

1 Introducción a redes inalámbricas

Las redes inalámbricas utilizan ondas de radio para conectar dispositivos, sin el uso de cables. Los dispositivos más comunes a conectarse son los ordenadores de escritorio o portátil, teléfonos, tabletas, netbooks y dispositivos localizadores. Las redes inalámbricas tienen varios propósitos una de ellas puede ser para obtener o proporcionar datos desde ubicaciones remotas.

La infraestructura inalámbrica tiene un costo mucho menor que el cableado tradicional. La red inalámbrica permite que los dispositivos remotos se conecten sin dificultad, sin depender si está alejado por metros o kilómetros, Esto sin necesidad de cable o instalación de conectores, la cual hace esta tecnología tan popular y muy usado. Hay varias otras tecnologías que difieren en la frecuencia que se usa, la velocidad, y el alcance que este tiene.

Las ondas electromagnéticas se transmiten en los dispositivos, pero suelen tener interferencias por la cual adoptan las regulaciones que definan los rangos de frecuencias y la potencia de transmisión. Estas ondas electromagnéticas no se limitan fácilmente a un área y por esta causa hackers pueden escuchar una red si este no se encuentra codificado por lo cual se debe garantizar la privacidad de los datos transmitidos.

2 Tecnologías inalámbricas

Las redes inalámbricas se clasifican en 4 grupos según la aplicación y el alcance: Para una red personal está la WPAN, red local está la WLAN, red metropolitana esta la WMAN y para una red amplia esta la WWAN. Estas redes inalámbricas también se pueden dividir en 2 segmentos: corto y largo alcance. El corto alcance tiene un área limitada la cual aplican a una red LAN y también sería una red PAN la cual son dispositivos que necesitan estar cerca para comunicarse. En la de largo alcance, la conectividad es comúnmente proporcionado por empresas que comercializan la conectividad inalámbrica como son los servicios. Estas redes abarcan grandes áreas la cual ocuparían una red WMAN. Este tiene el propósito de tener cobertura a nivel mundial. La red más común para un largo alcance sería la red inalámbrica WWAN o en caso de una cobertura global están las redes satélites

2.1 Redes inalámbricas de área personal (WPAN)

Las redes WPAN se basan en el estándar IEEE 802.15, este tiene un rango de alcance muy corta unos 10 metros. Las redes WPAN se caracterizan por un bajo consumo de energía y una baja velocidad de transmisión, son tecnologías como Bluetooth, IrDA, ZingBee y UWB.

Bluetooth

Este pertenece al estándar IEEE 802.15.1. Fue diseñado para una comunicación omnidireccionales (punto a multipunto), remplazando cables y conectando los dispositivos a una conexión ad hoc por radio.

Los dispositivos que tienen esta tecnología se clasifican en 3 grupos dando rangos de 100 metros, 10 metros y 1 metro. La banda de 2.4 GHz permite que 2 dispositivos dentro del rango puedan compartir hasta una velocidad de transferencia de 720 Kbps siendo la clase 2 la más usada.

La red Bluetooth también se domina piconet y está compuesto por 8 dispositivos con una relación de maestro-esclavo, siendo maestro el dispositivo Bluetooth y los demás esclavos, este tiene un alcance de 10 metros o en ocasiones puede llegar a 100 metros. Para tener una seguridad los enlaces son codificados y protegidos de las escuchas e interferencias. Se pueden conectar 2 piconet formando una red dispersa (scatternet). Permitiendo la posibilidad de que la información pueda llegar más allá de la cobertura de una piconet. En la red dispersa un dispositivo puede ser esclavo de varias piconet pero ser maestro de una de ellas.

IrDA

Esta red está denominada como Asociación de Datos por Interferencias, es un conjunto de estándares para la comunicación por infrarrojos. Es un estándar de transmisión de datos ad-hoc de bajo consumo de energía, bajo costo, unidireccional, cono de ángulo estrecho ($<30^\circ$), opera a distancias de 1m y una velocidad de 9600 bps a 4Mbps, los dispositivos pueden ser portátiles, impresoras o cámaras.

