

2008

Universidad Tecnológica
de Bolívar

BLANCA LUZ MÉNDEZ MARRUGO

VÍCTOR ALEJANDRO PAYARES MARZOLA

[REDES AD-HOC, INALÁMBRICAS Y SENSORIALES]

En la actualidad hemos sido partícipes del auge y amplio desarrollo de la tecnología en el mundo, visto más notoriamente en la creación de dispositivos que garantizan la movilidad de los usuarios sin pérdida de información, para esto se han creado tecnologías que sustentan la solución a estas necesidades.

REDES AD-HOC, INALÁMBRICAS Y SENSORIALES

Autores

BLANCA LUZ MÉNDEZ MARRUGO

VÍCTOR ALEJANDRO PAYARES MARZOLA

Monografía presentada para optar el título de Ingeniero de Sistemas

Director

GIOVANNI VÁSQUEZ

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA - COLOMBIA

AGRADECIMIENTOS:

A Dios agradezco por darme la sabiduría y entendimiento necesarios para culminar con éxito esta etapa de mi vida. De igual manera agradezco a mis padres por su apoyo incondicional en los momentos en los que más los necesité; a mis hermanas por la motivación que me brindaron en todo momento; por último a mi compañera de monografía por todas las experiencias que adquirimos en el transcurso del desarrollo de este trabajo.

VÍCTOR ALEJANDRO PAYARES MARZOLA

Muchas gracias primero a Dios por darme la vida y la salud y permitirme culminar con éxito esta etapa, gracias a mis padres y abuelos por todo el apoyo económico, espiritual y sentimental que me brindaron, convirtiéndose en mi motivación más grande para continuar en esos momentos que me sentía desfallecer. Gracias a mi hermana por ser un ejemplo a seguir y por sus consejos en momentos oportunos, igualmente agradezco a mi compañero de monografía y carrera, por todo el conocimiento que juntos logramos alcanzar.

BLANCA LUZ MÉNDEZ MARRUGO

Artículo 105

La Universidad Tecnológica de Bolívar se reserva el derecho de propiedad de los trabajos de grado aprobados y no pueden ser explotados comercialmente sin autorización.

Nota de Aceptación

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cartagena de Indias, Enero de 2008

Cartagena D. T. Y C., enero de 2008

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS

Programa de Ingeniería de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Respetados señores:

Con toda atención nos dirigimos a ustedes con el fin de presentarles a su consideración, estudio y aprobación la monografía titulada REDES AD-HOC, INALÁMBRICAS Y SENSORIALES como requisito parcial para optar al título de ingeniero de sistemas.

Atentamente,

BLANCA LUZ MÉNDEZ MARRUGO

VÍCTOR A. PAYARES MARZOLA

Cartagena D. T. Y C., enero de 2008

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS

Programa de Ingeniería de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Cordial saludo:

A través de la presente me permito entregar la monografía titulada REDES AD-HOC, INALÁMBRICAS Y SENSORIALES para su estudio y evaluación la cual fue realizada por los estudiantes BLANCA LUZ MÉNDEZ MARRUGO y VÍCTOR ALEJANDRO PAYARES MARZOLA, de la cual acepto ser su director

Atentamente,

GIOVANNY R. VASQUEZ MENDOZA

AUTORIZACIÓN

Yo BLANCA LUZ MÉNDEZ MARRUGO, identificada con la cedula de ciudadanía numero 1.128.050.472 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo online de la Biblioteca.

BLANCA LUZ MÉNDEZ MARRUGO

AUTORIZACIÓN

Yo VÍCTOR ALEJANDRO PAYARES MARZOLA, identificado con la cedula de ciudadanía número 73.009.730 de Cartagena, autorizo a la Universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo online de la Biblioteca.

VÍCTOR ALEJANDRO PAYARES MARZOLA

RESUMEN

La necesidad de permitir a los usuarios conectarse desde cualquier lugar de un entorno sin la utilización de cableado, la reducción considerable en cuanto a costos de instalación y mantenimiento, sin perder ni bajar notablemente la conectividad; son características que han generado el gran avance en materia de la implementación de redes inalámbricas en oficinas, edificios, hogares y campus universitarios. Esto lleva consigo la utilización de arquitecturas dinámicas y protocolos que faciliten el control, la seguridad y el acceso al medio, en donde la arquitectura ad hoc viene a ser fuente fundamental de los entornos LAN.

Por su parte las redes sensoriales representan un gran avance que ha presentado mayor aplicabilidad en el campo de la medicina, conglomerando los aportes de cada una, para la creación de nuevas piezas robóticas que sirvan en la implementación de prótesis en seres humanos, y así contribuir desde la tecnología y la medicina, a hacer mas fácil la vida de las personas.

Cada una de estas tecnologías presenta un pool de protocolos que permiten la aplicabilidad y eficiencia de estas; a la vez que se encuentra bajo la supervisión y constante investigación del Institute of Electrical and Electronics Engineers (IEEE), entidad que las ha estandarizado, facilitando la creación de dispositivos que puedan trabajar con cada una de ellas y vislumbrando las novedades que presentan cada día a los usuarios.

TABLA DE CONTENIDO

	Pág
INTRODUCCIÓN	
IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA	
OBJETIVOS	
JUSTIFICACIÓN	
METODOLOGÍA DE LA INVESTIGACIÓN	
1. DESCRIPCIÓN GENERAL DE LAS TECNOLOGÍAS	1
1.1 Historia y Antecedentes	1
1.2 Redes Ad Hoc	2
1.2.1 Características Generales de las Redes Ad Hoc	2
1.3 Redes Inalámbricas	6
1.3.1 Características de las WLAN's	8
1.3.2 Dispositivos Utilizados	10
1.3.3 Tecnologías Inalámbricas	11
1.4 Redes Sensoriales	25
1.4.1 Características de las Redes Sensoriales	26
1.4.2 Especificaciones del Dispositivo	28
2. PROTOCOLOS UTILIZADOS	30
2.1 Protocolos Usados en las Redes Ad Hoc	30
2.1.1 Basados en Tablas de Enrutamiento	30
2.1.2 Basados en Enrutamiento Bajo Demanda	32
2.1.3 Protocolos Híbridos	38
2.2 Protocolos Usados en la Redes Inalámbricas	39
2.2.1 Protocolos de Seguridad en Redes Inalámbricas	45
2.3 Protocolos Usados en las Redes Sensoriales	51
3. ACCESO Y CONTROL	55
3.1 Acceso y control en las Redes Inalámbricas y de Arquitectura Ad-Hoc	55
3.1.1 Mecanismo de Intercambio de Mensajes con Reconocimiento Positivo (Reservation-Based Protocol)	58
3.1.2 Protocolo CSMA/CA	59
3.1.3 Funcionamiento de una Red Inalámbrica	60

3.2 Acceso y Control en las Redes Sensoriales	62
3.2.1 Protocolos Utilizados	64
4. FUTURO DE ESTAS TECNOLOGÍAS	73
4.1 Futuro de las Redes Inalámbricas	73
4.1.1 Características de las Redes MESH	76
4.2 Futuro de las Redes Sensoriales	79
CONCLUSIÓN	
RECOMENDACIONES	
GLOSARIO	
REFERENCIAS	

LISTA DE FIGURAS

	pág
Figura 1: redes inalámbricas.	7
Figura 2: Clasificación de las redes Inalámbricas 1.	9
Figura 3: Clasificación de las redes Inalámbricas 2.	9
Figura 4: Tecnología Wimax.	15
Figura 5: Tecnología Wifi.	20
Figura 6: Estilo Ac-Hoc.	20
Figura 7: Extended Service Set.	21
Figura 8: Capas de la arquitectura bluetooth.	24
Figura 9: Cobertura de las tecnologías inalámbricas.	25
Figura 10: Arquitectura de los sensores.	28
Figura 11: Arquitectura del Estándar 802.11.	32
Figura 12: algoritmo de acceso CSMA/CA.	59
Figura 13: IEEE 802.15.4 Trasmisión con beacons.	66
Figura 14: IEEE 802.15.4 Trasmisión con beacons y GTS.	67
Figura 15: Estados del protocolo S-MAC.	69
Figura 16: Modos de trabajo de B_MAC.	70
Figura 17: Escenario típico de MESH.	78

LISTA DE TABLAS

	Pág
Tabla 1: Protocolos de enrutamiento redes ac-hoc.	33
Tabla 2: Resumen del estándar 802.11a.	41
Tabla 3: Resumen del estándar 802.11b.	42
Tabla 4: Resumen del estándar 802.11g.	43
Tabla 5: Comparativo de estándares inalámbricos.	43

INTRODUCCIÓN

En la actualidad hemos sido partícipes del auge y amplio desarrollo de la tecnología en el mundo, visto más notoriamente en la creación de dispositivos de tecnología móvil, para lo cual han surgido nuevas topologías de redes que dan cobertura a dichos aparatos.

El Bluetooth, redes Wi-fi, Wimax y Ad Hoc, son algunas de las nuevas tecnologías de punta con mayor implementación en celulares, portátiles, computadores de escritorio, PDAs, Tablet PCs y Notebooks.

Los avances de estas nuevas tecnologías de la información en las telecomunicaciones demandan la creación de nuevas y sofisticadas aplicaciones que permitan acceder de forma segura a la información distribuida en Internet desde diversos tipos de dispositivos electrónicos e inalámbricos que requieren una conexión móvil y confiable que no sufra ningún tipo de desconexión en su paso de un punto de acceso a otro.

Es indudable el hecho de que la tecnología inalámbrica ha ganado muchos adeptos y popularidad en los últimos años en gran diversidad de mercados tales como hospitales, fábricas, bodegas, tiendas, pequeños negocios, entornos académicos o simplemente, en el propio hogar. Este éxito se debe, fundamentalmente, a la posibilidad que ofrece este tipo de tecnologías de tener acceso a la información y la comunicación sin tener que estar en un lugar físico específico. Por lo tanto, el futuro de las redes inalámbricas se presenta prometedor, ya que en la actualidad se prevé un crecimiento masivo en el ámbito de las comunicaciones móviles, y en concreto las WLAN, debido a la creciente exigencia de ancho de banda motivada por la gran popularización de Internet y la necesidad de tener acceso a aplicaciones multimedia.

Por tal motivo, este trabajo se enfoca en el conocimientos de tales tecnologías, con el fin de comprender su funcionamiento y aplicación, determinar cuáles son los protocolos de que hacen uso y cómo se ejerce control sobre los nodos implicados en la comunicación.

IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

Las comunicaciones actuales y la evolución de los sistemas hacia arquitecturas inalámbricas que permitan la cobertura a lugares donde el cableado no puede, han hecho de las redes inalámbricas un tema de estudio interesante a nivel académico, así como también la aplicabilidad que se le está viendo en la cotidianidad, con la aparición cada día de dispositivos más pequeños y livianos; y la inclusión de esta tecnología a entornos donde electrodomésticos, teléfonos móviles, PDA, entre otros, necesitan comunicarse de forma inteligente y a la vez transparente al usuario final; al igual que ejercen control sobre parámetros como la luz, temperatura, humedad, sonido, entre otros.

La necesidad de comprender el funcionamiento y generalidades de estas tecnologías, así como los estándares que les dan validez internacional, son temas que proponen la profundización en ellas, para servir de plataforma a otros investigadores que pretendan crear entornos inteligentes, y formar un concepto claro y conciso de lo que se busca con estas técnicas.

OBJETIVOS

OBJETIVO GENERAL:

Determinar de manera clara y concisa la funcionalidad, los requerimientos de instalación y la aplicabilidad de las redes inalámbricas, ad hoc y sensoriales, con el fin de comprender sus conceptos y vislumbrar el futuro de las telecomunicaciones en el entorno cotidiano.

OBJETIVOS ESPECÍFICOS:

- ❖ Analizar los estándares que dan validez a las redes inalámbricas, ad hoc y sensoriales acreditados por la IEEE.
- ❖ Conocer cada una de las arquitecturas y protocolos que permiten el buen funcionamiento de cada una de estas tecnologías.
- ❖ Identificar qué protocolos hacen más segura la transmisión en estas tecnologías, permitiendo su implementación en dispositivos de última generación.
- ❖ Determinar hacia donde van dirigidas las redes ad hoc, inalámbricas y sensoriales, para dar a conocer los avances e implementaciones de estas tecnologías.

JUSTIFICACIÓN

Las redes inalámbricas, así como las sensoriales y las fundamentadas en arquitectura ad hoc, han brindado la posibilidad al ser humano de lograr mayor conectividad y control sobre procesos que antes eran muy tediosos de realizar, así como los fenómenos naturales, el clima, la luz, entre otros; que nos llevan a pensar y algunos casos a ver, cómo se están sistematizando entornos tan cotidianos como el hogar o la oficina, brindando cobertura y velocidades de conectividad cada vez mayores.

En la actualidad podemos hablar incluso de la interdisciplinariedad entre las tecnologías de comunicación con otras áreas o profesiones logrando avances científicos que hacen más fácil la vida de las personas.

Muchas de las ventajas de estas tecnologías también son palpables en nuestro entorno, por lo que es importante para nosotros como profesionales ahondar en estos temas que seguramente nos serán muy útiles en un futuro cercano.

Por otro lado, los nuevos esquemas de comunicación, arquitecturas y protocolos, así como los dispositivos que incorporan tecnologías como estas, son también motivo de estudio para enriquecer y afianzar el conocimiento adquirido durante nuestra formación profesional.

METODOLOGÍA DE LA INVESTIGACIÓN

Este trabajo de grado se ha desarrollado bajo la metodología propia de una investigación de tipo documental o teórica, ya que se ha contado en gran parte con el apoyo de otras investigaciones previas en el área que sustentan la temática manejada en cada capítulo, así como fuentes bibliográficas y aportes de autores e investigadores en la rama.

El tiempo de duración estimado ha sido de cuatro meses, en los que en primera instancia se determinaron las necesidades por las cuales realizar la investigación y luego se fijaron los capítulos que contendría, en los que se desarrolla toda la temática. Para esto nos apoyamos en investigaciones que anteriormente fueron ejecutadas tanto dentro como fuera de nuestro entorno universitario, así como del país, logrando resultados satisfactorios.

1. DESCRIPCIÓN GENERAL DE LAS TECNOLOGÍAS

1.1 Historia y Antecedentes

Las redes inalámbricas se fueron desarrollando a partir de la necesidad de interconectar terminales a grandes distancias y del difícil acceso entre dispositivos, pero más adelante surgen las WLAN's (Wireless Local Area Network), que adquieren todas las ventajas de una red inalámbrica para entornos locales. Estas redes se remontan a los años 70, cuando en una fábrica suiza se obtuvieron los primeros resultados satisfactorios de comunicación inalámbrica dentro de una red local, desde ese momento, se han visto una creciente motivación y muy buenos resultados en las actividades encaminadas hacia la investigación y el desarrollo de dispositivos que hacen posible la comunicación mediante redes inalámbricas.

La fuerza que a la fecha ha cobrado esta tecnología se debe, en gran medida, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes cableadas convencionales.

Con el nacimiento de estas redes nace también la Ad-hoc, que fue a su vez denominada WLAN independiente o peer to peer, ya que brinda, junto a las redes de infraestructura, la posibilidad de configurar las WLAN, de tal forma que estas alcancen un máximo rendimiento y mayor funcionalidad. Esta configuración busca conectar dos o más computadores, mediante adaptadores inalámbricos, de tal forma que cuando dos o más de estos equipos están dentro del rango de alcance de los adaptadores pueden establecer una red independiente, haciéndolos esto que sean redes que generalmente no requieren administración o preconfiguración alguna, o también llamadas autoconfigurables y pueden lograr también un alcance extendido a un edificio completo.

Por su parte las redes sensoriales tienen sus inicios desde las redes cableadas, siendo de mucha utilidad para medir niveles de temperatura, líquido y humedad,

así como fenómenos naturales. “Muchos sensores en fábricas o coches por ejemplo, tienen su propia red que se conecta con un ordenador o una caja de controles a través de un cable y, al detectar una anomalía, envían un aviso a la caja de controles”.¹

1.2 Redes Ad-Hoc:

“Una red móvil ad-hoc (MANET) es una colección de nodos móviles autónomos que se comunican entre si mediante enlaces wireless, dónde no existe una infraestructura de red fija y la administración se realiza de forma descentralizada. En este nuevo entorno, los nodos participan en la toma de decisiones, realizando las funciones propias del mantenimiento de la red y tomando parte en los algoritmos de encaminamiento.

En general, cualquier propuesta real aplicable a una MANET deberá tener en cuenta las restricciones impuestas por las características inherentes a este tipo de redes”.²

Esta definición tomada de manera literal, refleja la capacidad que tienen los nodos para tomar sus propias decisiones dentro de la red y deja claro que en este tipo de redes no existe una jerarquía de trabajo entre los dispositivos, ni funciones específicas para cada uno, sino que por el contrario todos están en la capacidad de realizar todas las tareas requeridas para la transmisión de información.

Algunas características propias de esta topología se muestran a continuación.

1.2.1 Características Generales de las Redes Ad Hoc³:

¹ GONZÁLEZ VELASCO, Jorge Antonio; CAÑIZARES ORMAZA, Luis Vinicio. *Redes De Sensores*. Escuela Politécnica Nacional. <http://clusterfie.epn.edu.ec/ibernal/>

² VIDAL, Iván et. al. *Servicios de Valor Añadido en Redes Móviles Ad-hoc*. Universidad Carlos III, Madrid, España. http://www.it.uc3m.es/ividal/articulos/telecom03_adhoc.pdf

³ CORTÉS GRAJALES, Miguel Ángel; ALVIS LARA, Maryori Tatiana. *Redes Móviles Inalámbricas Ad Hoc*. Universidad Tecnológica de Bolívar, pág. 7 – 11, 2004.

Dentro de las características de estas redes que ya hemos venido hablando, tenemos la de que en principio mantienen una topología dinámica, operan de manera distribuida y con enrutamiento de múltiples saltos, poseen enlaces de ancho de banda y radio de transmisión limitados, errores en la transmisión y pérdidas de paquetes, terminales y seguridad física limitados, pueden trabajar tanto en entornos simétricos como asimétricos y poseen energía reducida. Estas características, de las que algunas también representan desventajas de esta topología especifican los aspectos a seguir al momento de implementar este tipo de redes.

- **Topología Dinámica:**

- Los cambios en la topología de red son imprevisibles, lo cual indica que los nodos pueden entrar y salir de ella cambiando el esquema de la misma.
- La conectividad entre terminales puede cambiar con el tiempo.
- Los mismos terminales están encargados tanto del tráfico como de las condiciones de propagación del medio, y deben adaptarse a esta.
- Tiene la capacidad de establecer enrutamiento dinámico entre los mismos nodos.

- **Operación Distribuida:**

- El control y el manejo de la red está distribuido entre todos los nodos.
- Todos los nodos involucrados en este tipo de redes se colaboran entre ellos mismos.

- **Enrutamiento de múltiples saltos (Multihop Routing):**
 - Poseen algoritmos que permiten el enrutamiento, estos algoritmos pueden ser de un solo salto (*single hop*) o de múltiples saltos, basados en diferentes atributos de enlace y de protocolos de enrutamiento.
 - En cuanto a su estructura e implementación se considera que los protocolos *single hop* o de un salto, son más simples que los *multihop* o múltiples saltos.
 - Para establecer una eficiente comunicación entre dos nodos que se encuentren distantes y fuera del rango directo de transmisión, es necesario que los paquetes viajen a través de nodos intermedios que permitan llegar hasta el destino.
 - En estas redes es frecuente que se presente el problema de terminales ocultas.
 - En ocasiones también puede presentar el problema del terminal expuesto.

- **Enlaces de Ancho de Banda Limitado:**
 - Se puede presentar una mayor tasa de error de bits, que la frecuentemente presentada en redes inalámbricas convencionales.
 - El medio o canal utilizado para la transmisión, es susceptible a factores como el ruido, la interferencia, el retardo o desvanecimiento.
 - Estas redes no han logrado alcanzar el ancho de banda que se ha logrado en las redes cableadas comunes.
 - Como se mencionó en el ítem anterior, en este tipo de ambiente inalámbrico el ancho de banda es usualmente restringido, por lo tanto el tráfico tanto para el mantenimiento de la red, como el causado por las aplicaciones debe ser mínimo, evitando así una gran ocupación del canal y facilitando la comunicación.

- **Radio de Transmisión Limitado:**

Debido a la naturaleza inalámbrica, la distancia y la potencia están limitadas. Conforme la distancia aumenta la velocidad de transmisión disminuye.

- **Errores de Transmisión o Pérdidas de Paquetes:**

Estas pérdidas son debido a varios intentos de retransmisión predeterminadas y a factores como calidad de enlace, información de rutas desactualizadas, y desbordamiento de buffer.

- **Terminales limitados.**

- Esta característica se debe a que los nodos en las redes Ad hoc son dispositivos móviles con capacidad de procesamiento y memoria pequeños y reducido poder de almacenamiento de energía (Batería).
- Se necesitan algoritmos optimizados en cada uno de los nodos para que presenten mayor eficiencia en cada nodo, debido a las limitaciones que estos poseen, como las mencionadas en el ítem anterior.

- **Seguridad Física Limitada:**

En las redes de topología Ad Hoc, la seguridad está medida según los mismos criterios que se tienen para las redes comunes, como los son la confidencialidad, integridad, autenticación, encriptación y disponibilidad.

- **Trabajo en Entornos Simétricos y Asimétricos:**

- Pueden tener diferentes radios de transmisión.
- La duración de la batería difiere de acuerdo al equipo utilizado.
- Capacidad de procesamiento diferente en cada equipo.
- Se pueden utilizar tecnologías diferentes o iguales.

- **Energía Reducida:**

Los dispositivos móviles que conforman la red, dependen de baterías.

1.3 Redes Inalámbricas:

Las redes inalámbricas buscan conectar dos o mas nodos en una red, sin la utilización de medios guiados como el cable coaxial, utp, o de fibra óptica; con miras a hacer más fácil la comunicación y transmisión de información hacia lugares donde es imposible o es necesario que los nodos estén en constante movimiento.

Hasta el momento es difícil considerar la idea que las redes inalámbricas remplacen a las cableadas, debido a que con estas últimas se ha logrado alcanzar velocidades de transmisión mayores que las logradas con la tecnología inalámbrica, la cual actualmente ofrecen velocidades de 2 Mbps, mientras que las redes cableadas logran velocidades de 10 Mbps y se espera que lleguen hasta 100 Mbps. Además con los sistemas de Cable de Fibra Óptica se tienen velocidades aún mayores, mientras que las redes inalámbricas se prevé que alcancen velocidades de solo 10 Mbps.

Debido a algunas de estas limitantes, esta tecnología se ha fortalecido en las implementaciones a nivel de redes LAN, con la creación de las llamadas WLAN (Wireless Local Area Network).

Una red de área local o WLAN (Wireless LAN) puede definirse como una red local que para enlazar los equipos conectados a ella, no hace uso de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas, sino que usa como medios de unión entre sus terminales un medio inalámbrico, como por ejemplo la radio, los infrarrojos, el láser, tecnología Bluetooth o Wi-fi.

Las WLAN cuentan con dos tipos de topologías, la peer-to-peer o la de infraestructura (ver figura 1) que han surgido como una opción dentro de la corriente hacia la movilidad universal en base a una filosofía "seamless" o sin discontinuidades, es decir, que permita el paso a través de diferentes entornos de una manera transparente. Estas redes necesitan de una velocidad de transmisión mínima establecido por la IEEE 802.11 que es de 1 Mbps, aunque actualmente se alcanzan velocidades de 2 Mbps, y además deben trabajar en el entorno de frecuencias de 2,45 GHz⁴.



Figura 1 Redes Inalámbricas Tomada de Modelo de Cobertura de Redes Inalámbricas
Néstor García Fernández Pág.20

Una de la causas principales para el incremento acelerado de aplicabilidad de estas redes, ha sido la también creciente aparición en el mercado tecnológico, de dispositivos como las PDA's, Laptop's y celulares de última generación, siendo cada vez más útiles y necesarios en la cotidianidad de las personas, debido a la movilidad que los caracteriza, para lo cual necesitan de una red que soporte todos los requerimientos propio de su tecnología.

En una LAN convencional, cableada, si una aplicación necesita información de una base de datos central tiene que conectarse a la red mediante una estación de

⁴ UNIVERSIDAD INCCA DE COLOMBIA. Artículo: *Redes Locales Inalámbricas*
<http://www.unincca.edu.co/boletin/indice.htm>

acogida o "docking station", pero no puede estar en movimiento continuo y libre. La WLAN puede ser autocontenida o bien puede actuar como una extensión de la red de cable Ethernet o Token-Ring.

1.3.1 Características de las WLAN's:

- Permite una fácil incorporación de nuevos usuarios a la red.
Estas redes son de topología dinámica, lo cual les permite garantizar la movilidad de los equipos que pertenezcan a ella, siendo adaptables a la hora de integrar un nuevo dispositivo.
- Ofrece una alternativa de bajo costo a los sistemas cableados.
Una de las principales características de estas redes que ha permitido crear más soluciones con esta tecnología, son los bajos costos de implementación frente a las cableadas, garantizando también un rendimiento óptimo a las necesidades de la red.
- Posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red; es decir que es posible adquirir a través de estas, los mismos servicios a los que se tiene acceso mediante una red cableada.

Para estas redes la clasificación puede ser de manera similar a las redes cableadas convencionales⁵ (ver figura 2 y 3):

- WAN/MAN (Wide Area Network/Metropolitan Area Network)
- LAN (Local Area Network)
- PAN (Personal Area Network)

⁵ GARCÍA FERNÁNDEZ, Nestor. *Modelo de Cobertura de Redes Inalámbricas*. Pág. 6-7. Marzo de 2006

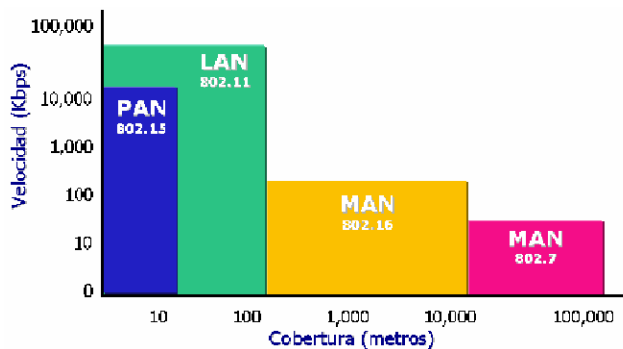


Figura 2 Clasificación de las redes Inalámbricas 1 Tomada de Modelo de Cobertura de Redes Inalámbricas Pág.6

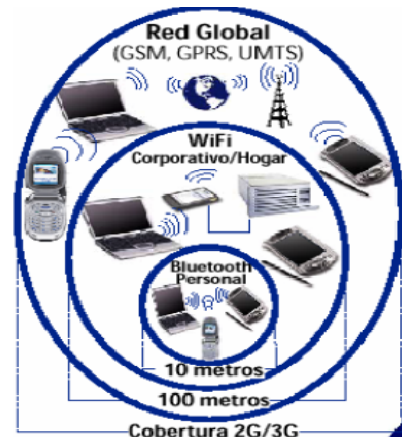


Figura 3 Clasificación de las redes Inalámbricas 2 Tomada de Modelo de Cobertura de Redes Inalámbricas Pág.6

En la primera categoría WAN/MAN, están ubicadas las redes que cubren decenas y hasta miles de kilómetros, y que tienen como objetivo la conectividad a nivel global. Las tecnologías presentes en esta clasificación, comprenden por lo general tecnologías de redes móviles como por ejemplo los siguientes sistemas:

- GSM (Global System for Mobile Communications): Sistema global de comunicaciones móviles de 2ª generación (2G) que permite comunicaciones de hasta 9,6 Kbps.
- GPRS (General Packet Radio Service): Estándar de comunicaciones móviles que permite velocidades de hasta 115 Kbps.
- UMTS (Universal Mobile Telecommunications System): Tecnología de comunicaciones móviles de 3º generación (3G) que ofrece velocidades desde 144 Kbps hasta 2 Mbps.

La categoría LAN, comprende las redes cuya cobertura alcanza desde varios metros hasta decenas de metros. Permiten la creación de redes locales, como su nombre lo indica, sin la utilización de cables y realizando la comunicación por

ondas de radio. La tecnología más conocida de esta clasificación es el estándar 802.11 (WiFi) que opera dentro de los 2.4 GHz (5 GHz 802.11a) y provee un ancho de banda de hasta 54 Mbps.

Por último, la categoría PAN comprende las redes que abarcan desde muy poca distancia hasta 30 metros. Estas son redes personales que tienen como objetivo eliminar los cables de comunicación en todos los dispositivos electrónicos (PC con periféricos o accesorios, teléfonos móviles, cámaras...). La tecnología más implementada de este tipo es la Bluetooth, pero existen otras como 802.15 y HomeRF.

1.3.2 Dispositivos Utilizados:

Para la implementación de una red inalámbrica, específicamente en un entorno LAN, sólo se necesita de dos dispositivos esenciales para establecer la comunicación, la tarjeta de red inalámbrica (NIC Inalámbrica) y un punto de acceso (AP, Access Point); en estas redes ambos dispositivos pueden funcionar como servidores y clientes, la topología que estaría en uso sería la de infraestructura, cuyos principios se presentan a continuación.

Por un lado, el AP se conecta a la LAN de manera cableada con el fin de proporcionar acceso a Internet y conectividad a la red cableada.

Por otro lado, los AP poseen antenas que proporcionan conectividad inalámbrica o cobertura a un área específica o celda.

Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar, siendo regularmente, el alcance de 91,44 a 152,4 metros (300 a 500 pies).

Cuando se requiere alcanzar una cobertura mayor a una celda, se pueden instalar múltiples AP's según sea necesario, con cierto grado de superposición, lo cual permite pasar de una celda a otra (roaming). Este mecanismo o forma de comunicación es muy implementado por los operadores de telefonía móvil o celular quienes garantizan a sus usuarios la conectividad sin que este último tenga conocimiento del traslado de una celda a otra lo que permite el constante movimiento de los dispositivos dentro de la WLAN⁶.

1.3.3 Tecnologías inalámbricas

En la actualidad las tecnologías inalámbricas han tenido una gran acogida por sus bajos costos de implementación y buen rendimiento en entornos de oficina, edificios y campus, pero sin lugar a dudas dentro de las más destacadas encontramos la tecnología wi-fi, wimax, infrarrojo y bluetooth, de las cuales se presentará un esquema general que permita un claro y concreto conocimiento de las redes inalámbricas.

- Tecnología GSM:

Esta tecnología tiene como propósito inicial que el sistema permita la libre circulación de dispositivos móviles celulares de una red a otra ("roaming"). Esto indica que un usuario de una determinada red nacional puede tener acceso a todos los servicios cuando viaja entre varios países, es decir que la propia

⁶ UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR, Minor de Comunicaciones y Redes, *Medios de Transmisión*.

estación móvil GSM le permite al usuario llamar o ser llamado donde quiera que se encuentre dentro del área internacional de cobertura⁷.

Como se ha mencionado con anterioridad esta es una tecnología utilizada para dispositivos móviles, como celulares y Smart Phones.

Como estándar de telefonía, GSM comienza a gestarse en 1982 cuando la Conferencia de Administraciones Europeas de Correos y Telecomunicaciones (CEPT), al tratar de resolver los problemas que se habían formado por el desarrollo descoordinado e incompatible de los sistemas móviles celulares en diferentes países de la CEPT, determinó:

- Crear un equipo con el nombre de Groupe Special Mobile (GSM), que se encargara del desarrollo de un conjunto de estándares para una futura red celular de comunicaciones móviles de ámbito paneuropeo.
- Recomendar la reserva de dos subbandas de frecuencias próximas a 900 MHz para este sistema.

Los problemas que más se destacaban eran:

- No poder disponer de un mismo dispositivo móvil al pasar de un país al otro.
- No disponer de un mercado propio suficientemente extenso, con lo que se dificultaba la consolidación de una industria europea de sistemas móviles competitiva a nivel mundial, hay que tener en cuenta que estos avances tuvieron sus inicios en la comunidad europea.

⁷ HERNÁNDEZ CARDOSA, Amaterazú. Tesis: *Operación de una radio base celular cuando coexisten GSM & IS-54, IS-136*, Universidad de Las Américas. Puebla, México
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/capitulo4.pdf

Se adoptó entonces la decisión de que el sistema fuera digital, en lugar de analógico, lo cual permitió mejorar la eficiencia espectral, mejor calidad de transmisión, posibilidades de nuevos servicios y otras importantes como la seguridad. También permitió el desarrollo y utilización de tecnología VLSI para la fabricación de chips electrónicos, lo que hizo posible la creación de móviles más pequeños y baratos, y en definitiva el uso de un sistema digital que complementaría el desarrollo de la Red Digital de Servicios Integrados o RDSI, con la que GSM tiene una interfaz.

En 1990, por requerimiento del Reino Unido, se añadió al grupo de estandarización la especificación de una versión de GSM a la banda de frecuencia de 1800 ± 75 MHz. A esta variante se le llamó DCS1800 ("Digital Cellular System 1800"), esto con el objetivo de implementar esta tecnología en dispositivos, pero fue sólo hasta junio de 1992 cuando aparecieron los primeros portátiles GSM de mano, dando pie al servicio comercial del sistema GSM, donde el tamaño de las áreas de cobertura y el número de usuarios era bastante dispar, además que las redes funcionaban basándose en las especificaciones de la fase 1 y no todos los servicios contemplados en ella estaban disponibles.

Estructura del sistema GSM:

En lo que se refiere a la estructura básica del sistema GSM, está organizado como una red de células radioeléctricas continuas las cuales brindan una gran cobertura a todo el área de servicio. Cada una de estas células pertenece a una estación base (BTS) que trabaja en un conjunto de canales de radio diferentes a los utilizados por las células adyacentes contenidas según un plan celular. Un grupo de estos BTSs están interconectados a un controlador de estaciones base (BSC), el cual tiene como tareas principales el handover o

traspaso del móvil de una célula a otra, y el control de potencia en las BTSs y los móviles. Por lo tanto, se puede decir que el BSC está encargado del manejo de toda la red de radio. Ahora, una o varias de estas BSCs están a su vez conectadas a una central de conmutación de móviles (MSC), este dispositivo es el corazón del GSM y es responsable de la inicialización, enrutamiento, control y finalización de las llamadas, así como de la información sobre la tarificación. Este es también la interfaz entre diversas redes GSM o entre una de ellas y las redes públicas de telefonía o datos.

- Tecnología Wimax:

Wimax⁸ viene de las iniciales de Worldwide Interoperability for Microwave Access (Interoperabilidad Mundial para el Acceso por Microondas), es considerado como el futuro de las redes WiFi y aunque soportará multitud de protocolos, el más importante será el protocolo 802.16x, sucesor del 802.11.

Haciendo un poco de historia en Enero de 2003, el IEEE aprobó el estándar 802.16a, el cual cubre las bandas de frecuencias entre 2 GHz y 11 GHz; este estándar es una extensión del estándar IEEE 802.16 para 10-66 GHz publicado en Abril de 2002. Este sub-rango de frecuencias en 11 GHz permite el buen desempeño de enlaces sin 'línea de vista', lo cual hace al IEEE802.16a la tecnología apropiada para aplicaciones de última milla, en donde los obstáculos como árboles y edificios están siempre presentes y las estaciones bases pueden necesitar ser montadas sin discreciones en los techos de viviendas o edificios en vez de en torres o montañas.

Una representación que resume todas las soluciones de este estándar y la forma de implementación, es presentada en la Figura 4.

⁸ BLAT, Fernando, *Wimax a Fondo*. <http://www.xataka.com>

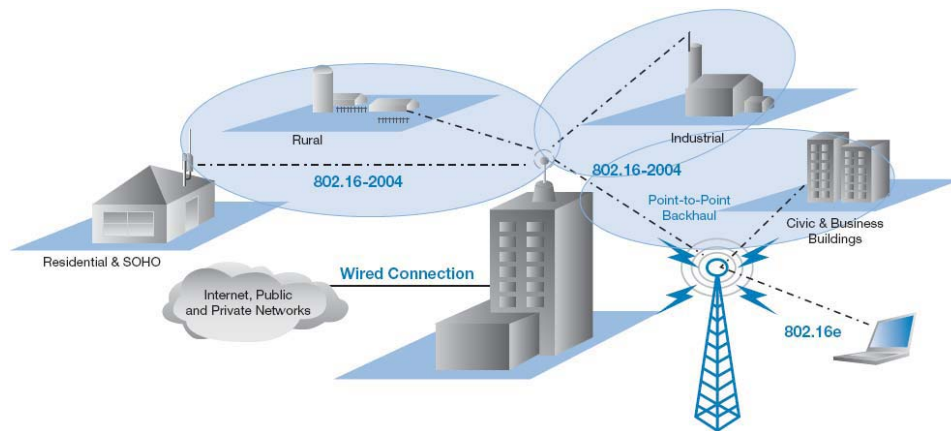


Figura 4 Tecnología Wimax Toma de *Estudio de Redes Inalámbricas Basadas en Tecnología Wimax* *Estudio de Redes Inalámbricas Basadas en Tecnología Wimax* pág.27

Un sistema WiMax tiene dos partes:

- Por un lado las torres WiMax, cuya cobertura alcanza hasta 8.000 km cuadrados según el tipo de señal transmitida.
- Por otro están los receptores, es decir, las tarjetas que se conectan a los PCs, portátiles, PDAs y demás dispositivos, para tener acceso.

Además, existen dos formas de ofrecer señal:

- Cuando hay objetos que se interponen entre la antena y el receptor: Para esto se trabaja con bajas frecuencias (entre los 2 y los 11 Ghz) con lo que se busca no sufrir interferencias por la presencia de objetos, en consecuencia el ancho de banda disponible es menor. Para ofrecer este servicio las antenas tendrán una cobertura de 65 km cuadrados (más o menos como las de los teléfonos móviles).
- Cuando no hay nada que se interponga y hay contacto visual directo: En este caso, por el contrario, se trabaja a muy altas frecuencias del orden de 66 Ghz, disponiendo entonces de mayor ancho de banda. Además, las antenas que ofrezcan este servicio tendrán una cobertura de hasta 9.300 km cuadrados.

Servicios de Wimax:

- Acceso a Internet de Alta Velocidad.
- Permite la transmisión de Voz (VoIP).
- Transmisión de Datos (VPN IP, Línea Dedicada).
- Brinda conectividad a Internet para redes Wifi/GSM/GPRS/ UMTS

Prestaciones de Wimax:

- Posee gran ancho de banda, alcanza velocidades de hasta 70 Mbps por usuario y hasta 420 Mbps por estación base.
- Es de rápido despliegue logrando hasta 50 km de cobertura.
- Es de fácil instalación ya que esta puede tomarse sólo en un plazo de 2 horas.
- Permite garantizar calidades de servicio en frecuencias de uso exclusivo (carrier class).
- Muy eficiente en el uso del espectro y la estabilidad.
- Permite transmisión simultánea de voz, datos y video.
- Soporta diferentes niveles de servicio para usuarios particulares y empresas.
- Tiene la posibilidad de aumentar el ancho de banda o las prestaciones de acuerdo con el aumento de las necesidades de los usuarios.
- Posee precios de servicios similares a los de ADSL/cable pero con mejores prestaciones que este, ya que tiene mayor ancho de banda, calidad de servicio y al mismo tiempo garantiza la velocidad, ejerce control remoto para la solución de incidencias.

Principales Características de WIMAX⁹:

Como hemos visto hasta el momento la tecnología Wimax ofrece muchos beneficios a sus usuarios, en comparación a las tradicionales redes cableadas, así como bajo costo a la hora de implementar esta solución. Además de esto posee características como la gran tasa de transferencia, escalabilidad, QoS y gran cobertura, que lo reafirman como el estándar con mayor proyección a futuro.

- Tasa de Transferencia:

El estándar IEEE 802.16 para redes Wimax, entrega una alta tasa de transferencia, con un alto nivel de eficiencia espectral debido al esquema de modulación que plantea que lo hace también tolerante a reflexiones de señal.

La modulación dinámica le permite a la estación base negociar la tasa de transferencia por rangos, lo cual lo hace más adaptativo a los requerimientos del medio, pasando incluso de un esquema de modulación de 64 QAM (Modulación por Amplitud en Cuadratura), a un orden de modulación de 16 QAM o QPSK, la cual reduce la tasa de transferencia e incrementa el rango efectivo.

- Escalabilidad:

El estándar 802.16 soporta canales de ancho de banda flexibles, es decir, que si un operador tiene asignado 20 MHz de espectro, este operador puede dividirlo en 2 sectores de 10 MHz cada uno, o 4 sectores de 5 MHz cada uno. Haciendo que el operador pueda incrementar el número de usuarios manteniendo un buen rango y tasa de transferencia.

⁹ PEREZ BECERRA, Giancarlo; FAJARDO SUÁREZ, Kenny. Tesis: *Estudio de Redes Inalámbricas Basadas en Tecnología Wimax*. Universidad Tecnológica de Bolívar.

Para escalar aun más la cobertura, el operador puede usar nuevamente el mismo espectro en dos o más sectores creando aislaciones propias entre las antenas de estaciones base.

- QoS:

Una de las características de esta tecnología es la capacidad de transmitir voz, video y datos en simultáneo, siendo estos tópicos extremadamente importantes, especialmente en mercados internacionales no cubiertos por servicio. Por esta razón el estándar IEEE 802.16a incluye características de calidad de servicio que permiten la prestación de estos servicios, los cuales requieren una red de baja latencia. Estas características de 'garantía' requeridas por el controlador de acceso al medio (MAC) del IEEE 802.16, le permiten al operador ejercer mejor control sobre sus enlaces y brindar simultáneamente niveles de servicio Premium garantizados para negocios, tanto como niveles de servicio T1, al mismo tiempo que servicios de alto volumen a hogares, similares a niveles de servicio de cable, todos estos dentro de la misma área de servicio perteneciente a una estación base.

- Cobertura:

Además de poseer un esquema de modulación robusto y dinámico, el estándar IEEE 802.16 también soporta tecnologías como la de malla o MESH que incrementan la cobertura.

Mientras la tecnología de radio mejora y los costos bajan, la habilidad de incrementar la cobertura y la tasa de transferencia usando múltiples antenas para crear 'diversidad en transmisión y/o recepción' aumentará sensiblemente la cobertura en escenarios extremos.

- Tecnología WIFI:

WiFi (Wireless Fidelity) o fidelidad sin cables, viene de HiFi, nombre utilizado para el sonido de alta fidelidad; es una tecnología que permite conectar computadoras y otros aparatos sin cables, utilizando ondas de radio.

Existen muchas personas cuyo trabajo, o incluso placer, les exige diariamente desplazarse de un lugar a otro y requieren de acceso continuo a Internet en forma simple y desde cualquier ubicación, mediante equipos portátiles en oficinas y bodegas, para lo cual necesitan no solo portabilidad sino movilidad, surgiendo así las redes inalámbricas como una imperiosa necesidad. Para lograr movilidad las computadoras portátiles requieren señales de radio para comunicarse, y así ya no es necesario estar atado a un alambre para conectarse. Lo que también ha llevado a que en muchas ciudades del mundo hoy sea posible conectarse a Internet en cualquier esquina.

Muchos lugares públicos como aeropuertos, cafeterías y universidades tienen acceso a esta conexión, siendo en estos últimos tiempos más evidente su aplicación en las cadenas hoteleras que le ofrecen este servicio a sus clientes, garantizando así el auge de esta tecnología¹⁰.

En fin, las redes Wi-Fi son un Conjunto de equipos interconectados a través de un “bridge” inalámbrico o Punto de Acceso. Para la implementación de estas redes se debe contar con tres dispositivos esenciales, la tarjeta de red, el punto de acceso (AP) y la antena, como se muestran en la Figura 5.

¹⁰CABAÑAS H., Adriana, *Tecnología Wifi en todos lados*, MICROASIST: Soluciones Humanas a problemas técnicos <http://microasist.com.mx/noticias/internet/achin201205.shtml>

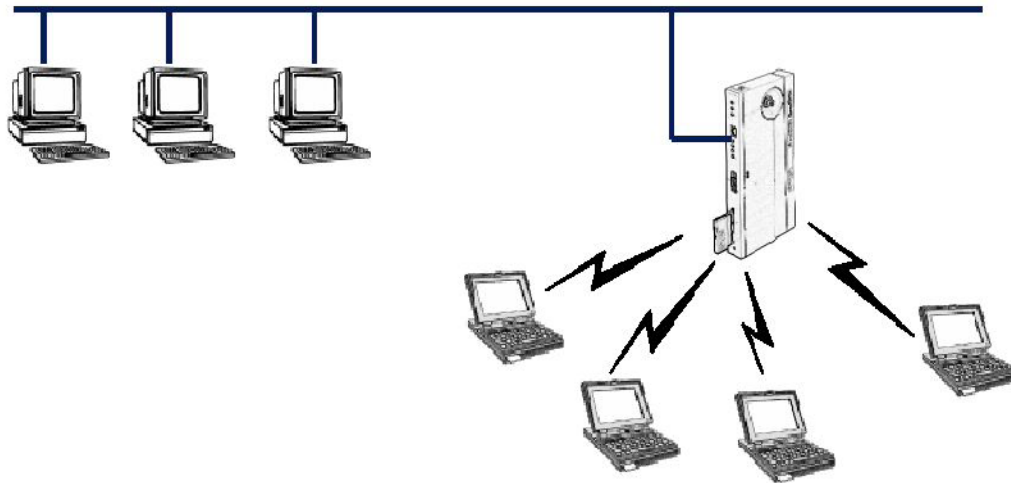


Figura 5 Tecnología Wifi Tomada de Seguridad En Redes Inalámbricas de Pablo Garaizar Sagarminaga pág. 3

Existen dos topologías utilizadas para implementar las redes WIFI. Una es conocida como ad-hoc o Independent Basic Service Set (ver figura 6) o el Extended Service Set (ver figura 7). En la primera de estas topologías pueden existir dos o varios nodos quienes por sí mismos establecen la comunicación a través de una arquitectura peer-to-peer siempre y cuando estos se encuentren dentro del área de cobertura de la red WIFI.

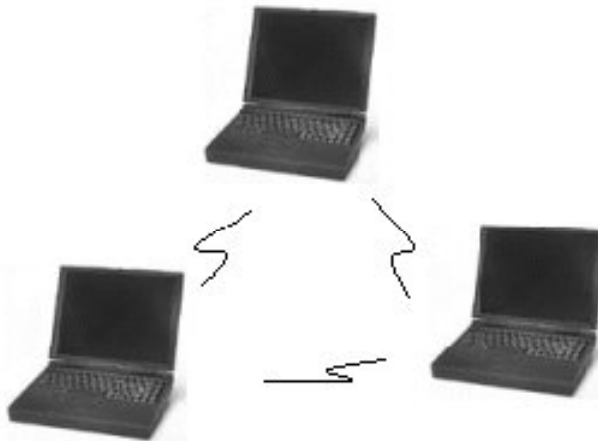


Figura 6 Estilo Ac-Hoc Tomada de Modelo de Cobertura de Redes Inalámbricas pág.18

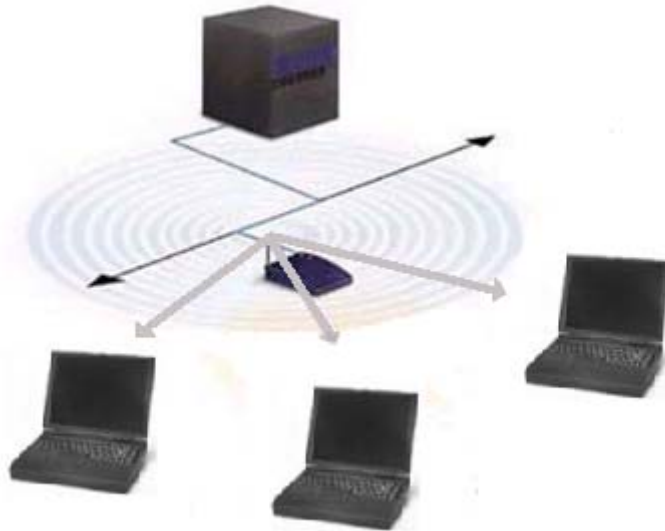


Figura 7 Extended Service Set tomada de Redes Inalámbricas 802.11 Enrique de Miguel Ponce, Enrique Molina Tortosa, Vicente Mompó Maicas

El segundo caso, consiste en más de dos BSS (Basic Service Set), los cuales están conectados a un tipo de servicio distribuido, como lo es el Ethernet; es decir que esta topología tiene una conexión a la red cableada que sirve como puente entre la cableada y la inalámbrica. Estos BSS pueden traspasarse entre ellos y así de esa manera un nodo móvil puede moverse de un lado a otro sin problema.

- Tecnología Bluetooth¹¹:

La tecnología Bluetooth es el resultado de la unión de esfuerzos y logros de nueve compañías líderes en la industria de telecomunicaciones e informática (3com, Ericsson, Intel, IBM, Lucent, Microsoft, Motorola, Nokia y Toshiba).

¹¹ LEDESMA Karen, CASTELLAR Israel. Diseño de una PAN Basada en Tecnología Bluetooth. Universidad Tecnológica de Bolívar. Monografía Minor de Comunicaciones y Redes. Facultad de Ingeniería de Sistemas.

Esta tecnología es utilizada para la conectividad inalámbrica de corto alcance entre dispositivos como PDA's (Personal Digital Assistance), teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, módems, proyectores, impresoras, etc. El principal mercado es la transferencia de datos y voz entre dispositivos y computadoras personales.

El enfoque de Bluetooth es similar a la tecnología de infrarrojo conocida como IrDAs (Infrared Data Association), sin embargo Bluetooth, es una tecnología de radiofrecuencia (RF) que utiliza la banda de espectro disperso de 2.4 GHz, pero que en muchas ocasiones se confunde con el estándar IEEE 802.11, otra tecnología de RF de corto alcance.

Las aplicaciones de esta tecnología, se ven más fundamentadas en redes residenciales o en pequeñas oficinas, ambientes que son conocidos como WPANs (Wireless Personal Area Network), siendo más estéticos ya que evitan el problema de alambrar las paredes de las casas u oficinas.

En el año 2002 la IEEE aprobó el estándar IEEE 802.15.1 compatible totalmente con la tecnología Bluetooth v1.1; en el que se definen las especificaciones de la capa física y MAC (medium access control) para este tipo de redes.

Este estándar permite mayor validez y soporte en el mercado de las especificaciones de Bluetooth, siendo de gran ayuda para los fabricantes de dispositivos basados en esta tecnología. Anteriormente a la estandarización, existían problemas de compatibilidad entre los dispositivos Bluetooth y los basados en IEEE 802.11b, quienes no podían coexistir generando interferencias entre sí.

El estándar Bluetooth define dos rangos de cobertura, uno es el rango corto que abarca distancias de hasta 10m, mientras que el rango medio cubre distancias de unos 100 metros. Este radio enlace es capaz de proveer

transmisión de voz y datos a velocidades de hasta 720 Kbps por cada canal, el cual agrupa de 2 a 8 dispositivos Bluetooth en topología de estrella.

Este radioenlace no requiere licencia para operar sobre una banda, la cual se denomina banda ISM (Industrial, scientific and medical). El ancho de banda del enlace se encuentra entre 2.4GHz y 2.48GHz; a su vez que utiliza un sistema de ensanchamiento del espectro (spread spectrum) con saltos de frecuencia del orden de 1600 saltos por segundo (FHSS), y una serial full duplex. Una misma señal fluctúa entre 79 frecuencias con intervalos de 1 MHz entre ellas, lo que hace que el rechazo a las interferencias sea alto.

En la versión de este estándar, de cobertura corta (10m), la potencia de la señal de radiofrecuencia de salida es de 0dBm, es decir, de 1 mW; mientras que para la especificación que ofrece coberturas de 100m se tiene que la potencia de salida deberá ser mayor, lográndose una potencia de hasta 20dBm (100mW), sin embargo, el radioenlace es capaz de operar con potencias de salida de hasta 20dBm. La especificación de este enlace radio, integra lo referente a radiofrecuencia en un circuito integrado que está basado en tecnología CMOS, y que posee ventajas como reducción de costos, bajo consumo, tamaño del chip reducido y demás características ideales para dispositivos móviles.

Para el tipo de transmisión que se puede llevar a cabo con esta tecnología, diferenciando entre transmisión de voz y transmisión de datos, se tiene en cuenta las siguientes características para cada uno:

- **Voz:** Bluetooth brinda la posibilidad de usar tres canales simultáneos síncronos de voz, u optar por la posibilidad de compartir un solo canal para el transporte simultáneo de datos asíncronos y voz síncrona. Cada

- **Datos:** El canal de transporte de datos asíncronos es capaz de soportar tasas de hasta 723.2Kbps en modo asimétrico (manteniendo una tasa de 57.6Kbps en la dirección de retorno), mientras que en transmisión simétrica otorga tasas de transmisión de hasta 433.9 Kbps.

Capas de la Arquitectura Bluetooth:

La Figura 8 muestra un esquema de los protocolos utilizados para la tecnología Bluetooth los cuales son empleados en la comunicación de voz y datos.

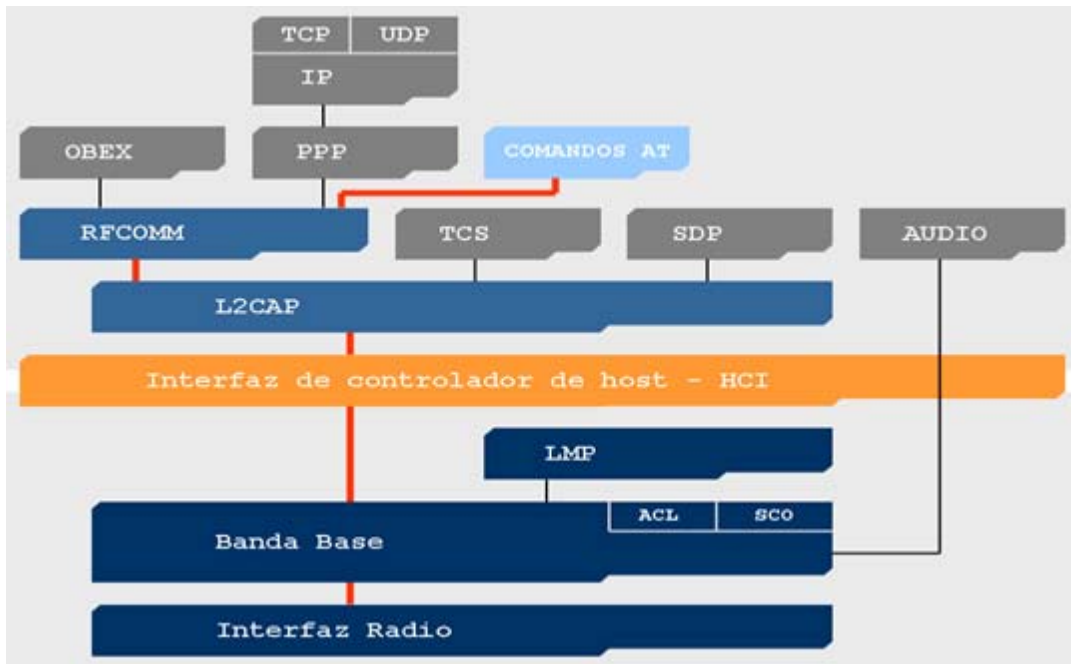


Figura 8 Capas de la Arquitectura bluetooth Tomada de de <http://gospel.endorasoft.es>

La figura 9, muestra en resumen las tecnologías inalámbricas y según la cobertura que ofrecen y los distintos estándares que la IEEE impone para estas:

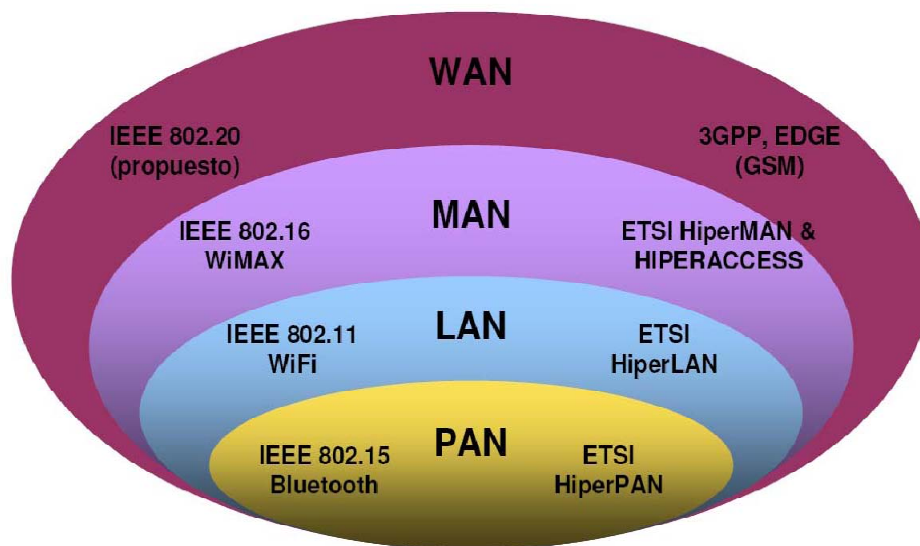


Figura 9 Cobertura de las Tecnologías Inalámbricas Tomada de ESTUDIO DE REDES INALAMBRICAS BASADAS EN TECNOLOGIA WIMAX pág.26

1.4 Redes Sensoriales:

Las redes inalámbricas de sensores (WSN, abreviado), por su naturaleza de red inalámbrica, tiene como metodología de trabajo la implementada por las redes Ad-Hoc, en la cual cada nodo es independiente y autónomo, a diferencia que en este caso las terminales son “sensores inteligentes”, representados en dispositivos pequeños (aproximadamente del tamaño de una moneda) equipados con funcionalidades avanzadas de percepción (térmico, presión, acústica y otros), un pequeño procesador y un transmisor inalámbrico de corto rango. En este tipo de redes, los sensores constantemente intercambian información entre ellos para

construir una vista global de la región monitoreada, a la cual tiene acceso un usuario externo a través de uno o más nodos de Gateway¹².

La construcción de estos nodos sensores ha sido posible debido a los avances en el área de sistemas micro electromecánicos (MEMS); estos MEMS son dispositivos miniatura fabricados sobre un substrato de silicón de la misma manera que los circuitos integrados y combinan circuitería electrónica (sensores) con actuadores mecánicos y capacidad sensitiva, de comunicación y procesamiento, constituyéndose así de tres subsistemas que tienen como función medir parámetros del medio ambiente, procesar la información recaudada por el sensor, y por último del intercambio de mensajes con los nodos sensores vecinos, función que es cumplida por el subsistema de comunicación.¹³

1.4.1 Características de las redes sensoriales:

- Movilidad de los nodos: Como toda red inalámbrica la movilidad representa una de sus características, pero cabe resaltar que no es mandato que se deba cumplir, ya que en algunos casos no lo requiere.
- Tamaño de la red: Estas redes pueden contar con un número de sensores en la red, mucho más grande que una típica red inalámbrica Ad Hoc.
- Densidad de la red: Varía de acuerdo al tipo de aplicación, ya que existen casos como el de la milicia, en donde se requiere que la red siempre esté disponible y con alto grado de seguridad y redundancia de información, debido a lo susceptible de la información.

¹² SANTI, Paolo, *Topología y Control en Redes Inalámbricas y Redes de Sensores*

¹³TAPIA ZURITA, José Luis; Tesis: *Redes Inalámbricas de Sensores Ad Hoc*
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/tapia_z_jl/capitulo2.pdf

- **Limitación de Energía:** Las redes de sensores, funcionan en ambientes agresivos en cuanto a condiciones ambientales y requieren de la mínima supervisión humana posible, por lo tanto emplean una única fuente de alimentación que es la batería, la cual limita la vida útil de la red, exigiendo la aplicación de un conjunto de protocolos de red muy eficientes a nivel de capa de red, capa de enlace de datos y hasta física para brindar un control óptimo de energía. Existen diferentes tipos de fuentes de alimentación en las redes de sensores las cuales se pueden clasificar en recargables, no recargables y regenerativas (capacidad de regenerar energía a partir del parámetro físico de estudio).
- **Fusión de los datos e información:** Debido a características como el reducido ancho de banda y la limitación de energía, estas redes demandan un aumento de bits y de información en los nodos intermedios, logrando que para la fusión de los datos, se necesita el aumento de múltiples paquetes dentro de uno solo antes de su transmisión, lo que se busca es reducir el ancho de banda a utilizar mediante encabezados redundantes en los paquetes y minimizando el retardo al acceder al medio para transmitir los múltiples paquetes, la fusión de la información busca retransmitir la salida del procesamiento del sensor a un nodo de monitoreo.
- **Distribución del Tráfico:** El tráfico varía con base al tipo de aplicación de la red que se implemente; por ejemplo, la percepción de un factor ambiental genera de manera periódica pequeños paquetes con datos que indica el estado del parámetro de estudio a una estación central de monitoreo, demandando un bajo ancho de banda, sin embargo, cuando la aplicación es de tipo rigurosa como por ejemplo, que se trate de detectar a un intruso, hablando en términos del ámbito militar, se genera un tráfico de detección de eventos con limitantes en la transmisión en tiempo real.

1.4.2 Especificaciones del dispositivo:

Un nodo de sensores, implementados en redes sensoriales, es un elemento computacional con capacidad de procesamiento, memoria, interface de comunicación y puede formar conjuntos de sensores.

El hardware básico de un nodo sensor se compone de un transceptor (transmisor/receptor), procesador, uno o más sensores, memoria y batería, los componentes brindan la opción de comunicación (enviar/recibir información), ejecutar tareas que requieren procesamiento más allá de efectuar funciones de percepción. Para ver un esquema de la arquitectura de un sensor, ver figura 10.

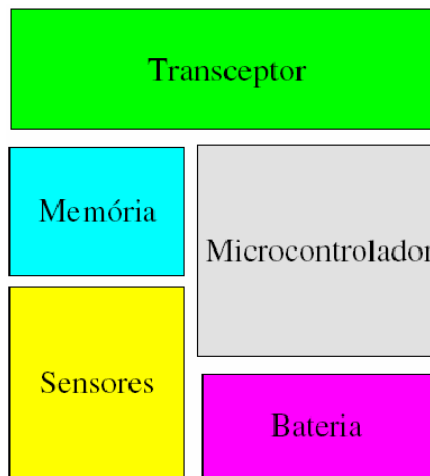


Figura 10 Arquitectura de los sensores Tomada de Redes Inalámbricas de Sensores Ad-Hoc pág. 6

La capacidad de procesamiento de los sensores, depende del tipo de microprocesador que se emplee, así mismo poseen una memoria interna en el microcontrolador, la comunicación se realiza mediante un transceptor (transmisor/receptor), además, se tiene la fuente de alimentación que varía dependiendo el tipo de tecnología con la cual la batería esté fabricada, en

cuanto al sensor, éste es el responsable de monitorear el parámetro de interés e informar del mismo.

Existen diferentes tipos de sensores con los cuales pueden ser equipados los nodos, estos van desde los acústicos, sísmicos, infrarrojos, hasta los de video cámaras, mecánicos, de calor, temperatura, radiación, entre otros, entre estos tenemos los micrófonos, fotómetros, diodos detector de luz, acelerómetro, un sensor de humedad, de radiación, de luz ultravioleta y un sensor de fuerza motriz. Por otra parte se puede resaltar el hecho de que estos nodos sensores tienen grandes restricciones en cuanto a la capacidad de memoria, de procesamiento y principalmente de energía, por lo cual en cuanto al hardware, se emplean microprocesadores de consumo mínimo de energía.

2 PROTOCOLOS UTILIZADOS

2.1 Protocolos usados en las Redes Ad-Hoc:

2.1.1 Capa Física y de Enlace de Datos:

La capa física y la de enlace para una red Ad Hoc, está determinada en el estándar IEEE 802.11, donde se describen las técnicas de modulación y codificación, y las velocidades de transmisión de 1 y 2 Mbps para las tecnologías inalámbricas, cuya frecuencia de operación según el estándar es de 2.4 GHz.

A medida que pasaba el tiempo o se hacía necesario mayor velocidad en este tipo de redes, la IEEE publicó el estándar 802.11b, con el que se ampliaba a 11 Mbps la tasa de transmisión, logrando que las WLAN ofrecieran a los usuarios las mismas prestaciones que una red cableada Ethernet común de esa época.

Junto a la aprobación de esta variante del estándar, también se publicó el 802.11a que ofrece una velocidad de transmisión de datos que oscila entre 6 y 54 Mbps, pero que al utilizar una banda de frecuencia de 5 GHz, distinta de los 2.4 del 802.11a, es incompatible con la tecnología Wi-Fi. Debido a esto se publicó el estándar 802.11g, aprobado en Junio de 2002, el cual desde su lanzamiento fue considerado como la continuación del anterior 802.11b, ya que trabaja en la frecuencia de 2.4 GHz, pero alcanza velocidades de hasta 54 Mbps.

El estándar 802.11 original, sin embargo, define la arquitectura básica, características y servicios de 802.11b cuyas especificaciones afectan solo a la capa física, generando un aumento en la velocidad de transmisión y proporcionado mecanismos para hacer la conexión más robusta. A éste estándar se le han realizado entre otras las siguientes modificaciones¹⁴:

¹⁴ GARCÍA FERNÁNDEZ, Nestor. Tesis: *Modelo de cobertura de Redes Inalámbricas basado en Radiosidad por Refinamiento Progresivo*. Universidad de Oviedo, pág. 23, marzo de 2006

- 802.11a: Hasta 54 Mbps en la banda de 5 GHz.
- 802.11b: Hasta 11 Mbps en la banda de 2.4 GHz (Wi-Fib).
- 802.11g: Hasta 54 Mbps en la banda de 2.4 GHz.
- 802.11d: Control de acceso al medio (MAC).
- 802.11e: Para poder definir QoS (calidad de servicio).
- 802.11f: Protocolo entre Access Point (IAPP).
- 802.11h: Selección automática de frecuencias y control de potencia.
- 802.11i: Incremento de niveles de seguridad en las comunicaciones.
- 802.11n: Velocidad mejorada hasta 100-500 Mbps.

El 802.11 define los dos tipos de configuración para las terminales, determinados como “configuración en modo independiente” y “configuración en modo infraestructura”. El primero de estos es el mismo denominado peer-to-peer, del que se ha venido comentando a lo largo de este texto cuando hablamos de redes basadas en Ad Hoc, y el segundo es el denominado punto de acceso (AP).

2.1.1.1 Arquitectura del Estándar 802.11:

El esquema de este estándar está basado en arquitectura celular, el cual divide el sistema en celdas. Cada una de estas celdas se denomina BSS (Basic Service Set) y es controlada por una estación base o AP (Access Point). La estructura de interconexión de las instalaciones está compuesta por un conjunto de celdas que forman una red con los APs conectados a un backbone; a ese conjunto de celdas se le denomina DS (Distribution System). El backbone al cual está conectado el DS puede ser una LAN cableada o incluso una WLAN. El conjunto completo de estos elementos forma una red única 802.11 para los niveles superiores del modelo de referencia OSI, al cual se denomina ESS (Extended Service Set) y está representado en la Figura 11.

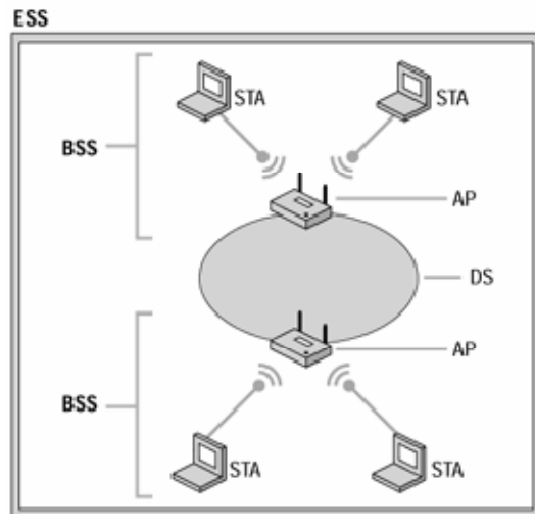


Figura 11 Arquitectura del Estándar 802.11 Tomada de Modelo de cobertura de redes inalámbricas pág.24

2.1.2 Protocolos de Enrutamiento¹⁵:

Las redes inalámbricas basadas en topología Ad Hoc, poseen técnicas para enrutar paquetes de datos que no pueden ser utilizadas en las redes clásicas cableadas. Los protocolos que por lo general son útiles en este tipo de enrutamiento, suponen una topología de red poco cambiante por lo que están basados en complicados algoritmos para determinar la mejor ruta hacia cualquier destino. Esta es la principal razón por la cual es inviable la utilización de estos mismos algoritmos o protocolos en las redes Ad-hoc, debido a que estas últimas requieren gran movilidad de los nodos. Por otro lado, el ancho de banda y la memoria son reducidos y se saturaría muy pronto la red debido al denso tráfico de control desplegado en este tipo de protocolos y al rápido crecimiento de las tablas de enrutamiento. Por este motivo se han creado distintas técnicas con las que conseguir enrutar de manera efectiva, las cuales se traducen en protocolos de

¹⁵ CORTES GRAJALES, Miguel Ángel; ALVIS LARA, Maryori Tatiana. Tesis: *Redes Móviles Inalámbricas Ad Hoc*. Universidad Tecnológica de Bolívar, 2004

enrutamiento que se pueden clasificar en tres grupos presentados a manera general en la siguiente tabla:

Basados en tablas de enrutamiento (Proactivo)	Basados en enrutamiento bajo demanda (Reactivo)	Hibrido
<i>Destination Sequenced Distance Vector (DSDV)</i> <i>Wireless Routing Protocol (WRP)</i> <i>Cluster Switch Gateway Routing (CSGR)</i>	<i>Signal Stability Routing (SSR)</i> <i>Dynamic Source Routing (DSR)</i> <i>Temporary Ordered Routing Algorithm (TORA)</i> <i>Ad Hoc on Demand Distance Vector Routing (AODV)</i> <i>Associativity Based Routing Protocol (ABR)</i>	<i>Zone Routing Protocol (ZRP)</i>

Tabla 1 Protocolos de Enrutamiento en Redes Ac-Hoc. Tomado de Monografía: Redes Móviles Inalámbricas Ad Hoc. Universidad Tecnológica de Bolívar pág. 50

2.1.1 Basados en Tablas de Enrutamiento:

Tienen como principales características:

- Tratar de mantener actualizada la información necesaria para el enrutamiento.
- Mantener rutas viables cada par de host, lo cual genera un mayor ancho de banda.
- Es posible que se presenten pequeños retardos al momento de determinar una ruta.
- Mantiene rutas que pueden no ser utilizadas.
- Cada nodo es responsable del enrutamiento, por lo tanto es tarea de cada uno mantener una o más tablas con los datos para enrutar hacia cualquier nodo de la red.

- Al poseer un topología dinámica es necesario el envío masivo de paquetes, para identificar los nodos pertenecientes a la red y en fin mantener las tablas actualizadas.

Dentro de esta clasificación podemos encontrar los protocolos:

- Destination Sequenced Distance Vector (DSDV):

Este protocolo se basa en tablas de enrutamiento, las cuales contienen las rutas destino posibles, el número de saltos que debería dar un paquete al viajar hacia un destino específico, un número de secuencia asociado al destino y el número del mensaje. Es aceptable en escenarios en los que todos los nodos intervienen en las comunicaciones y en los que la movilidad es media.

- Clusterhead Gateway Switch Routing (CGSR):

Este protocolo posee un tipo de direccionamiento y emplea un esquema para la organización de la red, que lo hace diferente a todos los otros protocolos; además, agrupa nodos móviles en los clústers, y a su vez cada clúster posee una cabecera. Esta cabecera puede controlar un grupo de hosts y realizar clustering proporcionando framework para la separación de la red (entre clústers), canal de acceso, enrutamiento, y también la asignación del ancho de banda. Por otro lado, es necesario que cada nodo contenga su propia tabla de clúster y de enrutamiento, y hace uso del DSDV como algoritmo para determinar la asignación de rutas subyacentes. Este mecanismo también posee desventajas, dentro de la que se vislumbra como principal, el hecho de que al utilizar este esquema es frecuente que los cambios de la cabecera puedan afectar el desempeño de los protocolos de enrutamiento, generando

inconvenientes como encontrar los nodos que estén ocupados en la selección de cabecera de clúster, en lugar del paquete transmitido.

- Wireless Routing Protocol (WRP)

Este protocolo está basado en tablas y tiene como función principal mantener la información actualizada sobre todos los nodos que conforman la red, para este fin cada uno de estos nodos debe implementar cuatro tablas, la tabla de distancias, de enrutamiento, tabla de coste de la ruta, y por ultimo la tabla con la lista de mensajes transmitidos (MRL).

Esta lista de mensajes transmitidos o MRL se utiliza para gestionar el envío de los paquetes de actualización de rutas, cada una de las entradas contienen el número de secuencia que identifica el paquete de actualización de rutas, un contador de retransmisiones, un vector de asentimientos con una entrada por vecino y una lista de las unidades enviadas en el paquete de actualización, además almacena que unidades deben ser retransmitidas y qué vecinos deben asentir todavía los envíos, lo cual facilita la labor de gestión y administración de la red por completo; además los nodos envían estos mensajes automáticamente, cuando son actualizados por medio de alguno de sus vecinos o cuando el mismo nodo detecta un cambio en los enlaces con sus vecinos activos.

2.1.2 Basados en Enrutamiento Bajo Demanda:

Reciben su nombre de la estructura o mecanismo de trabajo empleado, ya que las rutas son creadas al momento que se requiere, es decir “Bajo demanda”, por lo cual también reciben el nombre de reactivos.

En el momento que una terminal necesita determinar la ruta hacia un destino es necesario poner en funcionamiento un proceso de descubrimiento de ruta. Este termina cuando se ha encontrado un camino hacia el destino o cuando por el contrario, se han inspeccionado todas las posibles rutas y ninguna lleva al destino final. Cuando se descubre la mejor ruta hacia el destino, es necesario mantenerla (mantenimiento de ruta) hasta que este se vuelva inalcanzable o la ruta deje de ser necesaria. Algunos ejemplos de estos protocolos son:

- Ad hoc On-Demand Distance Vector Routing (AODV)

Este protocolo nace como evolución del anteriormente mencionado DSDV, pero en este se busca mantener números de secuencia y tablas de enrutamiento y añadir el concepto de enrutamiento bajo demanda, ya que como se explicó en el concepto, solo necesitan guardar información de los nodos que intervienen en la transmisión de datos. En comparación con su anterior diseño se consiguió un decremento del tiempo de proceso, disminución del gasto de memoria y reducción del tráfico de control por la red; además este protocolo es muy cuidadoso con las rutas, manteniéndolas en caché mientras son necesarias y deshabilitándolas cuando su información no es útil.

- Dynamic Source Routing (DSR)

Este protocolo está basado en el concepto de enrutamiento en origen, en el cual los nodos mantienen cachés, cuyas entradas contienen el destino y la lista de nodos para llegar a él. Cabe resaltar que las actualizaciones se dan a medida que se aprenden rutas nuevas y consta de dos mecanismos principales que son el descubrimiento y el mantenimiento de ruta.

- Temporary Ordered Routing Algorithm (TORA)

Este protocolo es de tipo Link Reversal Routing, y tiene como objetivo mantener un grafo dirigido que no contenga ciclos para llegar a un destino. Esto con miras a minimizar la carga sobre la red, pero con la imposibilidad de tener que estimar constantemente la distancia hacia el destino o mantener siempre la ruta más corta; sin embargo, posee la ventaja de que es un protocolo eficiente ya que no satura excesivamente de tráfico la red.

- Associative-Based Routing (ABR)

Este protocolo, por su parte está libre de desventajas como lazos, bloqueo, y duplicación de paquetes; además define un enrutamiento métrico para las redes móviles Ad hoc conocido como estabilidad de asociación, es decir, que una ruta se selecciona basándose en el grado de estabilidad de la asociación de nodos móviles, y periódicamente cada nodo genera una señal para que sus vecinos sepan de su existencia, cuando la señal es recibida por estos vecinos, se da entonces la actualización de tablas de asociación. Para cada señal recibida, se incrementa la asociabilidad del nodo actual. Por otro lado, un alto grado de estabilidad de asociación indica un estado bajo de movilidad del nodo es decir que este se mueve muy poco en la red, mientras que por el contrario, un grado bajo puede indicar un estado alto de movilidad del nodo, es decir que el nodo puede estar sufriendo constantes movimientos. Un objetivo fundamental del protocolo ABR es deducir largas rutas para las redes móviles Ad hoc, e implementa tres fases que agilizan este trabajo: el descubrimiento de ruta, la re-construcción de ruta (RRC), y la supresión de ruta.

- Signal Stability Routing (SSR)

Este protocolo es descendiente de ABR y SSR, por lo que implementa funcionalidades de estos al momento de seleccionar las rutas basándose

en la señal más fuerte entre los nodos y en la estabilidad de la localización de los mismos, lo cual trae como consecuencia, el obtener las rutas que tengan una comunicación mejor establecida. Por otro lado SSR puede ser dividido en dos protocolos cooperativos: el de asignación de ruta dinámico (DRP) y el de asignación de ruta estático (SRP).

El DRP o protocolo de asignación de ruta dinámico, es responsable del mantenimiento de la tabla de señal estable (SST) y la tabla de enrutamiento (RT). Esta tabla (SST), registra la señal más fuerte de nodos vecinos, que son obtenidos por señales periódicas de la capa de enlace de cada uno. Todas las transmisiones se reciben por el DRP. Después de actualizar todas las entradas de las tablas, el DRP le pasa el paquete recibido al SRP. Seguindo a esto el SRP procesa los paquetes pasando primero el paquete a la pila si es el receptor indicado o buscando el destino en la tabla de enrutamiento, y por último envía el paquete si lo es. Si el protocolo no encuentra ninguna entrada para el destino en la tabla de enrutamiento, comienza entonces el proceso para descubrir la ruta.

2.1.3 Protocolos Híbridos:

Estos protocolos resultan de la combinación de los dos anteriores y tienen como características principales:

- El nodo origen es el encargado de iniciar el descubrimiento de la ruta.
- Establece las rutas bajo demanda, como ya vimos esto indica que sólo las establece cuando estas son requeridas.
- Mantenimiento de ruta restringido.
- La actualizan el estado de la red y el mantenimiento de las rutas, se hace sin tener en cuenta si existe o no trafico de datos.

- Solo cuando se necesita enviar o transmitir algún dato hacia un destino, el protocolo determina las posibles rutas hacia él.

Dentro de los protocolos que cumplen con estas características se encuentra el protocolo Zone Routing Protocol (ZRP).

Este es un protocolo híbrido, como ya se ha mencionado antes, cuya utilidad está principalmente a medio camino entre los protocolos basados en tablas y los basados en enrutamiento bajo demanda; la implementación de este es generalmente en una clase de redes Ad-Hoc llamadas RWNs (Reconfigurable Wireless Networks). Estas redes se caracterizan por tener gran cantidad de nodos, mucha movilidad y alto tráfico, los protocolos vistos anteriormente no cumplen las especificaciones para satisfacer las necesidades de las RWNs, por lo que se decidió crear un nuevo protocolo, que usa zonas similares a clusters, en las que los nodos que actúan de bordes se van seleccionando dinámicamente, además, el radio de estas zonas se reajusta aún luego de haber sido implementado según las condiciones de la red, y se pueden usar protocolos distintos para comunicarse dentro, y entre, zonas distintas.

2.2 Protocolos usados en las Redes Inalámbricas:

Las redes inalámbricas, en general (PAN, WLAN, WMAN), están determinadas según los estándares 802.15, 802.11 a/b/g y 802.16 a/b.

- Estándar **802.15** está encargado de definir las redes de área personal (WPAN), también conocidas como redes inalámbricas de corta distancia y usadas principalmente en dispositivos como PDAs, periféricos, teléfonos móviles y electrónica de consumo. El objetivo de esta normativa es publicar estándares

WPAN para el mercado doméstico y de consumo que además sean compatibles con otras soluciones inalámbricas (Bluetooth) y basadas en cable.

- **802.11:** Este estándar define y gobierna las redes de área local inalámbricas (WLAN) que operan en el espectro de los 2,4 GHz (Giga Hercios) y fue definida en 1997. El estándar original especificaba la operación a 1 y 2 Mbps usando tres tecnologías diferentes:
 1. Frequency Hopping Spread Spectrum (FHSS)
 2. Direct Sequence Spread Spectrum (DSSS)
 3. Infrarojos (IR)

El estándar creado originalmente aseguraba la interoperabilidad entre equipos de comunicación dentro de cada una de estas tecnologías inalámbricas, pero generaba conflictos cuando se buscaba interconectar dispositivos de las tres tecnologías. Desde entonces, muchos estándares han sido definidos dentro de la especificación IEEE 802.11 que permiten diferentes velocidades de operación. El estándar IEEE 802.11b permite operar hasta 11Mbps y el 802.11a, que opera a una frecuencia mucho mayor (5 GHz), permite hasta 54Mbps.¹⁶

- El estándar IEEE **802.11a** se aplica a la banda de UNII (Unlicensed National Information Infrastructure) de los 5GHz. El estándar usa el método OFDM para la transmisión de datos hasta 54Mbps. Su mayor inconveniente es la no compatibilidad con los estándares de 2,4GHz, pero su modo de operación es muy parecida al estándar 802.11g; existe también un estándar desarrollado en Europa que es muy similar al 802.11^a, el cual recibe el nombre de HiperLAN2.

¹⁶ GARAIZAR SAGARMINAGA, Pablo Estándar 802.15 802.11 www.e-ghost.deusto.es

Resumen 802.11a:

Rango de frecuencias:	De 5,15 a 5,25 GHz (50 mW) De 5,25 a 5,35 GHz (250 mW) De 5,725 a 5,825 GHz (1 W)
Acceso:	Multiplexación por División de Frecuencia Ortogonal (OFDM)
Velocidad:	Hasta 54 Mbps
Compatibilidad:	No compatible con los sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos
Aplicación:	Todo tipo de red de datos Ethernet

Tabla 2 Resumen del Estándar 802.11a. Tomado del índice de estándares de redes inalámbricas

- **802.11b:** Esta extensión del estándar 802.11, definido en 1999, permite velocidades de 5,5 y 11Mbps en el espectro de los 2,4GHz. Esta extensión es totalmente compatible con el estándar original de 1 y 2 Mbps (sólo con los sistemas DSSS, no con los FHSS o sistemas infrarrojos) pero incluye una nueva técnica de modulación llamada Complementary Code Keying (CCK), que permite el incremento de velocidad. El estándar 802.11b define una única técnica de modulación para las velocidades superiores - CCK - al contrario que el estándar original 802.11 que permitía tres técnicas diferentes (DSSS, FHSS e infrarrojos). De este modo, al existir una única técnica de modulación, cualquier equipo de cualquier fabricante podrá conectar con cualquier otro equipo si ambos cumplen con la especificación 802.11b. Esta ventaja se ve reforzada por la creación de la organización llamada WECA (Wireless Ethernet Compatibility Alliance), una organización que dispone de un laboratorio de pruebas para comprobar equipos 802.11b. Cada equipo certificado por la WECA¹⁷ recibe el logo de compatibilidad WI-FI que asegura su compatibilidad con el resto de equipos certificados.

¹⁷ GARAIZAR SAGARMINAGA, Pablo Estándar 802.11^a 802.11b www.e-ghost.deusto.es

Resumen 802.11b

Rango de frecuencias:	De 2,4 a 2,4835 GHz
Acceso:	Direct Sequence Spread Spectrum (DSSS) usando Complementary Code Keying (CCK)
Velocidad:	Hasta 11 Mbps
Compatibilidad:	Compatible con sistemas 802.11 DSSS y de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF.
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación:	Todo tipo de red de datos Ethernet

Tabla 3 resumen del Estándar 802.11b. Tomado del índice de estándares de redes inalámbricas

- **802.11b+:** Es una variación del IEEE 802.11b pero que puede operar a 22Mbps contra los 11Mbps de la versión 11b. Su mayor problema es que no es un estándar. Aunque aparece en la mayoría de las documentaciones como IEEE 802.11b+, IEEE nunca lo ha certificado como estándar. Es un sistema propietario diseñado por Texas Instruments y adoptado por algunos fabricantes de dispositivos inalámbricos como D-Link y Global Sun que utilizan estos chipsets. Técnicamente utiliza técnicas que forman parte del estándar 11g. Comparativamente con el resto de estándares no ofrece grandes diferencias, ya que aunque anuncia velocidades de 22Mbps en prestaciones reales se obtiene una discreta mejora.
- El estándar IEEE **802.11g** ofrece 54Mbps en la banda de 2,4GHz. Dicho con otras palabras, asegura la compatibilidad con los equipos Wi-Fi preexistentes. Para aquellas personas que dispongan de dispositivos inalámbricos de tipo Wi-Fi, 802.11g proporciona una forma sencilla de migración a alta velocidad, extendiendo el período de vida de los dispositivos de 11Mbps. El estándar 802.11g se publicó como borrador en Noviembre de 2001 con los siguientes elementos obligatorios y opcionales:

1. El método OFDM (Orthogonal Frequency Division Multiplexing) es obligatorio y es lo que permite velocidades superiores en la banda de los 2,4GHz.
2. Los sistemas deben ser totalmente compatibles con las tecnologías anteriores de 2,4GHz Wi-Fi (802.11b). Por lo que el uso del método CCK (Complementary Code Keying) también será obligatorio para asegurar dicha compatibilidad.
3. El borrador del estándar marca como opcional el uso del método PBCC (Packet Binary Convolution Coding) y el OFDM/CCK simultáneo.

Resumen 802.11g

Rango de frecuencias:	De 2,4 a 2,4835 GHz
Acceso:	Obligatoriamente Complementary Code Keying (CCK) y Multiplexación por División de Frecuencia Ortogonal (OFDM), opcionalmente puede incluir Packet Binary Convolution Coding (PBCC) y CCK/FDM
Velocidad:	Hasta 54 Mbps
Compatibilidad:	Compatible con sistemas 802.11b de 11Mbps y 5,5Mbps. Compatible con sistemas 802.11 DSSS y de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF.
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación:	Todo tipo de red de datos Ethernet

Tabla 4 Resumen del Estándar 802.11g. Tomado del índice de estándares de redes inalámbricas

Comparativo de estándar inalámbrico¹⁸:

	802.11b	802.11 ^a	802.11g	802.11b+
Fecha de definición	Septiembre 1999	Septiembre 1999	noviembre 2001 (Borrador)	No estándar
Velocidad Anunciada	11Mbps	54Mbps	54Mbps	22Mbps
Velocidad Media Obtenida	4-5Mbps	27 Mbps	25 Mbps	6 Mbps
Frecuencia	2,4GHz	5GHz	2,4GHz	2,4GHz
Modulación	DSSS/CCK	OFDM	DSSS/PBCC	PBCC
Canales	11	12	11	11

Tabla 5 Comparativo de Estándares Inalámbricos. Tomado del índice de estándares de redes inalámbricas

¹⁸ GARAZAR SAGARMINAGA, Pablo Estándar 802.11g www.e-ghost.deusto.es

- La misión del grupo de trabajo **802.16** es desarrollar sistemas Inalámbricos de Área Metropolitana. En Enero de 2003 ha publicado nuevos estándares. El estándar del 802.16-2004 del IEEE (el cuál revisa y reemplaza versiones del IEEE del 802.16a y 802.16d) es diseñado para el acceso fijo que el uso modela. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo de una habitación o en el mástil, parecido a un plato de la televisión del satélite. 802.16-2004 del IEEE también se ocupa de instalaciones interiores, en cuyo caso no puede ser tan robusto como al aire libre. El 802.16-2004 para el estándar es una solución inalámbrica tiene acceso a Internet de banda ancha que provee un ínter operable, solución de clase de transportador para la última milla. WiMAX pues acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento en la licencia se agrupa. Esta tecnología le provee una alternativa inalámbrica al módem cablegráfico, las líneas digitales del suscriptor de cualquier tipo. El estándar del **802.16e** del IEEE es una enmienda para la especificación de la base 802.16-2004 y le apunta al mercado móvil sumando portabilidad y la habilidad para clientes móviles con IEEE Los adaptadores del 802.16e para conectarse directamente al WiMAX enlazan en red del estándar. Se espera que el estándar 802.16e ha sido ratificado en 2005. El estándar del 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), lo cual es similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, se pasa un paso más allá para entonces agrupando subportadoras múltiples en subcanales. Una estación del cliente solo del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión, o los clientes múltiples podría transmitir con cada uno usando una porción del número total de subcanales simultáneamente. El estándar del 802.16-2004 del IEEE mejora

última entrega de milla en varios aspectos cruciales como la interferencia del multicamino, El retraso difundido, La robustez.¹⁹

2.2.1 Protocolos de Seguridad en Redes Inalámbricas²⁰:

Hasta el momento hemos venido tratando aspectos generales, de funcionamiento y estructura interna de las redes inalámbricas, dejando de lado un tema crucial y del cual depende el auge y aplicabilidad que se de a futuro a este tipo de redes.

Desde el surgimiento de las redes inalámbricas la seguridad ha sido un aspecto muy importante y a la vez evaluado, al punto que aún es normal encontrar personas que posean escepticismo hacia ellas debido a los problemas de seguridad que desde su nacimiento han presentado y que se han venido resolviendo a medida que avanza el tiempo, mediante la creación de protocolos de encriptamiento, los cuales han cobrado especial relevancia cuando hablamos de redes inalámbricas.

Las redes cableadas difieren en muchos aspectos de las redes inalámbricas, pero un aspecto fundamental es que para acceder a estas últimas sólo es necesario una tarjeta de red y estar ubicado dentro de la celda de cobertura, así por ejemplo, en una red inalámbrica desplegada al interior de una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, y sólo bastaría con que estuviese en un lugar próximo donde le llegase la señal; para el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten identificar posteriormente quien fue.

El canal de transmisión en este tipo de redes, debe considerarse inseguro siempre, ya que cualquiera que tenga acceso a la red podría estar escuchando la información transmitida, y además que se pueden dar diferentes modalidades de

¹⁹ GARAIZAR SAGARMINAGA, Pablo. *Estándar 802.16 802.16e*. <http://www.e-ghost.deusto.es>

²⁰ BARAJAS, Saulo. Tesis Doctoral: *Protocolos de Seguridad en Redes Inalámbricas*. Universidad Carlos III de Madrid. <http://www.saulo.net/pub/inv/SegWiFi-art.htm>

alteración de información o suplantación, con lo cual se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Por tal motivo, la IEEE estandarizó el protocolo WEP (Wired Equivalent Privacy, privacidad equivalente al cable), que si bien no fue la panacea al momento de su lanzamiento, si buscaba encriptar la información que viaja por la red inalámbrica, para que no sea accedida por agentes externos, además de proporcionar confidencialidad, autenticación y control de acceso en redes WLAN.

Características del WEP:

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

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

conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

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

El estándar IEEE 802.11 incluye un mecanismo de autenticación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación:

- Una estación que quiere unirse a una red, solicita al punto de acceso autenticación.
- El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve.
- El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

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

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

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

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica. Por tal motivo se creó el protocolo WPA, con el fin de mejorar los problemas de seguridad que su antecesor presentaba.

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

WPA es, un subconjunto del IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales como solución a todas las debilidades conocidas de WEP y se considera suficientemente seguro.

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

WPA incluye las siguientes tecnologías:

- IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).
- EAP, definido en la RFC 2284, es el protocolo de autenticación extensible para llevar a cabo las tareas de autenticación, autorización y contabilidad; EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).
- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas [4].

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas, requiere un servidor configurado para

desempeñar las tareas de autenticación, autorización y contabilidad.

- Con clave inicial compartida (PSK); Este modo está orientado para usuarios domésticos o pequeñas redes, no requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autenticación, pero no para el cifrado de los datos.

Con la maduración de las tecnologías inalámbricas el IEEE ya a estandarizado el WPA2 como sucesor de WPA el cual incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIST; Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits, el cual requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

2.3 Protocolos usados en las Redes Sensoriales:²¹

Unified Network Protocol Framework (UNPF):

Desarrollado en la Universidad Estatal de Washington, UNPF es un conjunto de protocolos que son parte de la arquitectura de rangos para redes de Sensores, UNPF integra tres operaciones dentro de su propia estructura como el protocolo de inicialización y mantenimiento, de control de acceso al medio y por último, aunque no menos importante, de ruteo de información.

- o Protocolo Inicialización y Mantenimiento de la Red:

Este protocolo organiza los nodos sensores dentro de diferentes rangos, mediante su capacidad de radio difusión del nodo central. El nodo central puede alcanzar a todos los nodos mediante el canal de control.

El nodo central radiodifunde su Identificación (ID) usando un método de acceso al medio que utiliza codificación de la información en un ancho de banda compartido conocido como CDMA (Code Division Multiple Access) en el canal de control común, todos los nodos escuchan el canal y guardan la identificación del nodo central, ellos a su vez mandan de vuelta sus identificaciones con niveles bajos de potencia, Con esto le dan a conocer al nodo central aquellos nodos que pueden escuchar (debido a que conocen el código para descifrar la información) se encuentran en su primer salto. Subsecuentemente, el nodo central difunde un paquete de control con las identificaciones de los nodos del primer rango y los nodos que escuchen al nodo central responden con una señal de control. Así todos los nodos del primer rango registran las identificaciones de los otros nodos, formando éstos el segundo rango. Esto continúa hasta que se ha barrido toda la red en busca

²¹ TAPIA ZURITA, José Luis. Tesis: *Tutorial de Redes de Sensores Ad Hoc con énfasis en Energía*. Capítulo 3. http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/tapia_z_jl/capitulo3.pdf

de nuevos nodos, logrando así que la estructura de rangos se forme mediante rondas sucesivas de búsqueda, y para mantener la red periódicamente se actualiza la información de los nodos y la estructura de rangos ya sea por que no tiene energía o se han cambiado del rango donde se encontraba.

- Protocolo de Control de Acceso al Medio:

Este protocolo se ejecuta de forma previa a la fase de transmisión de información por lo que el canal transmisor distribuido TDMA (DTROC) lo solicita, Cada nodo tiene asignado un canal de recepción por el nodo central, y el canal es rehusado, para evitar colisiones la transmisión de los nodos se calendariza por ranuras de tiempo para todos los nodos vecinos, esto permite que la transmisión se realice libre de colisiones y se ahorre energía cada vez que los nodos se encuentren apagados ya que no realizan ninguna operación de envío/recepción. Las dos funciones que realiza el DTROC son la asignación de canal de recepción para los nodos y la calendarización para compartir el canal de recepción entre los nodos vecinos.

- Protocolo de Ruteo:

La responsabilidad del protocolo de ruteo es el intercambio de información, encontrando el camino más confiable para alcanzar el destino deseado teniendo en consideración la distancia, el requerimiento mínimo de energía y el tiempo de vida del enlace inalámbrico, búsqueda de la información en el caso de que la conexión falle, reparación de los enlaces caídos gastando el mínimo de potencia de procesamiento y mínimo uso del ancho de banda. La arquitectura de rango permite que la información de los nodos sensores se propague de enlace en enlace al nodo central, el nodo que transmite es seleccionado conforme a su nivel de energía, con el propósito de alargar la supervivencia de la red.

Arquitectura de Conjunto:

Esta arquitectura, se emplea especialmente en las redes de Sensores dada la oportunidad de agregar información a medida que ésta pasa de nodo en nodo, cuando los nodos recopilan la información de interés, el cluster-head (jefe de conjunto) la reúne y la envía a un nodo específico, dependiendo de la necesidad de información requerida por dicho nodo. A su vez, para formar y designar a estos jefes de conjunto, la red deberá de ser autónoma y auto-organizada de manera distribuida. Para lograr esto, se emplean protocolos a nivel capa de red como el denominado LEACH (Low-Energy Adaptive Clustering Hierarchy). En general, los nodos en una red de sensores, frecuentemente necesitan organizarse dentro de conjuntos (clusters), este tipo de arquitectura se basa en la creación de conjuntos o arreglos de nodos, gobernados mediante jefes de conjuntos llamados comúnmente clusterheads, los nodos en cada conjunto, tiene la función de intercambiar mensajes con sus respectivos jefes de conjunto (siguen siendo nodos), los cuales en general son el punto de acceso para que los nodos dentro del conjunto se conecten hacia la red cableada.

- Low-Energy Adaptive Clustering Hierarchy (LEACH):

Este protocolo enfocado para la arquitectura de conjunto, busca la minimización de la energía de disipación en las redes de Sensores, LEACH selecciona nodos de manera aleatoria y escoge un jefe de conjunto, esta elección no es permanente, sino que se lleva a cabo de forma periódica una reelección para que la disipación de energía que experimenta un jefe de conjunto se distribuya a todos los nodos de la red de forma equitativa. Cada iteración en la selección de los cluster-heads se le llama ronda (round). La operación del LEACH se divide en dos fases: la de ajuste de jefe de conjunto y la de establecimiento del tiempo que va a ser jefe de conjunto un nodo dado.

- Durante la fase de ajuste, cada nodo sensor escoge un número aleatoriamente entre 0 y 1. Si este número es menor que el umbral superior del nodo n , $T(n)$, el nodo sensor se convierte en un jefe de conjunto.

- En fase de establecimiento, una vez que los nodos han decidido a que jefe de conjunto pertenecer, es indispensable que se den de alta como miembros de ese conjunto específico. Cada nodo transmite su información al jefe de conjunto mediante un protocolo de acceso múltiple al medio de control con una percepción de portadora. Durante esta fase, todos los jefes de conjunto mantienen sus receptores encendidos. