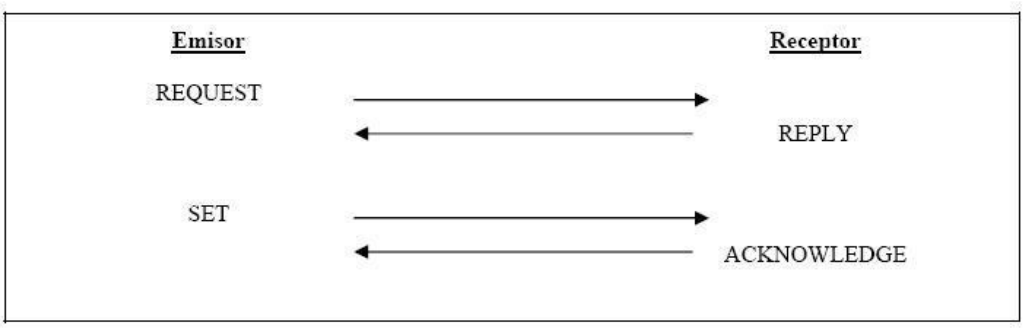


Figura 17 Esquema de una transacción de seguridad

El inicio de la comunicación siempre es precedido de una transacción de configuración dónde se intercambian dos *cookies* (Request/Reply). Este esquema permite evitar ataques de denegación de servicio (DOS) ya que hasta que no se reciba la respuesta el esquema no continúa. Posteriormente se producen los intercambios de información necesarios mediante envíos/reconocimientos de envío (Set/Acknowledge) dónde se negocian los diferentes parámetros de seguridad (SPI, clave común, tiempo de validez de la clave, algoritmo de cifrado a utilizar...) que gobernaran la comunicación.

El intercambio de mensajes mediante ISAKMP se realiza mediante el esquema de cabeceras de extensión (ver figura 18) ya utilizado en la definición del protocolo IP versión 6.

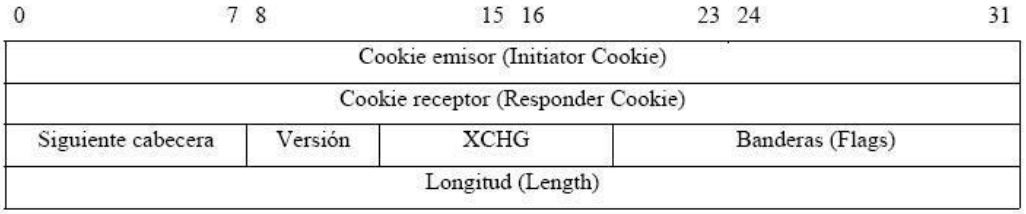


Figura 18 Formato de la cabecera de ISAKMP

El intercambio de claves entre el emisor y el receptor se realiza utilizando el algoritmo de Diffie-Hellman. En el caso de direcciones multicast (varios emisores/receptores en una misma comunicación) el algoritmo anterior resulta ineficiente, ya que está pensado para un emisor y un receptor. La solución adoptada es la de confiar en ordenadores servidores de claves.

- **El protocolo IKE**

El protocolo **IKE** (INTERNET Key Exchange) es un protocolo de dos fases para el establecimiento de un canal auténtico y seguro entre dos usuarios (Peers). Este protocolo utiliza la infraestructura de mensajes del protocolo ISAKMP para el intercambio de mensajes.

Fase1: Se negocian las asociaciones de seguridad (SA). Se utiliza el protocolo Diffie-Hellman para el intercambio de una clave común y se establece el algoritmo de cifrado (3DES-CBC...), el algoritmo de Hash

(MD5...) y del sistema de autenticación. En esta fase tanto el emisor como el receptor quedan autenticados mediante uno de los siguientes cuatro métodos:

HDR: Cabecera ISAKMP.

HDR*: Cabecera cifrada

HASH: Función Hash.

KE: Valor público Diffie-Hellman.

SA: Asociación de seguridad.

Ni y Nr: Valor temporal (Nonce payload).

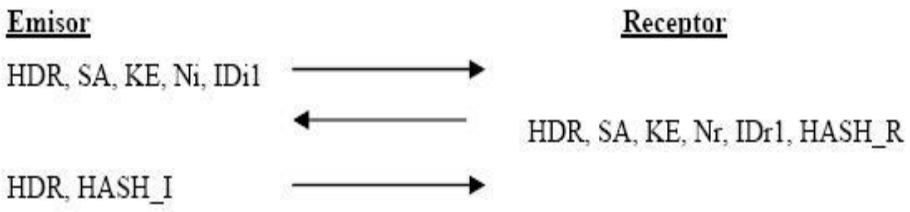
[Cert] y SIG: Certificado y firma digital.

ID: Identificador.

PubK: Clave pública.

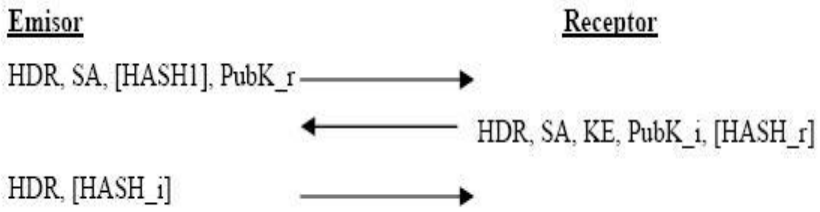
[ ]: Opcional.

1. **Autenticación con claves pre-compartidas (Pre-shared Keys).**

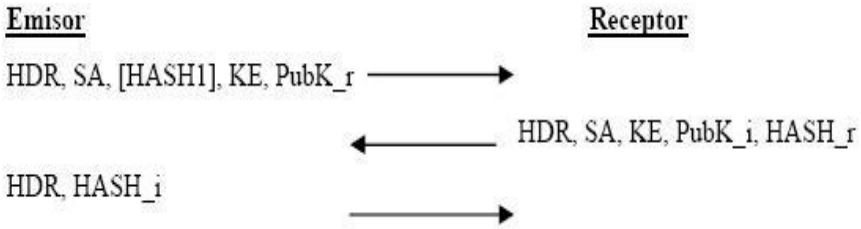


2. **Autenticación mediante firmas digitales (Digital Signatures).**

3. **Autenticación mediante clave pública 1.**

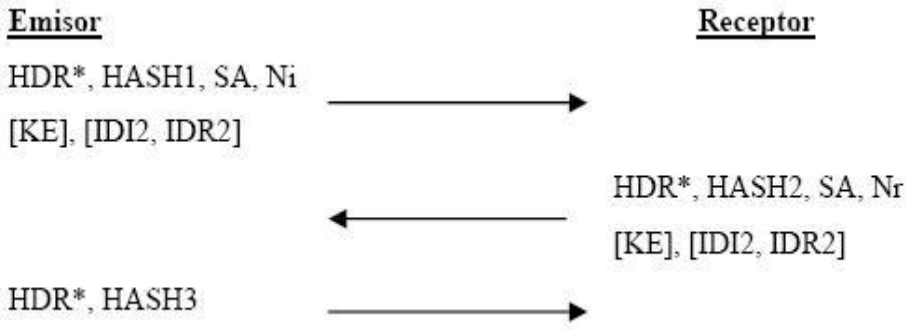


4. **Autenticación mediante clave pública 2.**



Fase 2: Una vez establecidos los distintos parámetros iníciales (SA) y aprovechando la seguridad de la fase 1, se inicia un modo rápido (Quick

Mode) dónde se vuelven a negociar asociaciones de seguridad (SA) con el objetivo de evitar ataques de reutilización (Replay) de los datagramas de la fase 1 por un atacante.



Esta combinación de algoritmos permite mantener una comunicación auténtica y privada entre dos usuarios (Peers), el problema principal radica en su complejidad, ya que pese a ser muy flexible

(permite distintos métodos de autenticación y utilización de firmas digitales) es difícil su implementación práctica.

2.2.5.3. Posibilidades y aplicaciones de IPSec

Las especificaciones IPSec tienen una gran versatilidad que les permite ser utilizadas en las distintas soluciones adoptadas actualmente en INTERNET (comunicación entre distintos cortafuegos (*Firewalls)*, configuración de ordenadores móviles...). El procedimiento de autenticación (fase1) permite que junto al protocolo de vecindad

(Neighbor Discovery Protocol) se puedan asegurar intercambios seguros entre los distintos routers, evitando la intercepción de los datagramas.

Una de las soluciones más adoptadas actualmente para la implementación de la seguridad en INTERNET es el uso de Firewalls (ver figura 19). Este esquema de actuación consiste en no permitir un acceso directo de los ordenadores a INTENET, colocando una máquina intermedia (denominada cortafuegos o Firewall) que mediante un sencillo conjunto de reglas (dejar pasar los datagramas que vienen de la dirección A, no aceptar datagramas de las direcciones B y C, no aceptar datagramas que vayan al puerto X...) filtra todo el tráfico de INTERNET (entrante y saliente).

