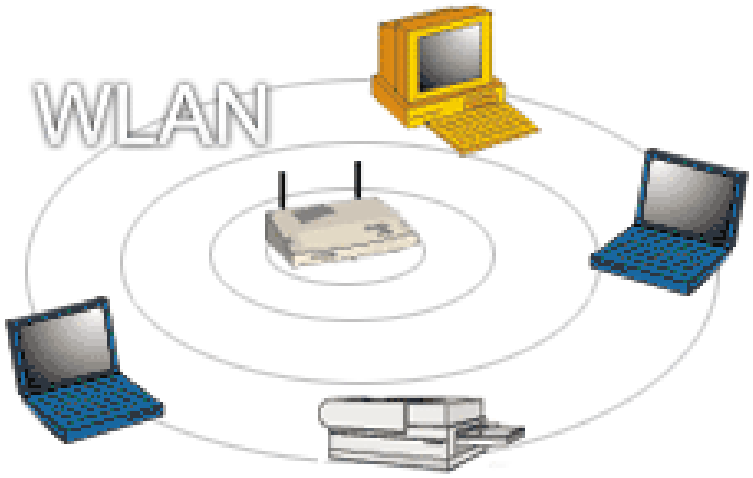
CAPITULO I



INTRODUCCIÓN A LAS SEGURIDADES DE REDES WLAN

La red inalámbrica de área local "WLAN[1]" es un sistema flexible de comunicación de datos implementado como extensión, o alternativa a una red cableada. Las redes WLAN transmiten y reciben datos por aire mediante tecnología de radiofrecuencia, minimizando la necesidad de disponer de conexiones cableadas lo que, a su vez, combina la conectividad de datos con la movilidad de usuarios [LIB01]. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red, conectada con el Punto de Acceso (AP), como se ve en la Figura 1.1

Figura 1.1: Conexión física de la WLAN

Sin embargo, en una red inalámbrica desplegada en un centro de cómputo un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la institución, 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.

[1] **WLAN** Wíreless Lan Area Network, Redes de Área Local Inalámbricas

Cualquiera podría estar escuchando la información transmitida, y no sólo eso, sino que también se pueden introducir nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

El IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos) publicó un mecanismo opcional de seguridad, denominado "WEP[2]", en la norma de redes inalámbricas "802.11[3]", WEP, desplegado en numerosas redes WLAN, ha sido vulnerado de distintas formas, lo que lo ha convertido en una protección inservible. Para solucionar sus deficiencias, el IEEE comenzó en el desarrollo de nuevas norma de seguridad, como es el 802.11b, 802.11a, 802.11i, etc, que han permitido dotar de seguridad a las redes WLAN.

1.1.- Propiedades de la información

La información que circula por la red, su proceso y almacenamiento esta sometida a varios tipos de amenazas, tales como espionaje, acceso no autorizado, interrupción del flujo, copia, alteración, destrucción de información e interrupción de los servicios.

Por lo que; las propiedades de la información permiten identificar si esta mantiene toda su integridad desde el emisor hacia el o los receptores, estas propiedades se describen a continuación [www01].

- ✓ **Confidencialidad.-** Es la propiedad por la que el destinatario de una comunicación puede conocer la información que está siendo enviada mientras que las personas que no son destinatarios no pueden determinar el contenido de lo que está siendo enviado.

[2] **WEP** Wíred Equivalent Privacy (privacidad equivalente a los sistemas inalámbricos)
[3] **802.11** Estándar inicial de redes WLAN

- ✓ **Integridad.-** Es la propiedad de asegurar que la información sea transmitida desde su origen hasta su destino sin sufrir ninguna alteración.

- ✓ **autentificación.-** Es la propiedad de conocer que la información recibida es la misma que la información enviada y que el que dice ser que los envió realmente los envió

1.2.- Descripción del Modelo de red OSI

Este tipo de redes se diferencian de las convencionales principalmente en la capa física y en la capa de enlace de datos, según el modelo de referencia OSI[4], La capa física PHY[5], indica como son enviados los bits de una estación a otra La capa de Enlace de Datos MAC[6], se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores, las demás capas se encargan de los protocolos, de los puentes, encaminadores o puertas de enlace que se utilizan para conectarse.

1.2.1.- Capa Física (PHY)

El IEEE 802.11 provee varias opciones en su capa física (PHY). Estas tecnologías llamadas "Direct Sequence Spread Spectrum, Espectro Amplio mediante Secuencia Directa (DSSS)", "Frequency Hopped Spread Spectrum, Espectro Amplio mediante Saltos de Frecuencia (FHSS).", "Orthogonal Frequency Division Multiplexing, Multiplexación de división frecuencia ortogonal OFDM", y "Infrarrojo IR", fueron diseñadas para las comunicaciones inalámbricas operando en las bandas de frecuencia de 2.4 y 5 GHz no licenciadas del ISM. (Industrial, Scientific and Medical, Bandas de uso industrial. Científico y Médico), como se ve en la Figura. 1.2 [www02].

[4] **OSI** Open Systems Interconnection, Interconexión de sistemas abiertos
[5] **PHY** Physical Signaling Layer , Acceso al Medio Físico
[6] **MAC** Media Access Control, Control de Acceso a Medios

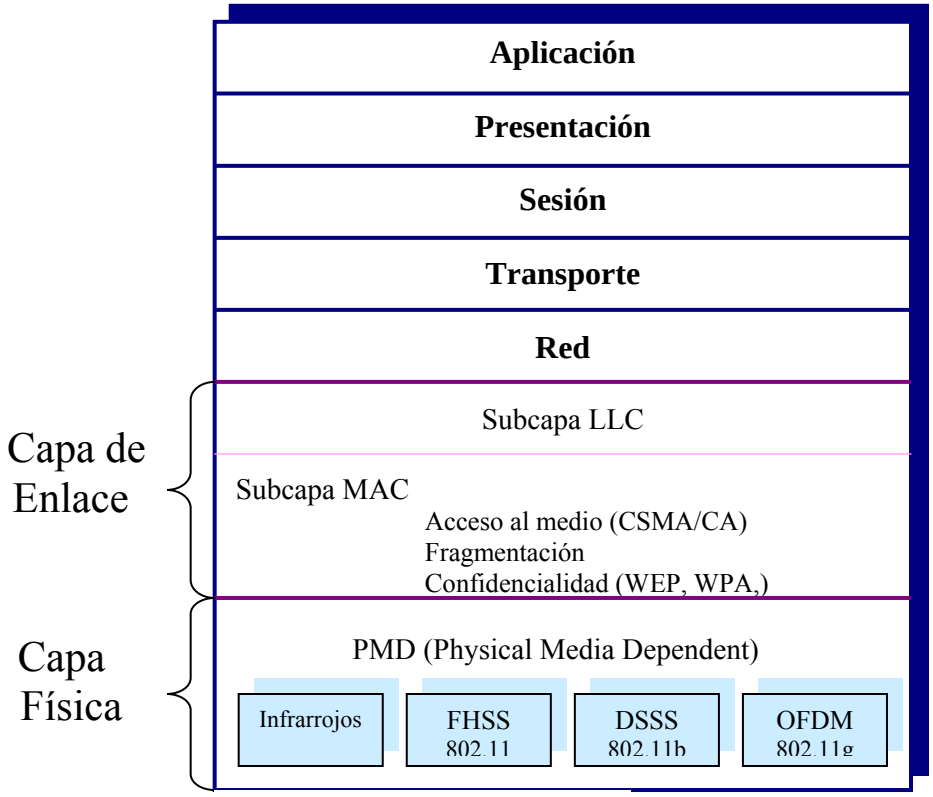


Figura 1.2: Modelo OSI y 802.11

1.2.2.- Capa de Enlace de Datos MAC

La capa MAC es la encargada de asociar un cliente inalámbrico con un punto de acceso (AP). Cuando un cliente entra en la cobertura de uno o más puntos de acceso, se elige uno de ellos al cual se vincula, basándose en criterios sobre la potencia de la señal recibida al igual que un faro. Una vez vinculado un punto de acceso, el cliente sintoniza un canal de radio en el que el punto de acceso está configurado.

La capa de enlace de 802.11 se subdivide en dos subcapas: LLC[7] y MAC, como vemos en la figura 1.2. La primera de ellas emplea la misma subcapa LLC con una dirección de 48 bits empleada también en las redes LAN 802.3. Debido a la imposibilidad de emplear la técnica de 802.3 CSMA/CD[8], dada la imposibilidad de "escuchar" una colisión, 802.11 emplea una modificación del protocolo

[7] **LLC** Logical Link Control
[8] **CSMA/CD** Carrier Sense Multiple Access with Collision Detect

denominada CSMA/CA[9]. Este protocolo evita las colisiones, enviando un paquete de reconocimiento (ACK) para confirmar la llegada al receptor del paquete enviado. Finalmente, la capa MAC ofrece dos características que mejoran la robustez del estándar: comprobación de suma CRC (Cyclic Redundancy Check) y fragmentación de paquetes. Cada paquete lleva asociado un CRC para asegurar que este no se ha corrompido en la transmisión. Esta es una diferencia con respecto a redes cableadas, ya que esta dejaba tales comprobaciones a los protocolos de niveles superiores. [www03].

1.3.- Tecnología WLAN

Aunque este estudio está dirigido a las seguridades de redes inalámbricas LAN, no se puede pasar por alto la constitución, topología y tecnologías de comunicación en las que se compone una WLAN.

La topología de estas redes consta de dos elementos, las estaciones cliente y los Access Point (AP), llamadas **Infrastructure y Ad-Hoc**, la comunicación puede realizarse entre las estaciones clientes o a través del Access Point, como veremos en la Figura 1.3 y Figura 1.4

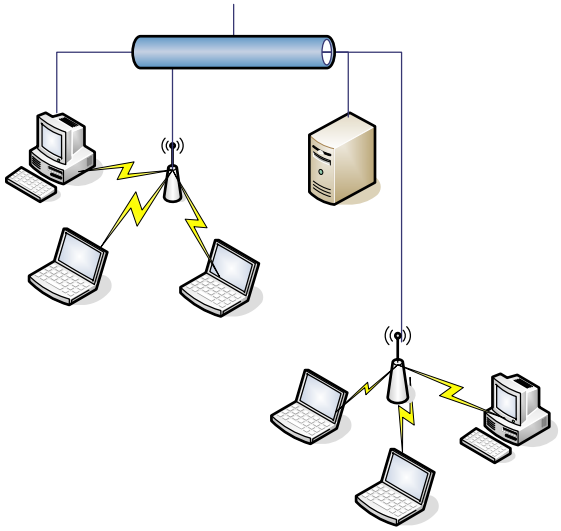


Figura 1.3: Modo Infraestructura

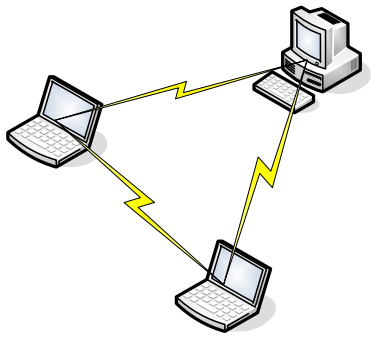


Figura 1.4: Modo Ad-Hoc o redes **aisladas**

[9] **CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance

En caso de estar con seguridad la comunicación puede realizarse entre el cliente, Access Point y el servidor de autenticación, produciéndose la asociación entre ellos, el Access Point transmite señales de gestión periódicas, el cliente las recibe e inicia la autenticación mediante el envió de una trama de autenticación, una vez realizado esto, la estación cliente envía una trama asociada y el Access Point responde con otra.

Las redes inalámbricas LAN en los últimos años han tenido un gran avance con la integración de nuevas tecnologías que permiten una mejor implementación de este tipo de redes. Las redes WLAN para su comunicación se basan en radiofrecuencia (RF) y luz infrarroja (IR).

Las comunicaciones inalámbricas a través de RF utiliza el sistema de radio de banda estrecha y sistema de banda ancha (Expansión de espectro), está última utiliza técnicas de expansión de espectro por salto de frecuencia FHSS y expansión de espectro por secuencia directa DSSS. [www02].

1.3.1.- Sistemas de radiofrecuencia (RF)

Los organismos de los distintos países encargados de regular la concesión de licencias sobre el espectro de radio han dispuesto una serie de frecuencias para el uso comercial sin licencia. Estas bandas ISM incluyen las bandas de 900 MHz, 2,4 MHz y 5 GHz utilizada por los dispositivos WLAN.

La mayoría de dispositivos que son utilizados para redes inalámbricas lan utilizan la frecuencia de 2,4 – 2,4835 GHz debido a su medio transmisión y a las menores interferencias que en ella producen. Hay varios medios de transmisión capaces de transmitir datos mediante ondas electromagnéticas como son sistemas de radio de banda estrecha y sistemas de banda ancha, atendiendo a su **capa física**. [www02].

1.3.1.1.- Sistema de radio de banda estrecha

Los sistemas de radio de banda estrecha transmiten y reciben datos en una frecuencia de radio específica, la limitación natural de este sistema resulta clara: si otro transmisor está operando a la misma frecuencia y dentro del rango de cobertura, se produce una interferencia y los datos se perderán o dañarán

1.3.1.2.- Sistemas de radio de banda ancha: Expansión de espectro

En lugar de utilizar una única frecuencia, la tecnología de expansión de espectro recorre la banda de frecuencias disponible para transmitir los datos. Está tecnología distribuye la señal sobre un amplio rango de frecuencias de manera uniforme, la forma de transmisión de banda ancha permite a los dispositivos evitar las interferencias y los ruidos provocados por otras señales.

Existen dos tecnologías de espectro expandido: la tecnología de expansión de espectro por salto de frecuencia FHSS y la tecnología de expansión de espectro por secuencia directa DSSS. De las dos, la tecnología de salto de frecuencia es más barata de implantar; sin embargó la tecnología de secuencia directa tiene un potencia de utilización mas amplio, debido a las mayores velocidades de datos, el mayor rango de cobertura y las capacidades integradas de corrección de errores que representa. Estas técnicas aplicadas a las redes inalámbricas permiten que la señal sea transmitida y recibida con un mínimo de interferencias.

1.3.1.2.1.- Expansión de espectro por salto de frecuencia (FHSS)

Consiste en transmitir la información en una determinada frecuencia durante un intervalo de tiempo inferior a 400ms. Pasando este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. La banda de frecuencia asignada se divide en varias sub-bandas de menor frecuencia llamadas canales.

Cada canal tiene el mismo ancho de banda, que esta determinado por la tasa de bits de datos y el método de modulación empleado, como se muestra en la Figura 1.5 Esta técnica la utilizan las tecnologías Bluetooth y HomeRF. [www04]

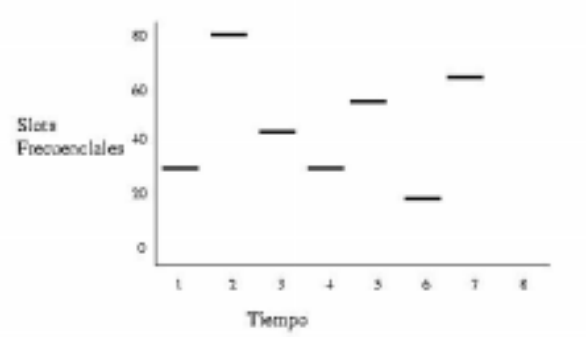


Figura 1.5: Modo de trabajo de la técnica FHSS [www04]

1.3.1.2.2.- Expansión de espectro por secuencia directa (DSSS)

Es una técnica que consiste en la generación de un patrón de bits redundante llamado señal de chip para cada uno de los bits que componen la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original, tal como se ve en la Figura 1.6.

Todos los miembros de la misma LAN inalámbrica conocen la secuencia binaria pseudoaleatoria que está utilizando. Todas las tramas de datos transmitidas van precedidas por una secuencia de preámbulo seguida de un delimitador de principio de trama. Una vez que han remodulado la señal transmitida, todos los receptores buscan primero la secuencia de preámbulo conocida y, una vez que lo encuentra comienzan a interpretar el flujo de bits recibidos según los limites de bits correctos de los datos de origen.

A continuación, los receptores esperan la llegada del delimitador de principio de trama y luego proceden a recibir el contenido de la trama. El o los destinatarios están determinados por una dirección de destino en la cabecera de la trama, igual que siempre.

Solo los receptores a los que el emisor haya enviado previamente la secuencia podrán recomponer la señal original. Además, al sustituir cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de transmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

Las estaciones que pertenecen a la misma WLAN ocupan la misma banda de frecuencias asignada y utilizan la misma secuencia binaria pseudoalatoria. Por ello es necesario usar un método de MAC apropiada que asegure que sólo se realizará una transmisión en cualquier momento dado.

Se tiene definidos dos tipos de modulaciones para la señal de información una vez que se sobrepone la señal de chip tal y como específica el estándar IEEE 802.11: la modulación **DBPSK**[10] **,** y la modulación **DQPSK**[11], proporcionando unas velocidades de transferencia de 1 y 2 Mbps respectivamente, con la técnica de modulación **PBCC** (Packet Binary Convolutional Coding) su velocidad llegando hasta 54 Mps (Millones de bits por segundo)

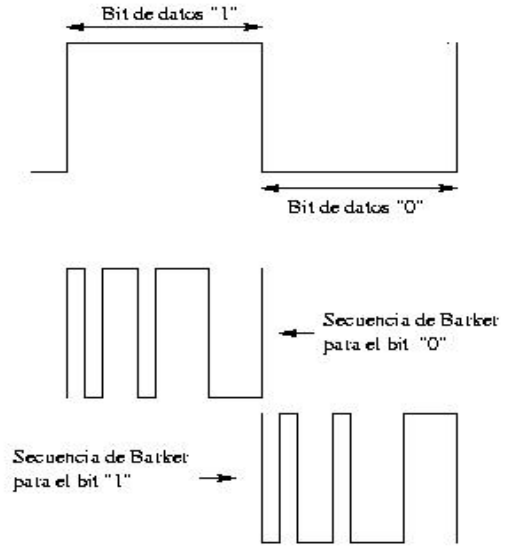


Figura 1.6: Codificación de la información mediante la secuencia de Barker. [www04]

[10]**DBPSK** Differential Binary Phase Shift Keying, Modulación de cambio de fase binario diferencial

[11]**DQPSK** Differential Quadrature Phase Shift Keying, Modulación de cambio de fase en cuadratura diferencial

En los estándares de redes WLAN, 802.11b define el uso de DSSS en la capa física para admitir intervalos de datos de 1 a 11 Mbps. [www04]

1.3.1.3. Múltiplexación por división de frecuencia ortogonal (OFDM)

La tercera banda de ISM hace referencia a los estándares 802.11a y 802.11g, que define el uso de OFDM[12], para obtener intervalos de transmisión de datos hasta 108 Mbps. En este caso veremos "Velocidad vs Modulación" Cuando transmitimos información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas, estas tramas son básicamente secuencias de bits.

Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir. La cabecera es necesaria por razones de gestión de los datos que se envían.

Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, como son:

- Barker. (RTS / CTS)
- CCK. Complementary Code Keying
- PBCC. Packet Binary Convolutional Coding
- OFDM. Orthogonal Frequency−Division Multiplexing

Una representación gráfica de las tramas más importantes:

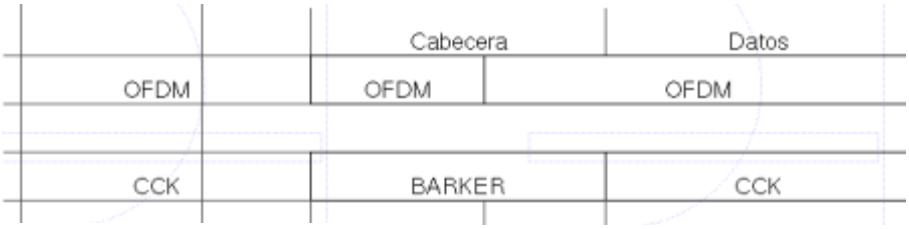


Figura 1.7: Estructura de la trama

[12]**OFDM** Wide-band Orthogonal Frequency Division Multiplexing, Múltiplexación por división de frecuencia ortogonal

Como podemos ver la cabecera en el caso de la codificación OFDM es más pequeña. A menor tamaño de cabecera menor es la transmisión, es decir, menor tráfico de bits de gestión luego mayor sitio para mandar bits de datos.

1.3.2.- Infrarrojo (IR)

Aunque los sistemas infrarrojos (IR) no permiten construir soluciones prácticas para la implementación de redes WLAN corporativas, y por tanto no se los utiliza ampliamente, si que son capaces de transferir datos aprovechando las frecuencias ubicadas en las cercanías del espectro electromagnético de la luz visible, aunque por debajo de las frecuencias de ésta. Estas bandas tienen las mismas limitaciones que la luz visible, en el sentido que no pueden penetrar objetos no transparentes como paredes. Como resultado, las redes WLAN que transmiten mediante rayos infrarrojos están restringidas a operar, como mucho, dentro de la misma habitación, estando limitadas a comunicación de corto alcance [LIB01].

1.3.3.- Resumen de los medios del nivel físico en 802.11

Las especificaciones generales del medió de transmisión físico como son: Infrarrojo, FHSS, DSSS y OFDM, veremos en forma resumida en la siguiente Tabla 1.1, su frecuencia, velocidades, alcance a velocidad máxima, la forma en que es utilizada y sus características.

Nivel físico	Infrarrojos	FHSS	DSSS	OFDM
Banda	850 – 950 nm	2,4 Ghz	2,4 Ghz	2,4 y 5 Ghz
Velocidades	1 y 2 Mb/s (802.11)	1 y 2 Mb/s (802.11)	1 y 2 Mb/s (802.11) 5,5 y 11 Mb/s (802.11b)	6,24,36,54 Mb/s (802.11a) hasta 108 Mb/s (802.11g)
Alcance (a vel. Max)	20 m	150 m	30 m	5m
Utilización	Muy rara	Poca	Mucha	Creciente
Características	No atraviesa paredes	Interferencias Bluetooth y hornos microondas	Buen rendimiento y alcance	Máximo Rendimiento

Tabla 1.1: Medios del nivel físico en 802.11

1.4.- Estándares LAN Inalámbricos

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesario las recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades. [www04].

Desde 1997 los estándares inalámbricos empezaron a desarrollarse, una breve descripción general de cómo fueron evolucionando lo veremos en Figura 1.8

En la Tabla 1.2 proporciona un ámbito normal de los estándares IEEE. [LIB02]

Estándares	Descripción
802.11	Estándar original de LAN inalámbricas 1 y 2 Mbps
802.11b	Extensión DSSS que admite 1, 2, 5.5, 11 Mbps
802.11a	Opera la banda de 5 Ghz, 9 a 54 Mbps, OFDM
802.11c	Operaciones de puente
802.11d	Especificación para dominios de regulación
802.11g	Operaciones de la banda 2,4 y 5 Ghz, OFDM/DSSS
802.11i	Características de Seguridad

Tabla 1.2: Estándares 802.11 del IEEE

1.4.1.- Estándar básico IIEE 802.11

El estándar 802.11 representa el estándar original de LAN inalámbricas, que difunde el IEEE. Este estándar especificaba las operaciones de la capa física DSSS (Expansión de espectro por secuencia directa), FHSS (Expansión de espectro por salto de frecuencia) e infrarrojos a 1 o 2 Mbps. También se incluía un mecanismo de seguridad en forma de privacidad con cables equivalentes (WEP, Wired Equivalent Privacy), WEP también era considerado como un mecanismo que proporcionaba un nivel de privacidad a los usuarios LAN inalámbricos. [LIB02]

1.4.2.- Estándar 802.11b

La extensión 802.11b del estándar 802.11 se limita al uso de DSSS en la capa física. Sin embargo, el intervalo operativo del equipo se extendía desde 1 Mbps y 2 Mbps a 5,5 y 11 Mbps. Tanto el estándar original 802.11 como la extensión 802.11b operan en la banda de frecuencia de 2, 4 Ghz

1.4.3.- Estándar 802.11a

Se puede utilizar para representar una red de área local inalámbrica de alta velocidad. Está extensión agregaba velocidad a los datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps; sin embargo, solo es obligatoria la compatibilidad con 6, 12 y 24 Mbps. Este opera en la frecuencia de 5 Ghz. Existe mas atenuación en altas frecuencia, la velocidad de un equipo compatible con la extensión 802.11a es menor que la de los productos LAN inalámbricos que operan en una banda de frecuencias de 2,4 Ghz.

1.4.4.- Estándar 802.11c

Define operaciones de enlace, dado que un punto de acceso actúa como puente entre una infraestructura de redes inalámbricas y otras con cables, esta extensión define cómo conoce el punto de acceso las direcciones de cada infraestructura.

1.4.5.- Estándar 802.11d

Representa un complemento de la capa MAC para promover el uso LAN inalámbrico del estándar 802.11. El objetivo de este esfuerzo es habilitar los puntos de acceso para que operen en canales de radio aceptables, agregando al estándar características que hacen que el equipo opere legalmente en ciertos países

1.4.6.- Estándar 802.11g

Por la inmensa mayoría de productos LAN inalámbricos en la banda de frecuencias de 2,4 Ghz, una empresa que incorpore una LAN inalámbrica de alta velocidad en la banda de frecuencia de 5 Ghz no podría utilizar su inversión en

puntos de acceso. El estándar 802.11g se desarrolló para proporcionar a las empresas opciones de migración y compatibilidad con el antiguo equipo. El equipo que admite el estándar 802.11g puede operar en la banda de frecuencia de 2,4 Ghz a 11 hasta 108Mbps o en la banda de 5 Ghz hasta 54 Mbps

1.4.7.- Estándar 802.11i

Debido a que WEP representa un problema de seguridad importante para las redes WLAN del IEEE. La extensión 802.11i representa un grupo de características de seguridad, que incluyen el protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocol) y el estándar de cifrado avanzado (AES, Advanced Encryption Standard). TKIP representa un reemplazo temporal de Wep, que admitirá las estaciones de cliente heredadas y los puntos de acceso mediante actualizaciones de software.

Por el contrario, AES proporcionará un nivel de seguridad más alto, pero sólo estará disponible para hardware nuevo. Un componente adicional de la extensión 802.11i para el estándar 802.11 es el estándar 802.11x, define la autenticación basada en puertos, y proporciona un método para que los clientes se autentiquen en los puntos de acceso.

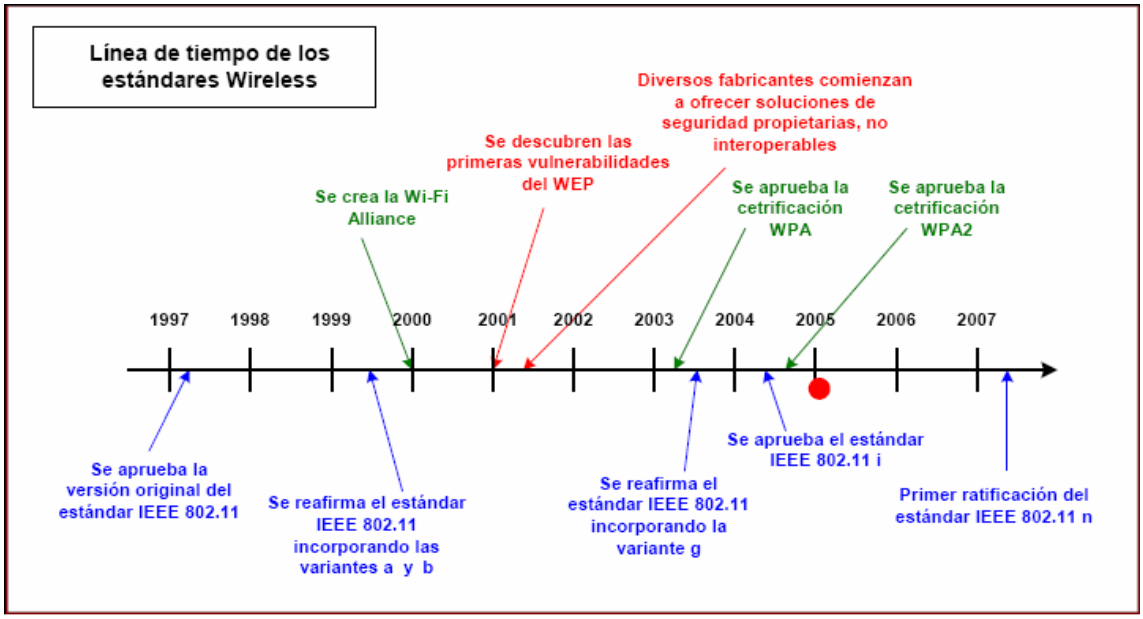


Figura 1.8: Tiempo de los estándares WLAN [www22]

1.5.- Mecanismos de seguridad

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que se podía acceder con relativa facilidad hacia redes WLAN desde la calle. El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable).

En el 2001 se publicaron las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica, [www05]

En la Figura 1.9 vemos como han ido evolucionado estos mecanismos. Con lo cual se clasifican en mecanismos básicos y avanzados de seguridad.

1.5.1.- Mecanismos Básicos

Los mecanismos básicos de seguridad fueron integrados en los primeros estándares de WLAN, si bien ya no son utilizados actualmente fueron un punto de inicio para la implementación de mecanismos y estándares de seguridad más avanzados. [www06]

1.5.1.1.- Wired Equivalent Privacy (WEP)

Se trata del primer mecanismo de seguridad implementado por el estándar IEEE 802.11, fue diseñado para ofrecer un cierto grado de privacidad. Mantenido sin cambios en los estándares 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

WEP comprime y cifra los datos que se envían a través de las ondas de radio, utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión, emplea el algoritmo RC4[13] de RSA Data Security, para cifrar las transmisiones realizadas a través del aire. En los dispositivos WLAN actuales el mecanismo de seguridad WEP está deshabilitado.

1.5.1.2.- Open System Authentication

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP.

1.5.1.3.- Lista de control de acceso (ACL)

Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC Figura en la lista de control de acceso (ACL, Access Control List)

1.5.1.4.- Closed Network Access Control

Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID[14]. Éste nombre viene a actuar como contraseña. Actualmente este mecanismo de seguridad es inseguro en exceso debido a que la mayoría de dispositivos WLAN existentes detectan el SSID automáticamente.

1.5.2.- Mecanismos Avanzados:

Los mecanismos avanzados fueron creados considerando las debilidades que existían mecanismos básicos de seguridad. [www06]

[13] **RC4** Algoritmo de Seguridad utilizado por WEP y WPA
[14] **SSID** Service Set Identifier, Es un identificador de la red

1.5.2.1.- Protocolo de Integridad de Clave Temporal (TKIP):

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes MIC[15] el cual cifra el checksum[16] incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

1.5.2.2.- EAP-TLS (Extensible Authentication Protocol with Transport Layer Security)

Protocolo de autenticación basado en certificados digitales. Ofrece una autenticación fuerte mutua (es decir tanto de la estación como del punto de acceso), credenciales de seguridad y claves de encriptación dinámicas.
Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS[17].

1.5.2.3.- Virtual Private Network (VPN):

Sistema para simular una red privada sobre una pública, como por ejemplo Internet, La idea es que la red pública sea vista desde dentro de la red privada como un "cable lógico" que une dos o más redes que pertenecen a la red privada

1.5.2.4.- Estándar IEEE 802.1X:

Utiliza el protocolo de autenticación extensible o EAP, para autenticar al dispositivo móvil**,** permitiendo a la Entidad de Autenticación de Puertos (Port Authentication Entity, PAE) un control del proceso de autenticación a la red.

[15]**MIC** Message Integrity Code, Código de integración de mensajes
[16]**Checksum** Comprobación de suma, realiza cálculos sobre cadenas de texto
[17] **RADIUS** Remote Authentication Dial In User service, Servicio de usuario de acceso telefónico de autenticación remota

1.5.2.5.- Wifi Protected Access (WPA)

WPA utiliza el protocolo de integridad de clave temporal (TKIP) para codificar los datos, además Implementa el estándar 802.1x utilizando el protocolo de autenticación extensible (EAP).

1.5.2.6.- Wifi Protected Access 2 (WPA2)

Esta basado en el estándar de seguridad para 802.11, 802.11i cumpliendo con las normas del National Institute of Standards and Technology (NIST) FIPS 140-2. WPA2 implementa el algoritmo AES a diferencia de WPA que utiliza RC4, sin embargo WPA2 es totalmente compatible con WPA

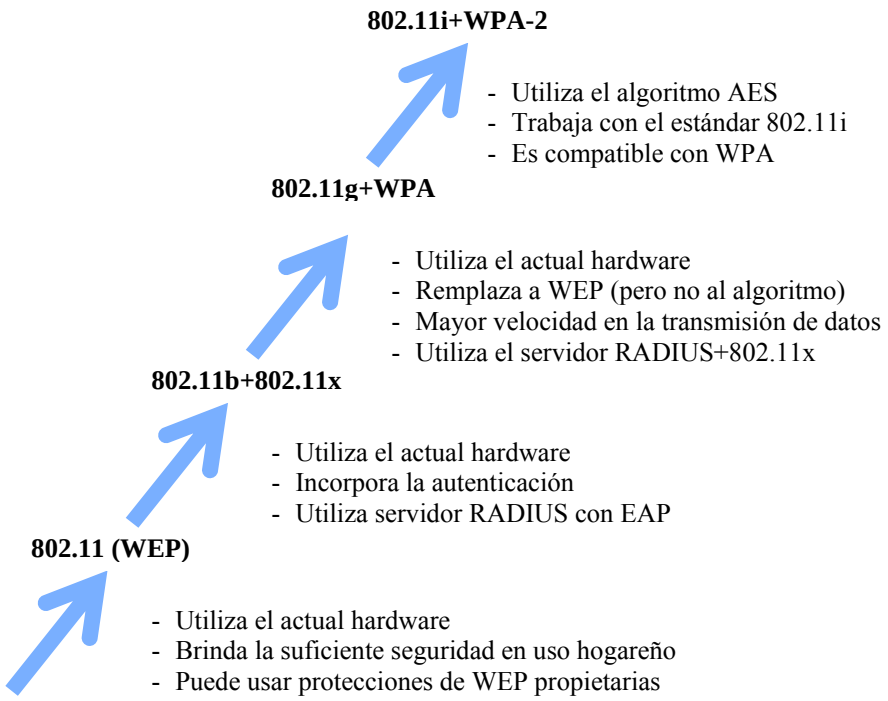


Figura 1.9: Mecanismos de seguridad [www23]