ZigBee

Está basada en el estándar IEEE 802.15.4, es un estándar global abierto que aborda la fácil aplicación, alta fiabilidad, bajo costo, bajo consumo de energía y baja velocidad de transmisión de datos. Opera en las bandas sin licencia de 2.4 GHz 900 MHz y 868 MHz con velocidad de transmisión de 250 Kbps. En la red pueden participar 2 tipos de dispositivos: dispositivos de funcionalidad completa (FFD) y dispositivo de funcionalidad reducida (RFD). Los FFD pueden operar 3 modos, como coordinador de WPAN, coordinador o dispositivo, El RFD es solo para aplicaciones simples, como interruptor de luz. La red ZigBEE puede soportar 3 tipologías: estrella, malla y árbol.

UWB

Basado en el estándar IEEE 802.15.3, tiene una alta velocidad y corto alcance en interiores. UWB permite transmitir archivos grandes a altas velocidades en cortas distancias. Ofrece una velocidad de 110 Mbps hasta 480 Mbps a una distancia de pocos metros, la frecuencia de banda está entre 3.1 GHz a 10.6 GHz en América y en Europa existen 2 bandas de 3.4 GHz a 4.8 GHz y de 6GHz a 8.5GHz. UWB transmite información mediante la emisión de pulsos de corta duración y gran ancho de banda, permitiendo modulaciones por posición o tiempo de pulso.

2.2 Redes inalámbricas de área local (WLAN)

Está diseñado para brindar acceso en zonas con rango de 100 metros, se usa en lugares como: hogar, escuelas, oficinas, etc. Esto permite movilidad dentro del área de cobertura. Se basa en el estándar IEEE

802.11 y conocidos como WI-FI. Este estándar está compuesto por diferentes estándares. EL IEEE 802.11b fue el primer estándar aceptado con hasta 11 Mbps con una banda de frecuencia de 2.4 GHz. Después siguió el estándar IEEE 802.11g siendo el sucesor de 802.11b con un mayor ancho de banda. Un punto de acceso IEEE 802.11g soporta clientes 802.11b ya que utilizan la misma banda de 2.4 GHz, La velocidad de transferencia es de 54 Mbps y se reduce si la señal de radio es débil o si hay interferencia.

2.3 Redes inalámbricas de área metropolitana (WMAN)

Se basan en el estándar IEEE 802.16, denominado como WiMAX (worldwide interoperability for microwave access), es una tecnología de comunicación con arquitectura punto a multipunto orientada a una alta velocidad de transmisión de datos. Se puede decir que WiMAX es como el Wi-Fi pero con más cobertura, este opera en 2 bandas de frecuencia una con licencia y la otra sin licencia, de 2 GHz a 11 GHz y de 10 GHz a 66 GHz, pueden alcanzar velocidades de transmisión a 70 Mbps en una distancia de 50 km.

2.4 Redes inalámbricas de área amplia (WWAN)

Esta red se extiende más allá de los 50 km y suelen usar frecuencias con licencia, pueden estar en grandes áreas como ciudades o países. Existen 2 tecnologías disponibles: telefonía móvil y los satélites

Red de telefonía móvil

En esta red el área de cobertura se divide por celdas. Los dispositivos móviles están conectados a una estación base y estas a una central de comunicación de telefonía que une el teléfono móvil y la red cableada de telefonía.

Existen diferentes generaciones de telefonía móvil desde 1980, empezando con la primera generación, 1G la cual era analógica y solo era para llamadas de voz con una velocidad de 2.4 kbs. La segunda generación, 2G es de tecnología digital, permite mensajes a una velocidad de datos 64 kbps. La 2.5G versión mejorada de 2G y una velocidad de 144 Kbps. Generación 3G en el año 2000 con velocidad de datos de 2 Mbps. La 3.5G versión mejorada que utiliza HSDPA acelerando transferencia hasta 14 Mbps Cuarta generación, 4G velocidad de 1 Gbps con cualquier tipo de servicio y por último la 5G lanzada en el 2020 con una mejor velocidad de datos.