Figura 19 Esquema de seguridad basado en un firewall

La nueva configuración que se propone con la ayuda de las especificaciones IPSec consiste en realizar un túnel virtual seguro (Secure Tunnel) de forma que dos firewalls estén virtualmente conectados a través de INTERNET de una forma transparente para los usuarios (ver figura 20). De esta forma, el

intercambio de información vendrá regulado por una comunicación entre los dos firewalls mediante datagramas IP versión

6 encapsulados en datagramas IP versión 6 autenticados (y cifrados si se requiere privacidad).

Las comunicaciones entre dos organizaciones (para nuestro ejemplo se utilizará el

MIT y la UAB) son realizadas de forma transparente y segura a través de los firewalls.

Cuando un ordenador de la UAB desea conectarse a uno del MIT, envía el datagrama correspondiente al firewall. Este se encarga de encapsularlo en un datagrama auténtico (y cifrado si se desea privacidad) y enviarlo al otro extremo del túnel por INTERNET.

Al recibir el firewall del MIT este datagrama, comprueba su autenticidad, lo descifra (si es necesario), lo desencapsula y lo envía al ordenador correspondiente.

De esta forma tan sencilla se puede proporcionar un canal seguro y auténtico entre dos puntos cualesquiera conectados a INTERNET. Esta configuración también es conocida como red privada virtual (Virtual Private Network, VPN).

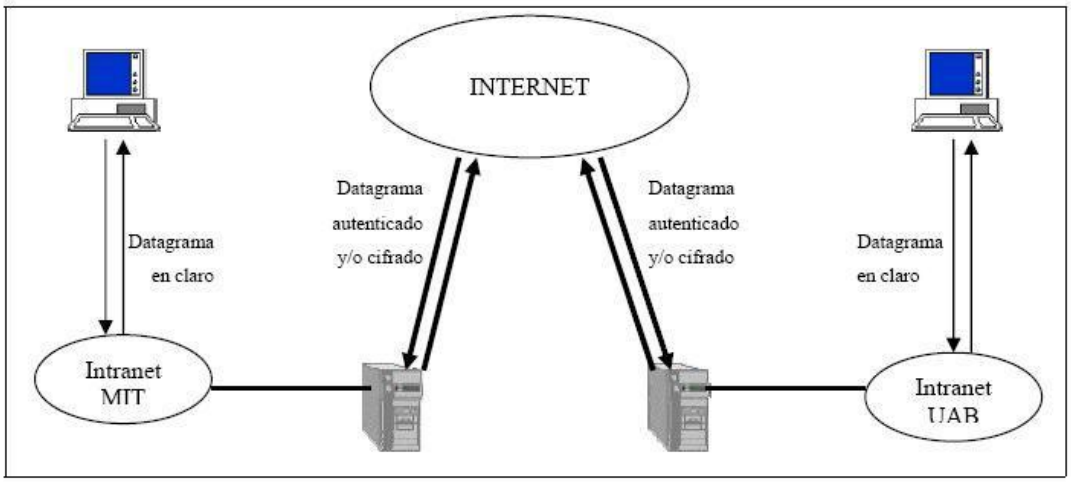


Figura 20 Esquema de seguridad proporcionado por IPSec basado en VPN

Además deja sin resolver el problema de comunicaciones seguras entre varios usuarios, ya que realizar este algoritmo entre todos ellos resulta en un alto coste de intercambio de datagramas. De esta forma para grupos (multicast o anycast) se debe utilizar un esquema dónde un servidor de claves (que se debe suponer que sea seguro) sincroniza la clave común a todos los componentes del grupo.

2.2.6. Autenticación, Autorización y Contabilidad (AAA) en WiMAX.

La seguridad es una preocupación importante para el operador de red y el usuario de la red. El operador de red que quiere saber los usuarios y los dispositivos conectados a su red, para prevenir ataques maliciosos, suplantación de identidad de usuario entre otros y que los usuarios que tienen acceso a los servicios están autorizados para acceder a la red ya que los usuarios pagan por esos servicios que han utilizado. Los usuarios de la red desea asegurarse de que la privacidad está protegida, que la integridad de los datos que enviar y recibir no es comprometida, que puede tener acceso a los servicios que han suscrito y que no son más acusados por esos servicios. De hecho, las expectativas del operador de la red y el usuario de la red no son contradictorios, sino complementarios. Cualquier red bien diseñada debe entregar estas perfectamente razonables expectativas que sólo pueden ser realizados por el equipo vendedores, integradores de sistemas y operadores de redes.

- **Preocupaciones de Seguridad de los usuarios:**
  - Privacidad: Proteger de las escuchas.
  - La integridad de los datos: Proteger los datos de los usuarios de ser manipulados en el tránsito.
  - El acceso a los servicios: Los usuarios tienen las correctas credenciales.
  - La exactitud de la contabilidad: Precisión y eficiencia de la contabilidad.
  - Autenticación de usuario: ¿Es el usuario que dice que es?
  - Autorización: ¿Es el usuario autorizado para recibir un servicio?
  - Control de acceso: Sólo los usuarios autorizados tener acceso a los servicios.

Se maneja la seguridad en múltiples capas de la red, cada capa da un manejo a aspectos complementarios de la seguridad. Funciones de seguridad pueden ser asignadas a diferentes capas de la capa OSI 7-modelo.

La capa de enlace de autenticación y autorización garantiza que la red sólo es visitada por los usuarios autorizados. Capa de enlace de codificación asegura la privacidad y protege los datos de tráfico de las escuchas por terceros no autorizados.

La capa de red de medidas de seguridad proteger la red de ataques malintencionados logrado mediante el uso de firewalls y servidores AAA. Radio es el medio más utilizado con el protocolo de AAA interacciones. Arquitectura de red WiMAX móvil se refiere a la utilización de estas técnicas, proporcionando un seguro de itinerancia AAA modelo.

Del Transporte y las capas de aplicaciones proporcionar medidas de seguridad adicionales que se consideren apropiado por el operador de red, proveedores de servicios de aplicación (ASP) o el final propio usuarios.

- **Seguridad de WiMAX por Capas del Modelo OSI.**

7	Nivel de Aplicación	Certificado y firmas digitales
4	Nivel de Transporte	Seguridad en el nivel de Transporte, EAP- TTLS
3	Nivel de Red	IPSec, Arquitectura AAA
2	Nivel de Enlace de Datos(MAC)	AES, PKMv2, X.509v3

Los principales problemas con el régimen de seguridad de WiMAX son la autenticación y confidencialidad, que se centra principalmente en la autenticación y autorización de WiMAX, ya que son componentes clave de cualquier solución de seguridad. En 802.16, las características de seguridad son prometedoras, ya que están mejor diseñadas. De hecho, el estándar WiMAX se incorpora más flexible y con mejor apoyo a la seguridad en la norma.

2.2.6.1. Problemas en la autenticación y autorización - EAP

El objetivo de la autenticación y autorización de las técnicas utilizadas en los sistemas para prevenir el snooping de ID de usuario, de denegación de servicio (DoS), sin conexión ataque de diccionario, el hombre en el medio de ataque, el método de autenticación de clasificación de los ataques y romper una débil llave. El protocolo de autenticación tiene que velar por la recopilación de información sobre el usuario antes de elegir el protocolo y para autenticar a ambas partes por igual (autenticación mutua).

EAP se presenta lo que puede ofrecer un esquema de autenticación para evitar el mencionado problema. Se integra diferentes métodos de autenticación para que coincida con la naturaleza de la canal de comunicación. Estos métodos son asesorados por IEEE incluidos PKM-EAP, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-TTLS, EAP-SIM y EAP-AKA.

WiMAX utiliza tres de estos métodos, es decir, PKM-EAP, EAP-TLS y EAP-TTLS. EAP-TLS es un estándar abierto IETF y está bien soportado entre los proveedores inalámbricos. Ofrece una buena dosis de seguridad, ya que TLS es considerada la sucesora de la SSL (Secure Socket Layer) estándar. Utiliza PKI para garantizar la comunicación al servidor de autenticación RADIUS, y este hecho puede hacer que parezca como una tarea de enormes proporciones para crear. Por lo tanto, a pesar de EAP-TLS proporciona una excelente seguridad, la sobrecarga de los certificados de cliente puede ser su talón de Aquiles.

EAP-TLS es el estándar original de LAN inalámbrica, protocolo de autenticación EAP. La exigencia de un cliente-lado certificado es el que da EAP-TLS de autenticación de su fuerza y pone de manifiesto la conveniencia clásico versus seguridad trade-off. Una contraseña tras haber sido comprometida no es suficiente para romper en EAP-TLS, porque los sistemas del pirata informático tienen que tener el lado del cliente certificado. Cuando el cliente del lado de los certificados están alojados en tarjetas inteligentes, esta ofrece la más segura solución de autenticación disponibles porque no hay manera de recuperar del usuario clave privada a partir de una tarjeta inteligente sin robar la tarjeta en sí. Cualquier robo físico de una tarjeta inteligente se notó de inmediato y revocada y una nueva tarjeta inteligente se publicará en breve.

