Trabajo Práctico
Seguridad en Redes Wireless

Materia: Auditoría y Seguridad Informática

Integrantes:
- Chilleti Emanuel
- Vietto Santiago

Profesor: Ing. Mariano Aliaga

Institución: Universidad Católica de Córdoba

Año: 2021

Universidad Católica de Córdoba
Universidad Jesuita

Introducción a las Redes Inalámbricas

Una red de comunicación inalámbrica (Wireless Network), es aquélla que se lleva a cabo sin el uso de cables de interconexión entre los participantes de una comunicación, es decir, se utilizan ondas de radio para conectar los dispositivos y tanto la transmisión como la recepción de información se realiza a través de puertos; por ejemplo una comunicación entre teléfonos móviles es inalámbrica, mientras que una comunicación con teléfono fijo tradicional no lo es. Algunos de los dispositivos que comúnmente utilizan las redes inalámbricas son las computadoras de escritorio y portátiles, teléfonos móviles o celulares, televisores, tablets, impresoras, reproductores de multimedia, periféricos (auriculares, mouse, teclado), dispositivos localizadores, etc. Estos dispositivos son susceptibles de intercomunicarse entre sí y, aunque pueden hacerlo por los sistemas de cables tradicionales, su mayor potencial se alcanza a través de las comunicaciones inalámbricas. Las redes inalámbricas funcionan de manera similar a las redes cableadas, sin embargo, estas deben convertir las señales de información en una forma adecuada para la transmisión a través del medio de aire. Estas tienen y sirven a muchos propósitos, en algunos casos se utilizan para sustituir las redes cableadas, también se utilizan para proporcionar acceso a datos desde ubicaciones remotas. Lo bueno, es que la infraestructura inalámbrica puede ser construida a bajo coste en comparación con las alternativas cableadas o alambricas tradicionales. Además, permiten a los dispositivos remotos que se conecten sin dificultad, independientemente que estos dispositivos estén a unos metros o a varios kilómetros de distancia, y todo esto se puede hacer sin la necesidad de romper paredes para pasar cables o instalar conectores, donde justamente esto hizo que el uso de esta tecnología sea muy popular, y se expandiera rápidamente. Hoy en día existen muchas tecnologías diferentes que difieren en la frecuencia de transmisión que utilizan, como también la velocidad y el alcance de sus transmisiones. Por otro lado, tenemos algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Tenemos en cuenta que las ondas electromagnéticas que se transmiten a través de muchos dispositivos, son propensas a la interferencia, por ende, todos los países necesitan regulaciones que definan los rangos de frecuencia y potencia de transmisión permitidos para cada tecnología, en el caso de Argentina el ente encargado de estas regulaciones es el ENACOM. Además, las ondas electromagnéticas no se pueden confinar fácilmente a un área geográfica limitada, y es por esta razón, que un hacker por ejemplo puede escuchar fácilmente a una red si los datos transmitidos no están codificados, por lo tanto, se deben tomar todas las medidas necesarias para garantizar la privacidad de los datos transmitidos a través de redes inalámbricas.

Historia

No fue hasta 1971 cuando un grupo de investigadores en la Universidad de Hawaii, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA. Ésta es la primera red de área local inalámbrica (WLAN), estaba formada por 7 computadoras situadas en distintas islas que se podían comunicar con un ordenador central al cual pedían que realizara cálculos. Un año después Aloha se conectó mediante ARPANET al continente americano. ARPANET es una red de computadoras creada por el Departamento de Defensa de los EEUU como medio de comunicación para los diferentes organismos del país. Martin Cooper fue el pionero en esta tecnología. A él se le considera (el padre de la telefonía celular) al introducir el primer radio-teléfono en 1973, en Estados Unidos, mientras trabajaba para Motorola. La primera red comercial automática fue la de NTT de Japón en 1979, seguida por la NMT, que funcionaba en simultáneo en Suecia, Dinamarca, Noruega y Finlandia en 1981 usando teléfonos de Ericsson y Mobira (el ancestro de Nokia).

En 1983 surge la red analógica AMPS o 1G. El primer antecedente respecto al teléfono móvil en Estados Unidos fue de la compañía Motorola.

A principios de los 90 surge GSM también conocida como 2G. También trajo otras ventajas como una mejor calidad de voz, mayor velocidad para transmitir datos, transmisión de faxes y los famosos SMS. En 1997, se creó el primer estándar WiFi, IEEE 802.11, a manos del Institute of Electrical and Electronics Engineers (del que recibe su nombre). Esto, permitía transferir datos a 1 o 2 Mbps.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red wifi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

En 1998 se crea el Bluetooth Special Interest Group (Bluetooth SIG) y es cuando Bluetooth vio la luz. Es una tecnología que no ha sufrido muchos cambios. En 1999 Nokia,Symbol Technologies y otras empresas crearon la asociación Wireless Ethernet Compatibility Alliance (WECA), que en 2003 fue renombrada a WI-FI Alliance (WIreless FIdelity), el objetivo de ésta fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos. En el 2000, la WECA certificó según la norma 802.11b (revisión del 802.11 original) que todos los equipos con el sello WI-FI podrán trabajar juntos sin problemas. 802.11b utilizaba la banda de los 2,4Ghz y alcanzaba una velocidad de 11Mbps. Posteriormente surgiría 802.11a que generó problemas puesto que usaba la banda de los 5Ghz que, si bien estaba libre en Estados Unidos, en Europa estaba reservada para fines militares. Esto generó un parón en esta tecnología inalámbrica, lo que nos hace ver la importancia de la instauración de unos estándares válidos para todos.