Satélite

Por su gran altura estos pueden cubrir una amplia área sobre la superficie tierra. Útiles en zonas remotas o islas, submarinos en servicio la cual necesitarían un teléfono vía satélite. Los satélites están equipados con varios transpondedores que consta de un transceptor y una antena. La señal entrante se amplifica y se retransmite en una frecuencia diferente.

3 Arquitectura de red

3.1 Términos y terminología

La arquitectura lógica del estándar 802.11 tiene varios componentes: la estación (STA), punto de acceso inalámbrico (AP), conjunto independiente de servicios básicos (IBSS), conjunto de servicios básicos (BSS), red de distribución (DS) y conjunto de servicios extendidos (ESS).

- Una STA puede ser una PC, ordenador portátil, una PDA, teléfono cualquier dispositivo que tenga un medio inalámbrico
- Un AP es un dispositivo que permite a los dispositivos inalámbricos conectarse a una red cableada mediante WIFI.
- Un BSS es como un maestro que controla las estaciones dentro BSS, un BSS simple está compuesto de un AP y una STA.
- Un ESS es uno o más conjuntos de BSS que aparecen como un solo BSS a la capa de control de enlace lógico de cualquier estación asociada con una de esas BSS.
- Un DS es el mecanismo por el cual diferentes puntos de acceso pueden intercambiar tramas entre sí o bien con las redes cableadas

3.2 Arquitecturas

Modo Ad hoc

Al usar este modo los dispositivos de la red inalámbrica se conectan directamente entre sí, en modo de comunicación punto a punto. Este modo es el más adecuado para un pequeño grupo de dispositivos que están físicamente en estrecha entre sí, el rendimiento se ve afectado si el número de dispositivos aumenta. Las desconexiones ocurren con frecuencia y la gestión de red es una tarea difícil, Este modo no puede conectarse con una red de área local cableada por la cual no podrá acceder a internet.

Modo infraestructura

En este modo los dispositivos están conectados a la red inalámbrica por medio de un punto de acceso como un router o switches la cual van pasando los datos a una Ethernet cableada, al tener conexión de varios puntos de acceso por una red troncal Ethernet por cable este puede expandir la cobertura de la red inalámbrica y a ello los clientes pueden moverse libremente del punto de acceso a otro y mantener la conexión sin cortes. Este modo ofrece mayor seguridad, facilidad de gestión y mucha escalabilidad y estabilidad.

Identificador del conjunto de servicios extendidos (ESSID)

Este es uno de los 2 tipos de identificadores del conjunto de servicios (SSID). Una red inalámbrica ad hoc sin punto de acceso se utiliza el identificador del conjunto de servicios básicos (BSSID). En una red inalámbrica de infraestructura, que incluye un punto de acceso se utiliza el ESSID. Un SSID se refiere a una clave alfanumérica de 32 caracteres que identifica una red inalámbrica de área local.

4 El estándar IEEE 802.11

Este es un conjunto de especificaciones de control de acceso al medio (MAC) y de la capa física (PHY) para la implementación de redes inalámbricas de área local en las bandas de frecuencia 2.4GHz, 5GHz y 60GHz. El estándar y las enmiendas constituyen la base de los productos para redes inalámbricas que utilizan la marca WIFI.

4.1 El protocolo 802.11

El estándar define 2 capas separadas la capa de enlace de datos del modelo de referencia OSI, la subcapa de control de enlace lógico y la subcapa de control de acceso al medio. El estándar define las especificaciones de estas subcapas al medio que se comunica por arriba con la capa de control de enlace lógico.

4.2 802.11 La trama MAC

El formato de la trama MAC comprende un conjunto de 9 campos que se proucen en un orden fijo en todas las tramas.

Campo control de trama

Este contiene información para definir el tipo de trama MAC 802.11 y proporcionar la información necesaria a los campos para entender como procesar la trama MAC.