EAP-TTLS (TUNNELES TRANSPORT LAYER SECURITY): Se trata de una extensión de EAP-TLS. EAP-TTLS sólo requiere certificados al servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y encripta credenciales y password para garantizar la protección de la comunicación inalámbrica. A continuación se observa una comparación entre estos dos protocolos.

Aspectos	EAP-TLS	EAP-TTLS
Certificado Digital	Del lado del cliente y del servidor	Del lado del servidor
Intercambio de llaves dinámicas	Si	Si
Autenticación mutua	Si	Si
Creador	Microsoft	Funk Software
Soporta Autentificación de Base de Datos	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP
Sistemas Operativos	Windows XP, 2003 y 2000	Diferentes plataformas y Sistemas Operativos

PKM-EAP, por otra parte implica un sentido y sistemas de autenticación mutua. Autenticación se presenta en dos formas:

- Autenticación unilateral que autentica el BS y la MS
- Cuando la autenticación mutua BS autentifica los Estados miembros y los Estados miembros autentica al BS.

Cada aplicación debe tener WiMAX unilaterales autenticación. La experiencia ha demostrado que la autenticación mutua es también muy útil.

La autenticación se logra mediante un protocolo de intercambio de clave pública que garantiza también el establecimiento de claves de cifrado. En clave pública el intercambio de planes de cada participante debe tener una clave privada y una clave pública.

La clave pública que se conoce más ampliamente que la clave privada se mantiene en secreto. WiMAX 802.16e-2005 define un estándar de privacidad de administración de claves (PKM) de protocolo que permite tres tipos de autenticación:

- Una autenticación basada en RSA - los certificados digitales X.509, junto con el cifrado RSA
- Basado en la autenticación EAP (opcional)
- RSA autenticación basada en seguida de autenticación EAP

PKM establece un protocolo de autenticación de llave secreta compartida denominada Autorización Clave (AK) entre la EM y el BS. Una vez que un AK compartido se establece entre el BS y los Estados miembros, la clave de cifrado clave (KEK) se deriva de ella. KEK se utiliza para cifrar PKM posterior intercambio de la clave de cifrado de Tráfico (CET). En la autenticación basada en RSA, un BS autentica la MS en virtud de su singular

X.509 certificado digital que ha sido emitida por el fabricante de la EM. El certificado X.509 contiene la clave pública de la EM (PK) y su dirección MAC. Cuando se solicite un AK, la MS envía su certificado digital a la BS que valida el certificado y entonces utiliza el PK verificado para cifrar un AK que va a ser enviado a los Estados miembros. Todos los Estados miembros que utilizan la autenticación RSA han instalado de fábrica privadas / públicas pares de claves (o una algoritmo para generar las claves dinámicamente), junto con la fábrica instalada certificados X.509.

En el caso de la autenticación basada en el PKM, EM es autenticado a través de un único operador expedido credencial, tal como una tarjeta SIM o bien un certificado X.509 se ha descrito anteriormente. La elección del método de autenticación depende del operador elección del tipo de EAP de la siguiente manera:

- EAP-AKA (Acuerdo de autenticación y clave) para la autenticación basada en SIM,
- EAP-TLS para la autenticación basada en X.509
- EAP-TTLS para MS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo de Microsoft versión 2)

El BS miembros asociados de la identidad a un suscriptor de pago y, por tanto, a los servicios que el abonado está autorizado a acceder. Así, mediante el intercambio de AK, BS determina la identidad de los Estados miembros y los servicios que se han autorizado a acceder.

2.2.6.2. Mecanismos de autenticación para WiMAX

- **Análisis de Seguridad**

El PKM-EAP de WiMAX se ha introducido en una más sólida y segura. Las siguientes mejoras se han tenido en cuenta:

- La autenticación mutua se proporciona en PKMv2, lo que podría evitar "Man in the Middle" los ataques.
- La firma digital X.509 certificado que se expide es único para cada SS y no pueden ser fácilmente falsificados.
- Cada servicio tiene un dicho, si un servicio se ve comprometida, los demás servicios no se vean comprometidas.
- La duración limitada de AK proporciona periódico y los principales reautorización de refresco, lo que impide que los atacantes de tener gran cantidad de datos para llevar a cabo el criptoanálisis.
- Añadir un valor aleatorio de la SS y BS a la autorización SA es una manera de prevenir la repetición de los ataques.
- Seguridad WiMAX admite dos cifrados estándares de calidad-DES3 y AES, que son considerados seguros para el futuro previsible.
- SS puede intentar usar un caché o traspaso a transferir Master Key y evitar una completa re-autenticación.
- PKM-EAP se basa en el TLS (Transport Layer Security) estándar que utiliza la criptografía de clave pública y es muy costoso para algunos dispositivos inalámbricos. Así, cada estación base de WiMAX en ha dedicado una seguridad de alto rendimiento del procesador, lo que da la oportunidad de aplicar un sistema de autenticación mutua en WiMAX. En otras palabras, un

protocolo de autenticación pueden diseñarse de manera que la mayoría de los procedimientos de cálculo se realizan dentro de la estación base.

Sin embargo, también hay algunos problemas conocidos que existen en la arquitectura de seguridad de WiMAX. No sólo define la forma de proteger la comunicación inalámbrica en la capa MAC, pero no ha considerado las amenazas de ataques contra toda la capa física, por ejemplo, la radio interferencia, o de manera continua el envío de paquetes. Esto podría resultar en un receptor abrumado, y, finalmente, causar una denegación de servicio (DoS) o el consumo de batería rápida. Independientemente de las deficiencias anteriores, el mecanismo de autenticación y autorización utilizado en WiMAX es aún muy prometedor.

- **Autorización**

Tras la autenticación, autorización de solicitudes de miembros de la BS. Esta es una solicitud de un AK, así como de una identidad SA (SAID). La solicitud de autorización incluye la EM, certificado X.509, algoritmos de cifrado y criptografía ID.

En respuesta, el BS lleva a cabo la necesaria validación (por la interacción con un AAA servidor en la red) y devuelve una respuesta de autorización que contiene el AK cifra con la clave pública del MS.

- **Cifrado de tráfico**

Como se ha visto anteriormente, el proceso de autenticación y autorización en los resultados la autorización y asignación de clave, es en claves de 160 bits de longitud. La clave de cifrado se deriva directamente de la AK y es de 128 bits de longitud. El KEK no se utiliza para la encriptación de los datos de tráfico, por ello, requieren el tráfico que es la clave de cifrado genera un número aleatorio como en la BS utilizando el algoritmo de cifrado que CTMA KEK se utiliza como clave de cifrado. CTMA se utilizan para cifrar el tráfico de datos.

2.2.6.3. Contabilidad

La contabilidad se refiere a la gestión de la sección donde el servicio es adquirido y entregado a los empresarios y los usuarios individuales. La cuestión es que la banda ancha proveedor de servicios inalámbricos para establecer las necesidades de una instalación basada en la zona metropolitana escalable, segura de banda ancha inalámbrica se ofrece a ser wholesaled proveedor de acceso a

Internet a través de socios de canal. Esto suele hacerse mediante el despliegue de bajo coste las tecnologías inalámbricas WiMAX para proporcionar servicios de datos de banda ancha que pueden personalizarse para apoyar el acceso de las viviendas, pequeñas empresas, oficinas o grandes empresas.

2.2.7. VoIP

2.2.7.1. ¿Qué es VoIP?

VoIP es el acrónimo de "Voice Over Internet Protocol", que tal y como el término dice, hace referencia a la emisión de voz en paquetes IP sobre redes de datos como puede ser Internet. Llegados a este punto se unen dos mundos que hasta entonces habían convivido separados: la transmisión de voz y la de datos. [14]

La tecnología VoIP trata de transportar la voz, previamente procesada, encapsulándola en paquetes para poder ser transportadas sobre redes de datos sin necesidad de disponer de una infraestructura telefónica convencional. Con lo que se consigue desarrollar una única red homogénea en la que se envía todo tipo de información ya sea voz, video o datos.

Desde el punto de vista de la seguridad, las llamadas en VoIP se transmiten por Internet o por redes potencialmente inseguras. Lo cual plantea riesgos de privacidad y seguridad que no surgen con un servicio telefónico tradicional. Un ejemplo de ello, es que la infraestructura VoIP se puede ver seriamente degrada por el efecto de algún virus, gusano o por el más que conocido SPAM. VoIP es vulnerable además en muchos otros puntos, ya sea en los protocolos utilizados, en los dispositivos que intervienen, o debilidades en la red por la que se transmite.