En el año 2001 surge la tecnología 3g. Con ello fue posible comenzar a transferir audio y video, imágenes, mensajes de texto y apareció el buzón de voz.

IEEE 802.11g: el Wi-Fi G es el sucesor del Wi-Fi B y también utiliza la banda de 2,4 GHz. La velocidad máxima de transmisión se incrementó hasta los 54 Mbps en dicha banda y empezó a estar disponible a partir de 2003.

IEEE 802.11n: en septiembre de 2009 se ratificó este estándar. Funciona tanto en la banda de 2,4 GHz como en la de 5 GHz y alcanza velocidades de hasta 600 Mbps.

Para 2010 la tecnología móvil 4G irrumpió en la escena introduciendo grandes mejoras a la velocidad de datos. Con eso fue posible, por ejemplo, visualizar videos sin interrupciones, pues se hizo realidad la verdadera banda ancha móvil de alta velocidad.

IEEE 802.11ac: se estandarizó a finales de 2013. Opera en la banda de 5 GHz y puede alcanzar velocidades de 1.300 Mbps.

IEEE 802.11ax: un avance importante que alcanza velocidades de hasta 10 Gbps. A partir del 3 de octubre de 2018, la Wi-Fi Alliance decide renombrar el estándar a Wi-Fi 6 o 6th Generation, esto con el fin de simplificar al usuario final el reconocimiento de la tecnología en los dispositivos que se empezaron a fabricar a principios de 2019.

En 2018 ya se empezó a hablar de tecnoloģia 5g. Los tres países principales que tienen la mayor cantidad de ciudades con 5G son China en 341. Estados Unidos con 279 y Corea del Sur con 85. El Reino Unido ahora tiene 5G en 54 ciudades, seguido de cerca por España con 53. Otros 27 países agregaron implementaciones comerciales de 5G el año pasado, incluidos tres países que ya han alcanzado los diez primeros en términos de ciudades cubiertas: Canadá con 49 ciudades, así como Francia y Tailandia empatadas en 24.

Tipos de Redes Inalámbricas

Las redes inalámbricas se pueden clasificar en distintos grupos según el área de aplicación y el alcance de la señal:

Redes inalámbricas de área corporal o WBAN (Wireless Body Area Network):

Este tipo de redes inalámbricas cubren distancias de 1 ó 2 metros. Esta se realiza entre dispositivos de baja potencia utilizados en el cuerpo humano, consistiendo en un conjunto móvil y compacto de comunicación por ejemplo entre micrófonos, auriculares, sensores, etc. También la red puede estar formada por dispositivos (como sensores) de baja potencia implantados en el cuerpo, donde estos dispositivos controlan los parámetros vitales del cuerpo y movimientos, y transmiten datos de forma inalámbrica desde el cuerpo a una estación base, en donde los datos pueden ser remitidos a un hospital, Clínica o a otro lugar, en tiempo real.

Redes inalámbricas de área personal o WPAN (Wireless Personal Area Network):

Son aquellas que cubren distancias inferiores a los 10 metros. A diferencia de otras redes inalámbricas, una conexión realizada a través de una WPAN implica, por lo general, poca o ninguna infraestructura o conectividad directa fuera del enlace establecido. Este tipo de redes se caracterizan por su bajo consumo de energía y también una baja velocidad de transmisión. Estas soluciones están pensadas para interconectar los distintos dispositivos de un usuario (por ejemplo, el ordenador con la impresora). Éste es el caso de la tecnología Bluetooth o de IEEE 802.15, entre otras.

Redes inalámbricas de área local o WLAN (Wireless Local Area Network):

Estas redes están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan sobre todo en el hogar, la escuela, una sala de computadoras, o entornos de oficina. Permite reemplazar mediante conexiones inalámbricas los cables que conectan a la red los PCs, portátiles u otro tipo de dispositivos proporcionando a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red para poder transmitir y recibir voz, datos, vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. Debido a la competencia, otros estándares como HIPERLAN nunca recibieron tanta aplicación comercial, ya que el estándar IEEE 802.11 fue más sencillo de implementar y se hizo más rápido con el mercado.

Redes inalámbricas de área metropolitana o WMAN (Wireless Metropolitan Area Network):

Estas pretenden cubrir el área de una ciudad o entorno metropolitano, pudiendo extenderse hasta 50 km. Podemos considerarla como una red LAN extensa o una red WAN de menor tamaño. Básicamente lo que hace es interconectar redes WLAN unas con otras y ampliar así el rango de acción. Incluso podría ser utilizado en zonas de difícil acceso, como pueden ser lugares remotos dentro de un municipio, zonas rurales, etc. Las WMAN se basan en el estándar IEEE 802.16, a menudo denominado WiMAX (Worldwide Interoperability for Microwave Access).

Redes inalámbricas de área extensa o WWAN (Wireless Wide Area Network):

También conocidas como de área global o WGAN, pueden cubrir toda una región (país o grupo de países), abarcando miles de kilómetros, y permitiendo la interconexión de varios sistemas de comunicaciones ayudando a que ésta sea cada vez más globalizada. Estas redes se basan en tecnología celular y han aparecido como evolución de las redes de comunicaciones de voz. Éste es el caso de las redes de telefonía móvil conocidas como la primera generación, 1G, que era analógica y fue concebida y diseñada exclusivamente para las llamadas de voz, la segunda generación, 2G, está basada en tecnología digital y la infraestructura de red (GSM), permitiendo mensajes de texto, la generación 2.5G se sitúa entre la 2G y la 3G, que también se la conoce como 2G + GPRS y se trata de una versión mejorada de 2G. La generación 3G fue introducida en el año 2000. La 3.5G es una versión mejorada de la 3G que utiliza HSDPA para acelerar las transferencias de datos. La cuarta generación, 4G, es capaz de proporcionar velocidades de hasta 1 Gbps y cualquier tipo de servicio en cualquier momento y en cualquier lugar. Y por último la generación 5G. Pero también existen opciones satelitales mucho más económicas para usuarios residenciales o para pequeñas oficinas, o gente que esté en zonas remotas como islas, debido a su gran altura, donde las transmisiones por satélite pueden cubrir una amplia área sobre la superficie de la tierra.

Otras:

- Redes inalámbricas de área regional (WRAN), están constituidas por una integración de las redes WLAN y WMAN, bajo el estándar IEEE 802.22. Son un proyecto de solicitud de autorización (PAR) aprobadas por el IEEE-SA, cuya función es desarrollar un estándar para la radio cognitiva basada en las capas PHY/MAC/(interfaz de aire), para el uso de una licencia exenta de los dispositivos, para no interferir en el espectro que se asigna a la emisión del servicio de TV.

Estándares y Tecnologías Inalámbricas

Bluetooth:

Bluetooth es un enlace radio de corto alcance que aparece asociado a las redes WPAN. Este concepto hace referencia a una red sin cables que se extiende a un espacio de funcionamiento personal con un radio de hasta 10 metros. Bluetooth trabaja en el rango de frecuencias de 2,402 GHz a 2,480 GHz (Banda ISM). Los terminales pueden estar en movimiento y no tener línea de vista (camino o path, limpio, sin obstrucciones, entre las antenas transmisoras y receptoras.) entre sí; además, las velocidades de transmisión oscilan entre 720kbps y 1 Mbps. Pertenece al estándar IEEE 802.15.1. La principal aplicación del Bluetooth es la de conectar entre sí equipos informáticos y de comunicación portátil y móvil, como ordenadores, PDAs, impresoras, mouse, micrófonos, auriculares, lectores de código de barras, sensores, displays, localizadores, teléfonos móviles, etc. El objetivo es que todos estos equipos se puedan comunicar e interoperar entre sí sin interferencias.

IrDA:

Infrared Data Association (IrDA) define un estándar físico para la transmisión y recepción de datos a través de rayos infrarrojos. Está asociada con las redes de tipo WPAN. No es una técnica muy usada ya que no pueden traspasar objetos opacos, por lo que necesitan que la comunicación tenga línea de visión directa. Esta tecnología fue pensada para redes personales de área reducida y ocasionalmente en algunas LANs específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Además, su uso no está regulado por ningún organismo. Su mayor aplicación es en ordenadores portátiles.

Zigbee:

ZigBee es una alianza sin fines de lucro de 25 empresas, la mayoría de ellas fabricantes de semiconductores, con la finalidad de promover el desarrollo e implantación de una tecnología inalámbrica bidireccional de fácil aplicación, alta fiabilidad, bajo costo, bajo consumo y bajas velocidades de transmisión de datos vía radio, para usarla en dispositivos de domótica, automatización de edificios, control industrial, periféricos de PC o sensores médicos. Está ratificado como estándar IEEE 802.15.4. También sirve para la creación de redes inalámbricas más grandes que no exijan una gran cantidad de transmisión de datos. Tiene velocidades comprendidas entre 20 Kbps y 250 Kbps y rangos de 10 m a 75 m. Puede usar las bandas libres ISM de 2,4 GHz, 868 MHz (Europa) y 900 MHz (EEUU). Los módulos ZigBee están pensados para ser los transmisores inalámbricos más baratos producidos de forma masiva.

UWB:

UWB, es una tecnología WPAN basada en una coexistencia de estándares, entre IEEE 802.15.3a, IEEE 802.15.4z y IEEE 802.15.1(capa física para bluetooth), donde esta red esta basada para comunicaciones y transmisión de grandes archivos a alta velocidad y corto alcance en interiores o en distancias cortas. Es capaz de transmitir más información en menos tiempo que las tecnologías anteriormente mencionadas. Esta tecnología ofrece una velocidad de transmisión de datos de más de 110 Mbps hasta 480 Mbps a distancias de hasta unos pocos metros. En EEUU, las frecuencias para UWB están asignadas en la banda de 3,1 GHz a 10,6 GHz, sin embargo, en Europa, las frecuencias incluyen dos bandas, una de 3,4 GHz a 4,8 GHz y de 6 GHz a 8,5 GHz. Las comunicaciones UWB transmiten información mediante la emisión de pulsos de muy corta duración y de gran ancho de banda.

Otras tecnologías de red WPAN:

- HomeRF: se basa en el teléfono inalámbrico digital mejorado (Digital Enhaced Cordless Telephone, DECT). Este transporta voz y datos por separado, al contrario que protocolos como Wi-Fi que transporta la voz como una forma de datos. Su alcance es de 50 metros aproximadamente. Posee multitud de capacidades de voz (identificador de llamadas, llamadas en espera, regreso de llamadas e intercomunicación dentro del hogar).
- Wibree: es una nueva tecnología digital de radio interoperable para pequeños dispositivos. Esta es la primera tecnología abierta de comunicación inalámbrica, que ofrece comunicación entre dispositivos móviles o computadores y otros dispositivos más pequeños, diseñado para que funcione con poca energía. Wibree se creó con dos alternativas:
    - Wibree, de implementación única; funciona para dispositivos que requieren un consumo bajo de energía, pequeños y de bajo costo, como relojes, sensores deportivos, teclados inalámbricos, etc.
    - Wibree, de implementación modo dual Bluetooth y Wibree; se diseña para su uso en dispositivos Bluetooth donde Wibree se integra con Bluetooth y Bluetooth RF utilizando los dispositivos existentes dirigido especialmente a dispositivos como teléfonos móviles y computadoras personales.
- DECT (Digital Enhanced Cordless Telecommunications): Telecomunicaciones Inalámbricas Mejoradas Digitalmente, es un estándar ETSI para teléfonos inalámbricos digitales conectados a una base. Un teléfono DECT es parecido a un terminal celular GSM, con la diferencia de que el radio de operación de los primeros es de 25 a 100 metros, mientras que GSM alcanza hasta los 10 kilómetros. Es comúnmente utilizado con propósitos domésticos y/o corporativos.

WI-FI (IEEE 802.11):

El estándar IEEE 802.11 es un conjunto especificaciones de control de acceso al medio (MAC) y de la capa física (PHY) para la implementación de redes WLAN en las bandas de frecuencias 2,4 GHz y 5 GHz. La versión base del estándar fue lanzada en 1997 con una

velocidad de transmisión de 2Mbps en el rango de frecuencia de 2,4 GHz a 2,5 GHz, y este ha tenido varias modificaciones posteriores. Por nombrar algunas modificaciones tenemos el IEEE 802.11b que fue el primer estándar aceptado (el primero creado fue IEEE 802.11), admitiendo hasta 11 Mbps en la banda frecuencial sin licencia de 2,4 GHz. Luego, el estándar IEEE 802.11a puede operar a una velocidad de hasta 48 Mbps y utiliza la banda de frecuencia de 5 GHz. Después tenemos el estándar IEEE 802.11g que puede operar a una velocidad de hasta 54 Mbps, pero utiliza la banda de frecuencia de 2,4 GHz y OFDM, este estándar también es compatible con 802.11b. Y por nombrar otros tenemos el IEEE 802.11n y el IEEE 802.11ac. El estándar y las enmiendas constituyen la base de los productos para redes inalámbricas que utilizan la marca Wi-Fi.

WiFi: viene de Wireless Fidelitys (fidelidad inalámbrica), y es una tecnología de transmisión de datos inalámbrica utilizada para Internet principalmente, y que se basa en el estándar 802.11, en donde se permite el acceso a Internet a los distintos dispositivos que estén conectados a una red determinada. El funcionamiento del WiFi requiere de un router que está conectado a Internet a través de un cable, y es el encargado de distribuir la conexión a los distintos dispositivos de una misma red de manera inalámbrica, donde el enrutador transforma la información digital en ondas de radio que se transmiten por el aire dentro de un alcance concreto, y posterior los decodificadores de los dispositivos receptores vuelven a transformar las ondas de radio en señales digitales, que son interpretadas por el microprocesador del equipo para permitir la conexión a Internet. La conexión será mejor cuanto más cerca estén los dispositivos del router.

Otras tecnologías de red WLAN:

- HiperLan (High Performance Radio LAN): estándar del ETSI (European Telecommunications Standards Institute) con el objetivo de desarrollar velocidades de transferencia mayores que 802.11, de hasta 25 Mbps. Con HiperLan se busca conseguir WLANs de alta capacidad y baja movilidad en un entorno reducido que no supere los 50 m.
- HiperLan/2 (High Performance Radio LAN/2): variante de HiperLan que fue diseñada como una conexión inalámbrica rápida para muchos tipos de redes. También funciona como una red doméstica pero incorpora toda una serie de características adicionales y con una velocidad de transmisión que puede llegar hasta 54 Mbps. Esta tecnología opera sobre la banda de frecuencia de los 5 GHz.

WiMAX:

WiMAX (del inglés Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos, regido en el estándar IEEE 802.16, que proporciona accesos concurrentes en áreas de hasta 50 km de radio (WMAN) sin necesidad de visión directa con las estaciones base. Funciona por debajo de los 11 GHz y alcanza velocidades de hasta 70 Mbps. Se obtiene mayor ancho de banda en distancias mayores (hasta 50 km) permitiendo por tanto mayores coberturas. Además no requiere de visión directa. El sistema está diseñado para que escale a varios cientos de usuarios cómodamente y además permite un uso flexible de frecuencias para poderse adaptar a cualquier tipo de legislación.

Otras tecnologías de red WMAN:

- Wibro (Wireless Broadband Technology): es una tecnología de banda ancha inalámbrica de Internet. Esta tecnología fue ideada para superar la limitación de la velocidad del teléfono móvil y para agregar movilidad a Internet de banda ancha. Las estaciones de la base Wibro ofrecen un rendimiento de procesamiento de datos de 30 a 50 Mbps/s y cubren un radio de 1,5 km. Detalladamente, proporcionan la movilidad para los dispositivos móviles hasta 120 km/h, comparado al LAN inalámbrico cuya movilidad es la velocidad de una persona en movimiento y la del teléfono móvil que tiene movilidad de hasta 250 km/h.

GSM (Global System for Mobile Communications):

GSM (Global System for Mobile communications, Sistema Global para Comunicaciones Móviles) pertenece a los tipos de redes WWAN. Actualmente representa más del 80% de la telefonía móvil a nivel mundial y es el estándar más representativo de los sistemas de Segunda Generación (2G). Fue creado en 1990 por el ETSI (European Telecommunications Standards Institute) con el objetivo de presentar una tecnología eficiente, con cobertura internacional y que permitiera obtener un mercado abierto y extenso como el actual. Tiene una baja tasa de transferencia de datos y fax, de sólo 9.6Kbps, aunque a veces va de 14kbps a 64Kbps. El área de cobertura de la célula está limitada por la distancia de reutilización de frecuencias, por lo que en áreas muy pobladas, con una alta densidad de células, esta área es pequeña. Las zonas del espectro posibles para su uso son la banda de 900 MHz y posteriormente la de 1800 MHz.

GPRS (General Packet Radio System):

Es la llamada generación 2.5 de telefonía móvil, estándar intermedio entre la segunda y la tercera generación, GSM y UMTS respectivamente. Debido a problemas en la implantación de 3G, esta tecnología se ha mantenido un periodo relativamente prolongado. Su nuevo mecanismo para el tráfico de datos le permite alcanzar velocidades mayores que teóricamente oscilan entre los 54 y los 172 Kbps, pero que en la práctica son sensiblemente inferiores debido a las adversidades físicas y al despliegue de los operadores, que no buscan llegar a proporcionar estas velocidades, por ende se estima como un máximo de 144 Kbps.

UMTS (Universal Mobile Telephone Standard):

Es la denominada 3G. Se propuso como el gran avance en la telefonía móvil aunque ha tenido problemas importantes a la hora de su implantación, que han retrasado su llegada. El objetivo primordial de esta es obtener una conexión de alta velocidad para abrir a la telefonía móvil al campo de las aplicaciones multimedia de forma total. Utiliza CDMA (multiplexión por código) en lugar de TDMA como forma de multiplexión de comunicaciones en un medio compartido. En este caso el tamaño de la célula no está marcado por la distancia de reutilización de frecuencias, sino que el factor limitante es la relación señal a ruido. Ésta depende del número de usuarios en un instante, por lo que cuando la estación

base detecta un número demasiado elevado de usuarios, que están produciendo demasiada interferencia, reacciona disminuyendo su potencia de transmisión, dejando a algunos usuarios fuera y reduciendo el tamaño de la célula (cell breathing). Su velocidad va desde 144 Kbps a 2 Mbps, y su rango de frecuencias está en torno a 2 GHz.

Otras tecnologías de red WWAN:

- HSDPA (High Speed Downlink Packet Access): es la optimización de la tecnología UMTS y consiste en un nuevo canal compartido en el enlace descendente (downlink) que mejora significativamente la capacidad máxima de transferencia de información hasta alcanzar tasas de 14 Mbps. Es popularmente conocida como 3.5G.
- HSUPA (High Speed Uplink Packet Access): es una evolución de HSDPA que añade una mejora sustancial en la velocidad para el tramo de subida o uplink (desde el terminal de usuario hacia la red) llegando a tasas de transferencia de subida de hasta 7.2 Mbps. Se la conoce como 3.75G o 3.5G Plus.
- LTE Advanced (Long Term Evolution Advanced): la cuarta generación, 4G, es capaz de proporcionar velocidades de hasta 1 Gbps y cualquier tipo de servicio en cualquier momento de acuerdo con las necesidades del usuario y en cualquier lugar.

A continuación realizamos una comparación entre todos los tipos de redes y algunas de sus tecnologías:

Tipo de red	Nombre	Estándar	Banda de frecuencia	Rango nominal	Máxima Velocidad. Transmis.
WPAN	Bluetooth	IEEE 802.15.1	2.4 GHz	10 m:	720 Kbps
	IrDA	IrDA	Ventana Infrarrojo 850-900 nm longitud de onda	1 m	16 Mbps
	ZigBee	IEEE 802.15.4	868 MHz, 900 MHz, 2.4 GHz	10 m	250 Kbps
	UWB	IEEE 802.15.3	3.1-10.6 GHz (USA) 3.4-4.8 GHz & 6-8.5 GHz (Europa)	10 m	480 Mbps
WLAN	Wi-Fi	IEEE 802.11	2.4 / 5 GHz	100 m	1 Mbps
		IEEE 802.11ª	5 GHz	100 m	48 Mbps
		IEEE 802.11b	2.4 GHz	100 m	11 Mbps
		IEEE 802.11g	2.4 GHz	100 m	54 Mbps
		IEEE 802.11n	2.4 / 5 GHz	250 m	600 Mbps
		IEEE 802.11ac	5 GHz	250 m	1.3 Gbps
WMAN	WiMAX	IEEE 802.16	2-11 GHz y10-66 GHz	50 km	70 Mbps
WWAN	Móvil	AMPS, GSM, GPRS, UMTS, HSDPA, LTE	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2600 MHz	> 50 km	1 Gbps
	Satélite	DVB-S2	3-30 GHz	> 50 km	60 Mbps

Arquitectura de tecnologías Inalámbricas

A continuación definimos diversos términos utilizados en una arquitectura de red inalámbrica. La arquitectura lógica del estándar 802.11 contiene varios componentes principales:

Estación (Station - STA): puede ser una PC, un ordenador portátil, una PDA, un teléfono o cualquier dispositivo que tenga la capacidad de interferir en el medio inalámbrico.

Punto de acceso (Access Point - AP): también llamado estación base (BS), es un dispositivo que permite a los dispositivos inalámbricos que se conecten a una red cableada mediante Wi-Fi, o estándares relacionados.

Conjunto de servicios básicos (Basic Service Set - BSS): consiste en un punto de acceso, junto con todas las estaciones asociadas. El punto de acceso actúa como un maestro para controlar las estaciones dentro de ese BSS. El BSS más simple se compone de un AP y una STA.

Conjunto de servicios extendidos (Extended Service Set - ESS): conjunto de uno o más conjuntos interconectados de servicios básicos (BSS) que aparecen como un solo BSS a la capa de control de enlace lógico de cualquier estación asociada con una de esas BSS.

BSS independiente (Independent Basic Service Set - IBSS): cuando todas las estaciones en el conjunto de servicios básicos son estaciones móviles y no hay conexión a una red cableada. Es una red ad hoc que no contiene puntos de acceso, lo que significa que no pueden conectarse a cualquier otro conjunto de servicios básicos.

Sistema de distribución (Distribution System - DS): es el mecanismo por el cual diferentes puntos de acceso pueden intercambiar tramas entre sí o bien con las redes cableadas, si las hubiera. El DS no es necesariamente una red y el estándar IEEE 802.11 no especifica ninguna tecnología en particular para este. En casi todos los productos comerciales se utiliza Ethernet por cable como la tecnología de red troncal.

Por otro lado, existen dos modos de configurar una red inalámbrica:

Modo Ad hoc: todos los dispositivos de la red se comunican directamente entre sí, de igual a igual, en el modo de comunicación punto a punto. No se requiere ningún punto de acceso para la comunicación entre dispositivos. Es el más adecuado para un pequeño grupo de dispositivos que se encuentren presentes y físicamente muy cerca entre sí. El rendimiento de la red sufre si el número de dispositivos aumenta. El modo ad hoc funciona bien en un entorno pequeño siendo la forma más fácil y menos costosa de configurar una red inalámbrica.

Modo Infraestructura: todos los dispositivos de la red están conectados con la ayuda de un punto de acceso. Los puntos de acceso inalámbricos son generalmente routers o switches que pasan los datos de la red inalámbrica a datos en una Ethernet cableada, actuando como un puente entre la LAN cableada y los dispositivos inalámbricos. Los clientes

inalámbricos pueden moverse libremente del dominio de un punto de acceso a otro y seguir manteniendo la conexión de red sin cortes. Este modo ofrece una mayor seguridad, facilidad de gestión, y más escalabilidad y estabilidad, pero incurre en un costo adicional debido al despliegue de puntos de acceso.

Ventajas y desventajas

Ventajas:

- Fácil instalación y reducción de costes: como no es necesario tender cables, podemos adaptar la red a cualquier entorno, así como establecer redes con carácter temporal, donde acabada su utilidad, se pueden reciclar todos los componentes para su próximo uso. También, a diferencia del cable que es sensible a agresiones externas, para las inalámbricas el medio de transmisión es el aire, y está libre de agresiones físicas. Y por último, no se requieren obras de mantenimiento ni para ampliación o remodelación.
- Movilidad: se puede tener acceso a la información en cualquier punto dentro de la zona de cobertura del punto de acceso, conservando su acceso con todas las prestaciones. Además, al no usar cables permite a este tipo de redes llegar a puntos donde el acceso con cables sería imposible.
- Escalabilidad: facilidad de expandir la red después de la instalación inicial. Se puede ajustar el tamaño de la red a nuestras necesidades, El añadir nuevos puntos de acceso es muy sencillo y podemos cubrir grandes áreas.
- Uso del espectro libre: la mayor parte de las redes inalámbricas operan en un rango de frecuencias de uso libre, es decir, no están sujetas al pago de ningún tipo de licencias para su uso.
- Altas tasas de transmisión: se pueden alcanzar tasas de transmisión que llegan hasta los 54 Mbps.

Desventajas:

- Interferencias: debido al medio usado, es muy difícil darse cuenta que dispositivos son los que están produciendo interferencias. Además las interferencias pueden provenir de otras redes inalámbricas próximas, efecto que se puede prevenir gestionando conjunta y adecuadamente las redes. Todas estas interferencias provocan que nuestra red inalámbrica no funcione a su más alto rendimiento.
- Cobertura: el radio de acción de una red inalámbrica está limitado por la potencia máxima que se puede radiar según la legislación vigente. Para extender la zona de acción de la red sólo se puede añadir nuevos puntos de acceso o colocar repetidores.
- Velocidad de transmisión: la transmisión inalámbrica puede ser más lenta y menos eficiente que las redes cableadas. En las grandes redes inalámbricas, por lo general, la red troncal será cableada en vez de inalámbrica.

- Seguridad: se debe diseñar una red, con el nivel de seguridad más alto posible, ya que la transmisión inalámbrica es más vulnerable, y para así evitar que usuarios no autorizados tengan acceso a la red o realicen ataques.

Seguridad WI-FI

Las redes de telecomunicaciones sufren muchos y variados ataques, y van desde la intrusión de virus y troyanos hasta la alteración y robo de información confidencial. La seguridad es uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi. La mayoría de las redes son instaladas por administradores de sistemas y redes, por su simplicidad de implementación sin tener en consideración la seguridad y, por ende, convirtiendo sus redes en redes abiertas, sin proteger la información que circula por ellas. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP y el WPA que se encargan de codificar la información transmitida para proteger su confidencialidad, o IPSEC en el caso de las VPN, y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

Peligros y Ataques

Las violaciones de seguridad en las redes wireless (WLAN) suelen venir de los puntos de acceso no autorizados (rogue AP), es decir, aquellos que son instalados sin el conocimiento del administrador del sistema, y son aprovechados por los intrusos que pueden llegar a asociarse al AP y así acceder a los recursos de la red. Algunos ataques son:

Warchalking y Wardriving: el primero hace referencia a la utilización de un lenguaje de símbolos para reflejar visualmente la infraestructura de una red inalámbrica y las características de alguno de sus elementos. Estas señales se suelen colocar en las paredes de edificios situados en las zonas en las que existen redes inalámbricas para indicar su condición y facilitar el acceso a las mismas. Y el wardriving es la acción de ir recorriendo una zona en busca de la existencia de redes wireless y conseguir acceder a ellas; esta requiere de un software especial que capture las tramas broadcast que difunden los AP.

Ruptura de la clave WEP: este mecanismo de seguridad especificado en el estándar 802.11 es el cifrado de la información utilizando una clave simétrica denominada WEP, sin embargo, WEP tiene deficiencias, como la corta longitud de su clave o la propagación de la misma, que permiten acceder a redes protegidas solamente mediante WEP.

Suplantacion: es un ataque en el que el intruso pretende tomar la identidad de un usuario autorizado. Una variante de este es la escucha o eavesdropping. Como las comunicaciones inalámbricas viajan libremente por el aire cualquiera que esté equipado con una antena que opere en el rango de frecuencias adecuado y dentro del área de cobertura de la red podrá recibirlas. Una técnica es el spoofing que consiste en que el intruso consigue suplantar la identidad de una fuente de datos autorizada para enviar información errónea a través de la red. Otra técnica es la captura de canales o hijacking, que sucede cuando un intruso se

hace con un canal que, desde ese momento, ya no estará accesible para usuarios autorizados disminuyendo así las prestaciones de la red. Otra posibilidad es que un punto de acceso intruso logre conectarse a la red para que las estaciones le envíen información reservada como son nombres de usuario o contraseñas.

Denegación de servicio (DoS): ataques en los que el intruso consigue que los usuarios autorizados no puedan conectarse a la red. Hay algunos ataques de denegación de servicio como crear un nivel elevado de interferencias en una zona cercana al punto de acceso, ataques por sincronización (Smurf) donde el intruso envía un mensaje broadcast con una dirección IP falsa que, al ser recibida, causa un aumento enorme de la carga de red.

Mecanismos de Seguridad

La seguridad WIFI abarca dos niveles. En el nivel más bajo, se encuentran los mecanismos de cifrado de la información, y en el nivel superior los procesos de autenticación. Al igual que en el resto de redes, la seguridad para las redes wireless se concentra en el control y la privacidad de los accesos. Un control de accesos fuerte impide la comunicación entre los usuarios no autorizados a través de los AP. Por otro lado, la privacidad garantiza que solo los usuarios a los que van destinados los datos transmitidos los comprendan. Así, la privacidad de los datos transmitidos solo queda protegida cuando los datos son encriptados con una clave que solo puede ser utilizada por el receptor al que están destinados esos datos. La seguridad en las comunicaciones se describe a menudo en términos de tres elementos:

Autenticación: garantiza que los nodos son quién y lo que dicen ser. Se basa normalmente en demostrar el conocimiento de un secreto compartido, como la pareja nombre de usuario y contraseña.

Confidencialidad: (privacidad) asegura que los intrusos no pueden leer el tráfico de red. Típicamente, la confidencialidad se protege mediante el cifrado del contenido del mensaje, donde esté cifrado aplica un método reversible de transformación (llamado algoritmo de cifrado o encriptación) al contenido del mensaje original (llamado texto plano), codificándolo u ocultándolo para crear el texto cifrado. Y sólo los que saben cómo revertir el proceso (descifrar el mensaje) pueden recuperar el texto original.

Integridad: asegura que los mensajes son entregados sin alteración. Esta se refiere a la capacidad de asegurarse de que el mensaje recibido no ha sido alterado de manera alguna y que es idéntico al mensaje que se envió. Los bytes de la secuencia de verificación de trama (Frame Check Sequence - FCS) son un ejemplo de comprobación de integridad, pero no se consideran seguros.

La seguridad es siempre relativa, nunca absoluta. Para cada defensa, hay (o seguro habrá) un ataque exitoso, y para cada ataque, hay (o seguro habrá) una defensa exitosa. Cuanto mejor sea la defensa, más tiempo y esfuerzo se necesita para romperla. La defensa adecuada es aquella que está equilibrada y que coincide con el número esperado de ataques.

Criptografía aplicada a redes inalámbricas

Como mencionamos anteriormente, la confidencialidad (impedir el acceso no autorizado a los contenidos de un mensaje) se logra mediante la protección del contenido de los datos con el cifrado. El cifrado es opcional en las WLAN, pero sin él, cualquier dispositivo compatible con el estándar dentro del alcance de la red puede leer todo su tráfico. Principalmente ha habido tres métodos de encriptación para hacer seguras las redes WLAN. Desde finales de 1990, los algoritmos de seguridad Wi-Fi han sufrido múltiples actualizaciones con una pura y simple depreciación de los algoritmos más antiguos y una sustancial revisión de los algoritmos más recientes. En orden cronológico de aparición, estos son:

- WEP (Wired Equivalent Privacy):

    - Fue ratificado en septiembre de 1999.
    - En español Privacidad equivalente a cableado
    - Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación) o de 128 bits (104 bits más 24 bits del IV).
    - RC4: Cifrador de flujo con longitudes de llave 8 a 2048 bits (128 bits por defecto) en múltiplos de 8 bits. Puede ser inseguro dependiendo del uso que se le de.
    - Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad.
    - Las primeras versiones no eran particularmente fuertes.
    - Hay tres tipos principales de claves WEP: Una clave WEP estándar de 64 bit, una clave WEP de 128 bits y una clave WEP de 256 bit. La clave de 64 bit es la de seguridad más corta y la más débil, mientras que la de 256 bit es la más fuerte. Los usuarios de redes inalámbricas generalmente suelen utilizar una configuración de 64 bit o 128 bit, ya que la plena seguridad de 256 bits no es necesaria.
    - A pesar de la introducción de WEP 256 bits, 128 bits sigue siendo la más usada.
    - Con el tiempo se fueron descubriendo fallos de seguridad y por la capacidad cada vez mayor de potencia de cálculo de las computadoras , fue cada vez más fácil explotarlos.
    - Antes de 2005 el FBI hizo una demostración pública (en un esfuerzo por aumentar la conciencia de las debilidades de WEP) en la que rompían las contraseñas WEP en minutos utilizando software de libre distribución.
    - Sigue siendo utilizado pero es muy vulnerable por lo que deberían ser actualizados aquellos sistemas basados en WEP.

- WPA (Wi-Fi Protected Access):

- El grupo Wi-Fi Alliance estableció WPA a principios de 2003 para hacer frente a las vulnerabilidades de WEP.
- La configuración más común es WPA - PSK (Pre-shared Key).
- Psk: es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice. Para crear una clave de secreto compartido, se debe utilizar la función de derivación de claves. Estos sistemas utilizan casi siempre algoritmos criptográficos de clave simétrica. El término PSK se utiliza en cifrado Wi-Fi como WEP o WPA, donde tanto el punto de acceso inalámbrico (AP) como todos los clientes comparten la misma clave.
- Las claves son de 256 bits y de 8 o más caracteres de longitud y hasta un máximo de 63.

Algunos de los cambios:

- Comprobación de integridad del mensaje (para determinar si un atacante había capturado o alterado paquetes transmitidos entre el punto de acceso y el cliente.
- Protocolo de integridad de clave temporal (Temporal Key Integrity Protocol - TKIP): utiliza un sistema de claves por paquete que era radicalmente más segura que la clave fija utilizada en el sistema WEP. Donde luego fue reemplazado más tarde por el Advanced Encryption Standard (AES).

- WPA2 (Wi-Fi Protected Access, version 2):

  - WPA es sustituido por WAP2 a partir del 2006.
  - Uno de los cambios más significativo fue el uso obligatorio de los algoritmos AES y la introducción de CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) como un reemplazo del TKIP.
  - AES: El Advanced Encryption Standard, abreviado AES, se usa con el fin de cifrar datos y de protegerlos contra cualquier acceso ilícito. El método criptográfico emplea para este objetivo una clave de longitud variada y se denomina según la longitud de clave usada AES-128, AES-192 o AES-256. Es un algoritmo cifrador de bloques de 128 bits con una llave de longitud variable de 128, 192 o 256 bits. Deriva de un algoritmo llamado Rijndael. No posee patentes.
  - CCMP: El protocolo CCMP en Wi-Fi significa Counter Mode CBC-MAC Protocol, y es que AES puede operar en varios modos diferentes, dependiendo de cómo se gestione el cifrado de los datos, la autenticación de los mensajes y su integridad.
  - La principal vulnerabilidad requiere que el atacante ya tenga acceso a la red Wi-Fi protegida con el fin de tener acceso a ciertas claves para luego perpetrar un ataque en contra de los dispositivos de la red.

- WPA3 (Wi-Fi Protected Access, version 3):

  - Anunciado en enero de 2018, por la Wi-Fi Alliance. Se esperaba una amplia implementación hasta finales de 2019 como muy pronto.
  - Existen dos tipos: el WPA3 Personal y el WPA3 empresarial

- Mayor protección ante ataques, incluso cuando no se cuenta con una contraseña fuerte.
- Cifrado de tráfico entre dispositivos y puntos de acceso, de manera que intensifica la protección en redes públicas.
- Cifrado de 192 bits para redes empresariales o personales, donde se traten datos confidenciales.
- Configuración más amable y simplificada para el emparejamiento de dispositivos.

A continuación realizamos una lista de clasificación de métodos actuales de seguridad Wi-Fi de mejor a peor:

1. WPA3
2. WPA2 + AES
3. WPA + AES
4. WPA + TKIP/AES (TKIP aparece como método alternativo)
5. WPA + TKIP
6. WEP
7. Red abierta (ningún tipo de seguridad)