- Protocol version: proporciona la versión actual del protocolo.
- Type and subtype: determina la función de la trama.
- To DS and from DS: indica si se dirige o sale del DS y solo se usa en las tramas de tipos de datos de las STA asociadas con un AP.
- More fragments: indica si hay más fragmentos de trama ya sea de tipo dato o de gestión
- Retry: indica si la trama está siendo retransmitida ya sea de tipo de datos o de gestión.
- Power management: indica si la STA que envía esta en modo activo o ahorro de energía.
- More data: indica a un STA que se encuentra en el modo de ahorro de energía que el AP tiene más tramas para enviar.
- WEP: indica si se utiliza cifrado y autenticación en trama.
- Order: indica que todas las tramas de datos recibidos deben ser procesadas en orden.

Campo duración/ID

Este se utiliza en las tramas de tipo de control, excepto las de subtipo Power Save (PS) Poll. Para indicar la duración restante necesaria hasta recibir la próxima transmisión de trama. Depende del tipo de trama, los 4 campos de dirección contendrán una combinación de los siguientes tipos de direcciones: BSS

identifier (BSSID), Destination Address (DA), Source Address (SA), Receiver Address (RA) y Transmitter Address (TA).

Control de secuencia

Este está formado por 2 subcapas, el número de fragmento que indica los fragmentos de cada trama, inicia en 0 y incrementa en 1 por cada fragmento de trama enviado y el número de secuencia que indica la secuencia de las tramas, empieza en el mismo número de cada trama enviada, de lo contrario va incrementando de 1 hasta 4095 y vuelve a empezar desde 0.

Cuerpo de la trama

Este contiene datos o la información incluida en cualquier trama del tipo de gestión o de datos.

4.3 Capa física PHY

En esta capa el estándar 802.11 define una serie de esquemas de codificación y transmisión para las comunicaciones inalámbricas. Los esquemas más comunes son Espectro ensanchado por salto de frecuencia (FHSS), Espectro ensanchado por secuencia directa (DSSS) y Multiplicación por división de frecuencias ortogonales (OFDM). Los estándares que existen en la capa PHY son los siguientes: 802.11, 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac.

5 Seguridad

Las redes inalámbricas no son tan seguras como las cableadas ya que en las redes inalámbricas pueden escuchar dentro del rango limitado en cambio al cableado puede estar protegido en sus extremos.

5.1 Comunicaciones seguras

Se describe en 3 elementos: autenticación, confidencialidad e integridad.

- La autenticación garantiza que los nodos son quien, y lo que dicen ser,
- La confidencialidad asegura que los intrusos no puedan leer el tráfico de red.
- La integridad asegura que los mensajes son entregados sin alteración.

5.2 Confidencialidad y encriptación

La confidencialidad se logra mediante la protección del contenido de datos con el cifrado. Hay 3 métodos de encriptación para las redes WLAN surgen a finales de 1990 y desde ahí los algoritmos de seguridad reciben múltiples actualizaciones.

- WEP (wired equivalent privacy)
- WPA (wi-fi protected access)
- WP2 (wi-fi protected access, version 2)

6 Ventajas y desventajas

Los beneficios que tiene las redes inalámbricas a comparación de las cableadas son la movilidad, rentabilidad y capacidad de adaptación, pero a su vez la desventaja de seguridad.

Ventajas

- Aumento de la eficiencia
- Mejor cobertura y movilidad
- Flexibilidad
- Ahorro de costes
- Adaptación
- Nuevas oportunidades/aplicaciones

Desventajas

- Seguridad
- Problemas de instalación
- Cobertura
- Velocidad de transmisión

7 Aplicaciones

Aplicaciones para dispositivos embebidos con conectividad Wi-Fi:

- Aplicaciones de control y proceso industrial, las conexiones son costosas o inconveniente
- Aplicaciones de emergencia que requieran configuración inmediata y transitoria.
- Aplicaciones móviles.
- Cámaras de vigilancias.
- Mercados verticales como medicina, educación o fabricación.
- Aplicaciones maquina a máquina, referida a tecnologías que permite los sistemas inalámbricos como a los cableados poder comunicarse con otros dispositivos del mismo.

REFERENCIAS

[1] J. Salazar, Redes Inalámbricas, República Checa: European Virtual Learning Plataform for Electrical and Information Engineering, 2016.