2.2.7.2. Infraestructura básica VoIP

Dentro de la estructura básica de una red VoIP hay que diferenciar tres elementos fundamentales:

• **Terminales:** Son los dispositivos que utilizarán los usuarios para comunicarse.

Implementados tanto en hardware como en software realizan las funciones de los teléfonos tradicionales.

• **Gateways:** De forma transparente se encargan de conectar las redes VoIP con las redes de telefonía tradicional.

• **Gatekeepers:** Son el centro neurálgico de las redes VoIP. Se encargan de realizar tareas de autenticación de usuarios, control de admisión, control de ancho de banda, encaminamiento, servicios de facturación y temporización.

En la siguiente imagen se puede ver una estructura de red básica entre lo que serían dos delegaciones de una misma empresa conectadas telefónicamente a través de Internet.

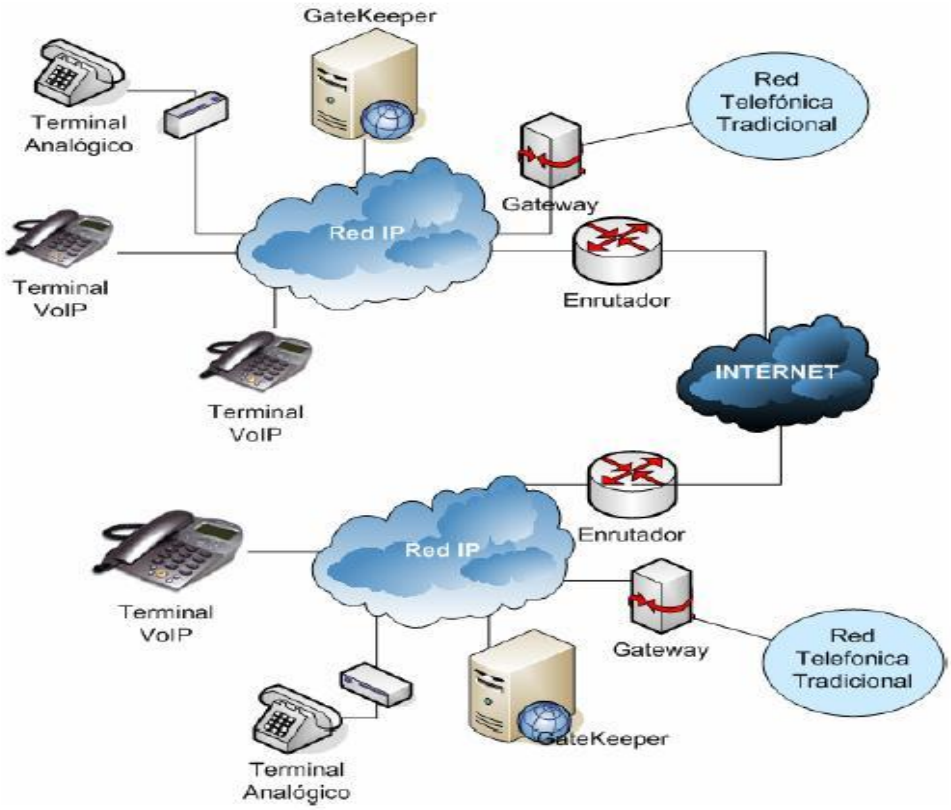


Figura 21 Infraestructura básica VoIP

2.2.7.3. Seguridad en VoIP.

1. La seguridad de VoIP se puede dividir en cuatro áreas: configuración, control de llamadas, flujo de voz y flujo de datos. La configuración se realiza en equipos que se encuentran en la fase de inicio, conectándose al servidor de configuración. Después de la configuración, el equipo puede comenzar el flujo de datos. Este flujo es independiente del control de llamada o del flujo de voz. Cuando el equipo detecta un mensaje entrante se inicia el proceso de control de llamada con un Call Manager/Servidor. Una vez que se establece la conexión el flujo de voz puede ser trasmitido entre dos CPE´s (Customer Premises Equipment, Equipo Local del Cliente).

Configuración **RC4, SSL, TLS, HTTPS**
Control de llamada **TLS, IPSec**
Seguridad de Voz **SRTP**
Seguridad de Datos **IPSec, SSH, VPN de Cisco**
Áreas de Necesidades **-Configuración -Intercambio de claves** **-Autenticación -Encriptación**

2.2.7.4. Componentes de Seguridad en VoIP

Aunque las cuatro áreas tienen diferentes mecanismos de seguridad, los componentes básicos de seguridad son los mismos. Los principales objetivos son autorización, autenticación, integridad, y la

privacidad. Con el fin de alcanzar estos objetivos los mecanismos de seguridad consisten en la configuración, autenticación, intercambio de claves y la encriptación. La configuración es en la etapa inicial donde se autoriza el dispositivo en la red. La autenticación puede tener lugar en la etapa de configuración o más adelante. La encriptación o cifrado es el mecanismo para la lograr la integridad y privacidad y exige una clave de seguridad que puede ser asignada o dinámicamente obtenida a través de intercambio de claves.

2.2.7.5. Medidas de los resultados en la Seguridad de VoIP

Lo principal en las medidas de los resultados en la Seguridad de VoIP consiste en el nivel de seguridad, retraso del cifrado, retraso del mensaje y el poder de procesamiento que lleva. Por lo general cuanto más pequeño es el tamaño del mensaje menor es la seguridad, el tiempo de encriptación y la potencia de procesamiento. Una clave de tamaño inferior a los 56 bits puede ser rota en menos de 3 horas por e quipos sofisticados. Una de 192 bits consume demasiada potencia de caculo y no es deseado por el tiempo que consume, aunque si proporciona un alto nivel de seguridad. La clave ideal es la de 128 bits.

2.2.7.6. Protocolos de cifrado

Breve resumen de los protocolos de cifrado más utilizados en VoIP con sus ventajas:

- **AES (Advanced Encryption Standard)**

AES utiliza una clave de 128 bits, con mucho más alto nivel de seguridad que DES, mientras que la potencia de cálculo es de 3 a 10 veces más que 3DES. AES es un protocolo de cifrado para voz y sistemas de señalización.

- **RC4 (Rivest Cipher)**

El algoritmo de encriptación y desencriptación es el mismo ya que el flujo de datos se fusiona con la secuencia de claves generada. El algoritmo es de serie por exigir sucesivos canjes de entradas del

estado sobre la base de la secuencia de la clave. RC4 es el más común método de cifrado para los archivos de configuración.

- **Protocolo de encriptación de voz—Secure RTP (SRTP)**

SRTP es IETF RFC3711 [4]. SRTP proporciona un marco para el cifrado y el mensaje de autenticación de los flujos RTP y RTCP.SRTP añade dos partes a la cabecera de RTP: autenticación y encriptación. Es opcional para la autenticación SRTP, mientras que se requiere para SRTCP. La encriptación es necesaria para SRTP. Solo la encriptación AES se apoya en SRTP.

2.2.7.7. Métodos de intercambio de claves

Los métodos de intercambio de claves comunes son simétrica, publicas, hibridas y Diffie-Hellman (DH).

- **Clave Simétrica**

Este sistema usa una sola clave para el cifrado y el descifrado. En ambos lados de la llamada se usa la misma clave. La clave puede ser generada por un extremo, y se distribuye hasta el otro extremo, o puede ser asignada por un servidor a todas las partes de un dominio. Este método no es escalable, pero es el más sencillo de todos.

- **Clave Pública**

Este método utiliza dos claves. El extremo remoto utiliza la clave pública para encriptar el mensaje saliente. La clave privada se utiliza para descifrar el mensaje que reciben. Este método es escalable, pero se necesita de 100 a 1000 veces más potencia de cálculo.

- **Clave Hibrida**

Este método usa la clave pública para cifrar la clave simétrica. Una vez que la clave simétrica se recibe, se utiliza para descifrar los mensajes. Este es el método más eficiente y se utiliza en muchas aplicaciones tales como MS Outlook, Netscape Comunicator, y garantiza también el almacenamiento de datos.

- **Clave Diffie-Hellman (DH)**

Los dos extremos que interactúan deben ponerse de acuerdo en la contraseña para que la llamada pueda pasar. Esto es el llamado método Diffie-Hellman. Uno de los dos CPE tiene que elegir un número aleatorio de base 2 y el otro dispositivo tiene que coincidir con este número. Hay cinco algoritmos DH, o grupos. Cuanto mayor sea el grupo más complejo es el algoritmo, lo que se supone una mayor seguridad y un nivel más intenso de cálculos. Debido a su potencia de cálculo este método es el menos utilizado.

2.2.7.8. Asociación de Seguridad (SA)

Una asociación de seguridad es la conexión virtual entre dos o más dispositivos con el propósito de la seguridad. Durante el establecimiento de la SA los dispositivos realizan la autenticación y el intercambio de fichas o certificados, que se utilizan para crear claves de cifrado. Una vez que la SA sea establecida algún dispositivo realizara el intercambio de claves. La etapa más óptima para el establecimiento de la Asociación de Seguridad es en la configuración de CPE

y servidor.

2.2.7.9. Configuración de la seguridad en VoIP

Al inicio, el equipo premisa del cliente proporciona un ID seguro de la red del servidor de configuración. El servidor de configuración responde con una clave de autenticación. El CPE utiliza esta clave para iniciar el proceso de autenticación. Una vez que el CPE es autenticado, el servidor de configuración proporciona una clave de cifrado. A partir de este punto la clave de cifrado se utiliza para cifrar todos los mensajes entre el CPE y el servidor de configuración. Los protocolos más comunes utilizados en este proceso son RC4 (Rivest Cipher), Periodo de la Capa de Sesiones de seguridad (SSL), Seguridad de la Capa de Transporte (TLS).

2.2.8. Conclusiones del capítulo

En este capítulo se observaron las principales áreas de seguridad de la tecnología WiMAX. Estas áreas fueron: uso clandestino de la conexión wireless, donde se estudiaron los protocolos de cifrado de paquetes 3DES, AES y RSA; otra área es la de la autenticación tratada por los certificados digitales tales como X.509, analizándose sus versiones; otra de las áreas es el protocolo de administración de claves PKM, basado en certificados digitales y protocolos de encriptación, contando con varias

versiones. Se realizo un detallado estudio en cada aspecto de la seguridad para realizar una propuesta de los protocolos y certificados, que resultaran más convenientes para su posible implantación en la universidad. Se observo también la seguridad en el protocolo IPv6, ya que sobre este está basada la tecnología WiMAX de cuarta generación, desarrollándose así también un breve estudio de VoIP e IPTV y observando sus principales aspectos a tener en cuenta para la seguridad.

Capítulo 3 Propuesta de Seguridad en WiMAX

3.1. Introducción

En capítulos anteriores se realizo el estudio de la seguridad de la tecnología WiMAX principalmente para la cuarta generación. Se realizaron estudios bastantes profundizados acerca de cada certificado o protocolo de encriptación para así llegar a una conclusión en este capítulo de cuál en estas áreas de seguridad sería el más factible para su utilización en la implantación de la tecnología WiMAX en la Universidad de las Ciencias Informáticas.

La propuesta se realizara teniendo en cuentas las capas del modelo OSI, desglosándolo por capas y observándose así la seguridad en cada una de ellas.

3.2. Propuesta de seguridad teniendo en cuentas las capas del modelo OSI.

El modelo OSI (Open System Interconection) es el modelo de red descriptivo, o sea es la marca de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. A continuación se muestra el modelo separado por capas.

Con el estudio realizado en esta investigación se presentaran en una tabla a continuación las propuestas de seguridad (según en la capa que se encuentre).

7	Nivel de Aplicación	Certificado y firmas digitales
4	Nivel de Transporte	Seguridad en el nivel de Transporte, EAP- TTLS
3	Nivel de Red	IPSec, Arquitectura AAA
2	Nivel de Enlace de Datos(MAC)	AES, PKMv2, X.509v3

3.2.1. Nivel de Aplicación

Para este nivel las técnicas de seguridad son introducidas por el propio operador de la red de los proveedores de servicio y aplicación o incluso de los usuarios finales de la red. Siendo el caso de la UCI, los administradores de la red se encargaran de dar la autorización a los usuarios del dominio y de limitar sus movimientos por la red. Estas medidas pueden ser las mismas que se toman en las redes por cable. En este nivel se aplica lo que es la denegación de servicios.

A continuación se muestra una tabla donde se observa los protocolos y certificados en las acciones de autenticación y autorización donde interviene el usuario y administrador de la red.

Interesados	Criterios de seguridad	Comentario	¿Cómo funciona WiMAX uso de la palabra?
Usuario	Privacidad	Proteger de las escuchas	RSA, PKM, EAP-TLS
	Integridad de los Datos	Proteger los datos de usuario, ser manipulados en de tránsito	RSA, PKM, EAP-TLS
	Acceso a los servicios	Usuario tiene la correcta credenciales	X.509, EAP
	Exactitud de la contabilidad	Precisión y eficiencia de la contabilidad	Arquitectura AAA

Administrador de la red	Autenticación de usuario	¿Es el usuario que dice que es?	x.509, EAP-TTLS
	Dispositivo de autenticación	¿Es el dispositivo correcto?	x.509, EAP-TTLS
	Autorización	¿Es el usuario autorizado para recibir un protocolo servicio?	RSA, EAP, PKMv2
	Control de Acceso	Sólo los usuarios autorizados tienen acceso a los servicios	RSA, EAP, PKMv2

3.2.2. Nivel de Red

La seguridad en el protocolo IP (IPSec) es igual para todas las tecnologías o sea mantiene sus dos aspectos fundamentales: Cabecera de Autenticación y Cifrado de Seguridad, contando también con los protocolos ISAKMP y IKE, este aspecto en la capa de red es invariable.

3.2.3. Capa de Enlace de Datos (AES, PKMv2, X.509v3)

3.2.3.1. AES

Esto se evita mediante el cifrado de datos y la autenticación de los usuarios. Para ello existen varios protocolos, pero el más factible para la implantación de estos en la Universidad de las Ciencias Informáticas es el protocolo AES (Rijndael).

Los motivos por lo que se propone AES como algoritmo de cifrado son: proporciona cifrado más rápido y compatibilidad con una amplia gama de dispositivos. De no ser AES sería necesario disponer de diferentes tecnologías de cifrado para las aplicaciones con fines específicos, tales como la inalámbrica de correo electrónico o la calidad del servicio específico de aplicaciones. Se propone que su implementación se realice en C++, por ser C unos de los lenguajes más potentes y poseer más capacidad en el manejo de memorias e interrupciones que otros programas, además de ser uno de los lenguajes que estudia la UCI. No hay que pagar por utilizar el código, o sea es totalmente gratis.

AES se puede utilizar en claves de 80, 112, 128, 192 y 256. El uso de las claves de 80 bits será seguro hasta el año 2010, 112 hasta el 2020, y 128 posteriormente, lo que no significa un problema para AES.

Los 80 bits de seguridad de AES, equivalen a los 1024 del protocolo RSA. DES está casi descontinuado, 3DES lo estará en los próximos años, por lo que se espera usar AES con 128 bits.

El nivel de la velocidad de cifrado es alto, el tiempo al crack (asumiendo que la maquina pudiera intentar 255 claves por segundo) se tardaría 149 billones de años. Posee también un bajo consumo de los recursos de la maquina.

AES vs TDES

Aspectos	AES	TDES
Tipo de algoritmo	Simétrico, bloques de cifrado.	Simétrico, Cifrado de Feistel
Tamaño de claves(en bytes)	128, 192, 256	112 o 168
Velocidad	Alta	Baja
Tiempo al crack (máquina que procese 255claves/seg)	149 billones de años	4.6 millones de años
Consumo de recursos	Bajo	Alto

3.2.3.2. PKMv2

Este protocolo utiliza un fuerte algoritmo de autenticación basado en el protocolo de encriptación RSA. Posee la ventaja también de adaptarse independientemente de cuál sea el algoritmo de encriptación de la SA, si es DES, utiliza el algoritmo 3DES usando una clave 3DES KEK derivada de la AK. Si la SA utiliza una clave de encriptación de 128 bits este utiliza el algoritmo AES.

3.2.3.3. Certificado X.509v3

El certificado más recomendado para la autorización es el X.509 en su versión 3 ya que esta contiene todos los datos del sujeto (nombre, dirección, correo electrónico y otros datos.). Con esta versión no hace falta aplicar restricciones sobre la estructura de las CAs gracias a la definición de las extensiones de certificados. La principal ventaja de esta versión es que puede hacer el formato de los certificados y los CRLs extensible. Además de contar con tres vías de autenticación.

3.2.4. Nivel de Transporte

Como en la universidad se buscan softwares y protocolos libres, se escogió EAP – TTLS, teniendo en cuenta que funciona sobre todas las plataformas y sistemas operativos y es, a su vez, compatible con los otros EAP y con múltiples bases de datos como SQL y LDAP. Permite a los usuarios autenticarse mediante nombre de usuario y contraseña, sin pérdida de seguridad. Ofrece fuerte autenticación mutua, credenciales de seguridad y llaves dinámicas.

Las ventajas que posee son:

- El más sencillo de instalar y gestionar
- Seguridad difícil de traspasar
- No requiere Certificados Cliente (Obligatorio para EAP-TLS)
- Autentica de manera segura los usuarios frente a base de datos Windows
- Despliegue contra infraestructuras existentes
- Los usuarios se conectan con sus nombres de usuario y contraseñas habituales
- No existe peligro de ataques de diccionario
- Parámetros pre-configurados para el cliente WLAN, facilitando la instalación en los dispositivos WLAN

  Soporta Autentificación de Base de Datos tales como Active Directory, NT Domains, Token Systems, SQL, LDAP (EAP-TLS solo Active Directory).

3.3. Validación de la propuesta aplicando el Método Expertos

3.3.1. Método de Expertos

Mediante el Método de Expertos se pueden tomar decisiones tales como aceptar o rechazar determinada propuesta, en correspondencia con los criterios definidos y la evaluación dada por estos. Tales expertos fueron seleccionados debido a la experiencia profesional que tienen en el área de gestión de proyectos, la cual les permite poder realizar una valoración crítica en cuanto a la factibilidad de la estrategia propuesta.

3.3.2. Explicación del Método de Expertos

A continuación se definen las actividades efectuadas para la identificación de los criterios de evaluación, la selección de los expertos, la evaluación de la estrategia y la obtención de los resultados de la investigación, que permitirán posteriormente determinar la viabilidad de la propuesta de seguridad en WiMAX.

- *Actividad 1*: Identificar los criterios de evaluación en función de la estrategia y agruparlos convenientemente.
- *Actividad 2*: Establecer y evaluar el peso de cada grupo dependiendo de su valor representativo dentro de la estrategia.
- *Actividad 3*: Convocar y organizar un Comité de Expertos conformado como mínimo por 7 miembros.
- *Actividad 4*: Entregar a cada experto la estrategia, para un análisis previo a la evaluación de la misma. Serán entregados además a cada experto dos modelos en cuestión: en el primero (Consultar Anexo 1) se evaluarán los criterios en una escala del 1 al 5, seguidamente se podrá evaluar de forma cualitativa la apreciación de cada experto sobre la propuesta siguiendo los términos calificativos siguientes: excelente, bueno, aceptable, cuestionable y malo; también se brinda a los expertos la posibilidad de registrar criterios y consideraciones personales sobre la propuesta. Una vez recogidos el modelo comienza el proceso de verificación de la consistencia del trabajo de los expertos, así como los para determinar el índice de aceptación de la propuesta y la probabilidad de éxito de la misma.
- *Actividad 5*: Determinar por cada criterio en cuestión el peso promedio, partiendo de los pesos dados por los expertos. (Consultar Anexo 2)
- *Actividad 6*: Verificar la consistencia del trabajo de los expertos mediante el coeficiente de concordancia de Kendall y el estadígrafo Chi Cuadrado (Consultar Anexo 3). En caso de que existan inconsistencias en el trabajo realizado por los expertos este debe realizarse nuevamente.
- *Actividad 7*: Calcular el producto de: el peso relativo de cada criterio (P) y la calificación promedio dada por los expertos (c) o sea (P x c) (Consultar Anexo 4).
- *Actividad 8*: Calcular índice de aceptación de la estrategia propuesta.

- *Actividad 9*: Determinar la probabilidad de éxito de la estrategia propuesta.

3.3.3. Aplicación del Método de Expertos

- *Actividad 1*: Conformar criterios de evaluación y organizarlos por grupos.

- Grupo No. 1: Criterios de Valor científico
  - ✓ Valor científico de la investigación.
  - ✓ Calidad de la investigación desarrollada.
  - ✓ Novedad científica de la investigación.
- Grupo No. 2: Criterios de implantación
  - ✓ Necesidad real de implantación de la propuesta.
  - ✓ Posibilidad de ser aplicada la propuesta.
  - ✓ Integración de la propuesta cuando se implante la tecnología en la UCI.
- Grupo No.3: Criterios de adaptación
  - ✓ Adaptabilidad de la propuesta en la UCI.
  - ✓ Integración de la propuesta con la tecnología.
  - ✓ Integración con el entorno de producción donde se aplique.
- Grupo No.4: Criterios de impacto
  - ✓ Repercusión de la propuesta al implantarse la tecnología.
  - ✓ Organización en el proceso de documentación de la investigación.
  - ✓ Nivel de utilidad de la propuesta.

- *Actividad 2*: Partiendo de la importancia concedida a cada aspecto a evaluar, se determina que el peso asignado a cada uno es el siguiente sumando estos un total de 100.
  - Grupo No.1: Criterios de Valor científico...…….20

- Grupo No. 2: Criterios de implantación…….....20
- Grupo No.3: Criterios de adaptación……...30
- Grupo No.4: Criterios de impacto.....….30

- *Actividad 3*: Han sido seleccionados 7 especialistas para la conformación del Comité de Expertos, teniendo como aspectos importantes en su selección las siguientes características:
  - Experiencia en redes inalámbricas: los especialistas seleccionados para conformar el Comité de Expertos tienen como experiencia acumulada en redes inalámbricas 5.3 años de experiencia / experto.
  - Grado científico de los expertos: todos los expertos consultados son ingenieros.
  - Plazas de los expertos que los vincula con las redes inalámbricas: Existe un administrador del nodo central de la UCI, un Jefe de redes de la UCI, un jefe de departamento de Sistemas Digitales y cuatro profesores de la asignatura de Teleinformática.
- *Actividad 4*: Fueron entregados los modelos a cada experto, registrándose en los modelos la información de la evaluación y la clasificación final de la misma por parte de cada experto.
- *Actividad 5*: Cálculo por cada criterio en cuestión del peso promedio, partiendo de los pesos dados por los expertos.

Grupo	C / E	E1	E2	E3	E4	E5	E6	E7	ΣE	Exp. P
20	C 1	6	9	5	7	8	6	10	51	7.28571429
	C 2	7	8	8	7	6	8	6	50	7.14285714
	C 3	8	7	7	6	6	8	7	49	7
20	C 4	8	8	6	5	7	7	9	50	7.14285714
	C 5	10	7	10	10	11	10	10	68	9.71428571
	C 6	8	6	7	8	8	6	7	50	7.14285714
30	C 7	10	10	9	7	11	8	10	65	9.28571429
	C 8	9	10	12	10	9	10	9	69	9.85714286
	C 9	10	10	9	10	9	12	8	68	9.71428571
30	C 10	8	10	10	10	8	7	10	63	9
	C 11	10	9	8	10	10	11	9	67	9.57142857
	C 12	6	6	9	10	7	7	5	50	7.14285714
Totales		100	100	100	100	100	100	100	700	100.000

Peso Promedio / Criterio

- *Actividad 6*: Determinación de la consistencia en el trabajo de los expertos: Dado C el número total de criterios a evaluarse, y E el número de expertos involucrados en la evaluación, se realiza el siguiente procedimiento para determinar la consistencia en el trabajo de los expertos:

  - Calcular para cada criterio: ΣE, que representa la sumatoria del peso dado por los expertos.
  - Determinar el valor de PE: puntuación promedio de cada criterio.
  - Calcular peso medio de cada criterio MΣE.
  - Hallar el valor de ΔC, diferencia existente entre ΣE y MΣE.
  - Determinar la desviación de la media, que posteriormente se eleva al cuadrado para obtener la dispersión S, dada por la expresión: $S = \Sigma (\Sigma E - \Sigma E / C)^2$.
  - Conociendo la dispersión se puede calcular el coeficiente de concordancia de Kendall W, dado por la expresión: $W = S / E^2 (C^3 – C)/ 12$.
  - Calcular el Chi cuadrado real a partir del valor del coeficiente de Kendall teniendo en cuenta la siguiente expresión: $X^2 = E (C-1) W$.

A continuación se muestran los datos obtenidos luego de realizar los pasos anteriores:

C / E	E1	E2	E3	E4	E5	E6	E7	ΣE	Exp. P	ΔC	ΔC²
C 1	6	9	5	7	8	6	10	51	7.28571429	7.33	53.729
C 2	7	8	8	7	6	8	6	50	7.14285714	8.33	69.389
C 3	8	7	7	6	6	8	7	49	7	9.33	87.049
C 4	8	8	6	5	7	7	9	50	7.14285714	8.33	69.389
C 5	10	7	10	10	11	10	10	68	9.71428571	8.33	69.389
C 6	8	6	7	8	8	6	7	50	7.14285714	8.33	69.389
C 7	10	10	9	7	11	8	10	65	9.28571429	6.67	44.489
C 8	9	10	12	10	9	10	9	69	9.85714286	10.67	113.849
C 9	10	10	9	10	9	12	8	68	9.71428571	9.67	93.509
C 10	8	10	10	10	8	7	10	63	9	4.67	21.809
C 11	10	9	8	10	10	11	9	67	9.57142857	8.67	75.169
C 12	6	6	9	10	7	7	5	50	7.14285714	9.67	93.509
Totales	100	100	100	100	100	100	100	700	100.000	100.00	860.6668
MΣE	58.33										
W	0.099										
X²	7.623										

Consistencia en Trabajo de Expertos

Posteriormente, se compara el X^2 real, con el valor del dato estadístico, siendo $\alpha=0.01$, y $C=12$ y debe cumplirse que $X^2 < X^2 (\alpha; c-1)$ para que el trabajo realizado por los expertos sea valorado de consistente.

$X^2 (\alpha; c-1) = X^2 (0,01; 11) = 24.72$

Por tanto $X^2 < X^2 (\alpha; c-1)$ lo que es ,7.623 < 24.72, quedando demostrada la consistencia del trabajo realizado por los expertos.

- *Actividad 7*: Calcular el producto de: el peso relativo de cada criterio (P) y la calificación promedio dada por los expertos (c) o sea (P x c)

Criterios	P	c	P * c
C 1	0,0728	4	0,2912
C 2	0,0714	4	0,2856
C 3	0,07	4	0,28
C 4	0,0714	5	0,357
C 5	0,0971	4	0,3884
C 6	0,0714	4	0,2856
C 7	0,0928	4	0,3712
C 8	0,0985	5	0,4925
C 9	0,0971	5	0,4855
C 10	0,09	4	0,36
C 11	0,0957	4	0,3828
C12	0,0714	5	0,357
Totales			4,3368

Cálculo de P * c

- *Actividad 8*: Calcular Índice de Aceptación (IA) de la estrategia propuesta. Partiendo de la siguiente fórmula. IA = (P * c) / 5

Si (P * c) = 4,3368 entonces IA = 4,3368 / 5 obteniéndose IA = 0.8673.

- *Actividad 9*: Probabilidad de éxito de la estrategia propuesta.

Se determina a partir de los rangos predefinidos del índice de aceptación:

IA > 0,7. . . . . Existe Alta probabilidad de éxito

0,7 > IA > 0,5. . . . . Existe probabilidad Media de éxito

0,5 > IA > 0,3. . . . . Existe Baja probabilidad de éxito

0,3 > IA. . . . . No existe probabilidad Ninguna de éxito

Dado el resultado de IA igual a 0.8673 entonces se puede concluir que la probabilidad de éxito es: Alta

3.4. Conclusiones del capitulo

En este capítulo se dieron a conocer las propuestas de la seguridad teniendo en cuenta las capas de modelo OSI que poseen aspectos de la seguridad. Se comparó y analizo cada aspecto presentado en

el capitulo dos, proponiéndose los protocolos y certificados más óptimos para su implante en la UCI, validada la propuesta por el Método de Expertos.

Conclusiones Generales

Una vez concluida la investigación se cumplieron los objetivos planteados y se arribó a los siguientes resultados.

- Se consideraron todos los aspectos para proporcionar información sobre la seguridad en la tecnología WiMAX.
- Se examinaron los protocolos de encriptación que se pudieran implementar para lograr un cifrado de datos de alta calidad.
- Se analizaron los certificados digitales y la arquitectura AAA para la autorización y autenticación, justificando las propuestas trazadas para su implementación e instalación al implantarse la tecnología.

Esta investigación servirá de base para el montaje y puesta a punto de la tecnología WiMAX cuando se cuente con los dispositivos necesarios en la Universidad de Ciencias Informáticas.

Recomendaciones

Sobre el presente trabajo se recomienda:

- Que la propuesta de la investigación sea consultada en el momento que se implante la tecnología WiMAX en la Universidad de las Ciencias Informáticas.
- Que sean implementados los algoritmos matemáticos planteados en la investigación para la correcta aplicación de las políticas de seguridad en la tecnología WiMAX.
- Que se mantenga un monitoreo constante sobre posibles problemas de seguridad que se puedan dar durante la implantación de la tecnología.
- Que se continúe el estudio de la tecnología para posibles actualizaciones o nuevas variantes más seguras de estos algoritmos que puedan surgir.

Anexos

Anexo 1 Plantilla de Modelo para calificar los criterios.

Modelo para calificar los criterios

Nombre del evaluador: _____

Fecha de entrega: _____

Fecha de recogida: _____

1- Evaluación de los criterios en una escala del 1 al 5:

Grupo 1: Criterios de Novedad Científica	
Criterio	**Evaluación**
Valor científico de la investigación.	
Calidad de la investigación desarrollada.	
Novedad científica de la investigación.	
Grupo 2: Criterios de Implantación	
Criterio	***Evaluación***
Necesidad real de implantación de la propuesta.	
Posibilidad de ser aplicada la propuesta.	
Integración de la propuesta cuando se implante la tecnología en la UCI.	
Grupo 3: Criterios de Factibilidad	
Criterio	***Evaluación***
Adaptabilidad de la propuesta en la UCI.	
Integración de la propuesta con la tecnología.	
Integración con el entorno de producción donde se aplique.	
Grupo 4: Criterios de Adaptabilidad	
Criterio	***Evaluación***
Repercusión de la propuesta al implantarse la tecnología.	
Organización en el proceso de documentación de la investigación.	
Nivel de utilidad de la propuesta.	

2- Categoría final de la propuesta:

____ Excelente: alta novedad científica, grandes posibilidades de aplicabilidad y relevantes resultados esperados.

____ Bueno: novedoso científicamente y con buenos resultados esperados.

____ Aceptable: no es lo suficientemente bueno, pero puede aplicarse.

____ Cuestionable: sin relevancia científica y con resultados esperados no satisfactorios.

____ Malo: no aplicable

3- Evaluación final:

- Sugerencias del evaluador para mejorar los procesos propuestos.
- Elementos que deben mejorarse.

Anexo 2 Plantilla de Modelo para definir el peso de los criterios.

Modelo para definir el peso de los criterios

Nombre del evaluador: _____

Fecha de entrega: _____

Fecha de recogida: _____

Usted debe otorgarle a cada criterio un peso en dependencia del peso total dado al grupo al que pertenece:

Grupo 1: Criterios de Novedad Científica … 20	
Criterio	***Peso***
Valor científico de la investigación.	
Calidad de la investigación desarrollada.	
Novedad científica de la investigación.	
Grupo 2: Criterios de Implantación … 20	
Criterio	***Peso***
Necesidad real de implantación de la propuesta.	
Posibilidad de ser aplicada la propuesta.	
Integración de la propuesta cuando se implante la tecnología en la UCI.	
Grupo 3: Criterios de Factibilidad … 30	
Criterio	***Peso***
Adaptabilidad de la propuesta en la UCI.	
Integración de la propuesta con la tecnología.	
Integración con el entorno de producción donde se aplique.	
Grupo 4: Criterios de Adaptabilidad … 30	
Criterio	***Peso***
Repercusión de la propuesta al implantarse la tecnología.	
Organización en el proceso de documentación de la investigación.	
Nivel de utilidad de la propuesta.	

Anexo 3 Plantilla para determinar el peso promedio por criterio.

C / E	E1	E2	E3	E4	E5	E6	E7	ΣE	Exp. P
C 1									
C 2									
C 3									
C ,,									
C n									
C 4									
Totales									

Anexo 4 Plantilla para determinar Consistencia en Trabajo de Expertos.

C / E	E1	E2	E3	E4	E5	E6	E7	ΣE	Exp. P	ΔC	ΔC²
C 1											
C 2											
C 3											
C ,,											
C n											
C 4											
Totales											
MΣE											
W											
X²											

Anexo 5 Plantilla para determinar el producto del peso promedio de cada criterio y la calificación promedio de cada criterio concebida por los expertos.

Criterios	P	c	P * c
C 1			
C 2			
C 3			
C..			
Cn			
Totales			

Bibliografía

Agelet, F. A. 2006. *WIMAX 802.16.* 2006.

Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados .

Análisis del algoritmo de seguridad de redes WiMAX. . s.l. : Universidad Rafael Bellosos. Zulia, Venezuela.

Ángel, José de Jesús. *AES - Advanced Encryption Standard. .*

Corletti., Ing. Alejandro. *IPSec. Protocolo IPSec.* s.l. : Universidad de Madrid.

Crear una biblioteca de cifrado DES, Triple DES, RC2 y Rijndael en .Net.

CRIPTOGRAFÍA 5ºCURSO DE INGENIERÍA INFORMÁTICA. E.T.S.I. Informática. Criptografía simétrica. . s.l. : Universidad de Sevilla.

Forado, R. *SEGURIDAD EN REDES WIMAX.*

Francisconi, Hugo Adrian. *IPsec en Ambientes en IPv4 e IPv6.*

García, Gonzalo Álvarez Marañón y Pedro Pablo Perez. *Seguridad en redes inalámbricas Wi-Fi. .*

García., Federico. *Certificados X.509.*

Gil., Roberto Gutiérrez. *Seguridad en VoIP: Ataques, Amenazas y Riesgos.* s.l. : Universidad de Valencia.

González, I. G. R. 2006. *Redes Inalámbricas de Banda Ancha.* 2006.

http://www.publispain.com/adsl/ . [En línea]

IEEE 802.16 WiMAX Security. . **Wongthavarawat, Dr. Kitti.**

Intel. 2005. *Intel® PRO/Wireless 5116 Broadband Interface.* 2005.

01/21/2005. *Introducción a las redes inalámbricas.* 01/21/2005.

IPSec., El protocolo IPv6 y sus extensiones de seguridad. *Gabriel Verdejo Alvarez.* s.l. : Universidad Autónoma de Barcelona.

IPTV. Security. Protecting High-Value Digital Conte.

Robles, G. *Wireless MAN.*

Santidrián, Lourdes López. *ORGANIZACIÓN Y JERARQUIZACIÓN DE AUTORIDADES DE CERTIFICACIÓN PARA LA PROVISIÓN DE SERVICIOS DE SEGURIDAD EN REDES TELEMÁTICAS.*

Seguridad en redes WMAN y GPRS Ing. José Pablo Esquivel CCSP,CCNP. **Ing. José Pablo Esquivel CCSP, CCNP.**

Sierra, José María. *Seguridad a nivel de red. Arquitectura de IPSec. .*

WiMAX Security for Real-World Network Service Provider Deployments.

WiMAX™ System Evaluation Methodology. **Forum., WiMAX.**

www.pdfoo.com. [En línea]

www.verisign.es. [En línea]

www.wimax.com. [En línea]

Referencias Bibliográficas.

- **[1]** Montaje de WiMAX. Diseño de una red WiMAX para la Universidad de las Ciencias Informáticas. Jeanlup Castro y Miguel Garcia.
- **[2]** http://www.wimax.com/education
- **[3]** http://www.Wi-Fi.org
- **[4]** http://es.wikitel.info/wiki/LTE
- **[5]** IEEE http://www.ieee.org/portal/web/aboutus
- **[6]** Gónzalez, I. G. R. (2006). "Redes Inalámbricas de Banda Ancha."
- **[7]** Moreno Tablado, Alberto. Seguridad en Bluetooth. Madrid, Junio 2006.
- **[8]** TDES from http://www.tech-faq.com/lang/es/triple-des-data-encryption-standard.shtml
- **[9]** AES (Rijndael) de http://www.tech-faq.com/lang/es/aes-advanced-encryption-standard-rijndael.shtml.
- **[10]** http://es.tech-faq.com/x.509.shtml
- **[11]** http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/746/2/10485CAP2.pdf
- **[12]** http://www.scribd.com/doc/2926337/El-Protocolo-IPv6-y-sus-extensiones-de-seguridad-IPSec
- **[13]** Seguridad en VoIP: At
- **[14]** Ataques, Amenazas y Riesgos. Roberto Gutiérrez Gil.

Glosarios de términos

- **AAA:** *Authentication, Authorization and Accounting.* Autenticación, autorización y contabilidad.
- **ADSL:** *Asymmetric Digital Subscriber Line*. Línea de Abonado Digital Asimétrica
- **AK:** *Authentication Key.* Clave de authentication.
- **AP:** *Access Point.* Punto de acceso en redes WLAN.
- **ATM:** *Asíncronos Transfer Modo*. Modo de transferencia asíncrono (MTA). Tecnología de transferencia de datos a alta velocidad, basada en el empleo de paquetes (células) de tamaño fijo y pequeño, lo que supuestamente lo hace muy adecuado para manejar tipos de tráfico muy heterogéneo (voz, vídeo y datos genéricos.)
- **BWA:** *Mobile Broadband Wireless Access*. Acceso inalámbrico móvil de banda ancha.
- **CA:** Autoridad de Certificación.
- **CDMA:** *Code Division Multiple Access*. Acceso múltiple por división en código.
- **CPE:** *Customer Premises Equipment*. Equipos de cliente. Se refiere a los equipos que es necesario instalar en el domicilio del cliente, como son, por ejemplo, los routers y los módems.
- **CRL:** *Certificates Revoked List*. Listas de Certificados Revocados
- **EAP:** *Extensible Authentication Protocol*. Protocolo de autenticación extensible. Protocolo de seguridad para redes que permite mecanismos de autenticación múltiples, dependiendo del sistema operativo empleado.
- **EAP-AKA:** ***E****AP-Authentication and Key Agreement* .Acuerdo de la autenticación y la clave.
- **EAP-PSK:** *EAP-PreShared Key*.Clave precompartida.
- **EAP-SIM:** *EAP-Subscriber Identity Module*. Modulo de identidad del suscriptor.
- **EAP-TLS:** *EAP-Transport Layer Security.* Capa de seguridad de transporte.

- **EAP-TTLS:** *EAP-Tunnelled Transport Layer Security*. Capa de seguridad de transporte tunelizada.
- **IEEE:** *Institute of Electrical and Electronics Engineers*. Instituto de Ingenieros Electrónicos y Eléctricos (www.ieee.org).
- **IETF:** *Internet Engineering Task Force*. Foro de definición de los protocolos de Internet (www.ietf.org).
- **IP:** *Internet Protocol*. Uno de los protocolos del conjunto TCP/IP para comunicaciones de datos (www.ietf.org/ip).
- **IPSec:** *IP Security*. Seguridad en IP.
- **IPTV:** Televisión sobre el protocolo IP.
- **KEK:** *Key Encryption Key*. Clave de encriptación de clave.
- **LAN:** *Local Area Network***.** Redes de área local.
- **LOS:** *Line of Sight*. Línea de vista.
- **MAN:** *Metropolitan Area Network.* Redes de área metropolitanas.
- **MIMO:** *Multiple Input Multiple Output*. Sistema de múltiples entradas y múltiples salidas. Se refiere comúnmente a los sistemas de antenas con gestión inteligente de trayectos múltiples.
- **MAC:** *Medium Access Control*. Control de acceso al medio. Capa del modelo lógico de protocolos donde se engloban todos los mecanismos de gestión de acceso de los diferentes nodos de una red con acceso múltiple a un mismo medio (radio, cable).
- **MAN:** *Metropolitan Area Netwrok*. Red de Área Metropolitana.
- **MS-CHAPv2:** *Microsoft-Challenge Handshake Authentication Protocol*. Protocolo de autenticación por desafío mutuo de Microsoft versión 2. MS-CHAPv2 proporciona autenticación mutua, la generación de claves de cifrado de datos iniciales más seguros para cifrado punto a punto y distintos claves de cifrado para los datos enviados y los datos recibidos.

- **NLOS:** *No Line of Sight*. Sin visión directa. Término que indica la situación relativa de un transmisor y un receptor entre los que no hay visión óptica directa, y por lo cual a frecuencias radioeléctricas elevadas se produce una alta atenuación en el enlace.
- **OFDM:** *Orthogonal Frequency Division Multiplexing*. Multiplexado por división ortogonal en frecuencia.
- **PDU:** *Protocol Data Unit*. Unidad de Datos de Protocolo
- **PHY:** *Physical Layer*. Capa física.
- **PKI:** *Public Key Infrastructure.* Infraestructura de clave pública. Sistema formado por los servicios que hacen posible el soporte de la aplicación de firmas digitales y cifrado de la información.
- **PKM:** *Private Key Management*. Administración de la clave privada
- **QoS:** *Quality of Service*. Calidad de Servicio. Término genérico para definir el conjunto de parámetros que definen el tipo y la calidad del servicio proporcionado.
- **RSA:** *Rivest-Shamir-Adleman*. Iníciales de los nombres de los creadores del protocolo de encriptación RSA.
- **TEK:** *Traffic Encryption Keys*. Clave de encriptación del tráfico.
- **TLS:** *Transport Layer Security*. Capa de transporte de seguridad.
- **VPN:** *Virtual Private Network*. Red privada virtual.
- **VoIP:** *Voz sobre IP*. Tecnología de transmisión de voz a través de redes IP.
- **WLAN:** *Wireless Local Area Network*. Red inalámbrica de área local.
- **WMAN:** *Wireless Metropolitan Area Netwrok*. Red de Área Metropolitana Inalámbrica.
- **WiMAX:** *Worldwide Interoperability for Microwave Access*. Interoperabilidad Mundial para Acceso por Microondas. Tecnología para el bucle de usuario inalámbrico de banda ancha basada en el estándar IEEE 802.16. Sello de compatibilidad con las Glosario de términos y acrónimos 417 pruebas de certificación en interoperabilidad de dicha tecnología (ver « www.WiMAXforum.org »).

- **WAN:** *Wide Area Network*. Red de área extensa. Red de datos constituida entre nodos situados en emplazamientos distantes y unidos entre sí por líneas de comunicación.
- **WWAN:** *Wireless Wide Area Network*. Redes amplias inalámbricas
- **Wi-Fi:** *Wireless Fidelity*. Sello de cumplimiento para implementaciones de sistemas WLAN (IEEE 802.11) según las normas de interoperabilidad definidas por la alianza Wi-Fi (www.Wi-Fi.org).
- **3G:** Tercera generación de comunicaciones móviles. Denominación genérica para referirse a las redes móviles digitales posteriores a los primeros sistemas digitales. Generalmente engloba las redes consideradas bajo el paraguas del IMT-2000 (www.itu.int), aunque el término 3G es anterior.
- **4G:** Cuarta generación de comunicaciones móviles.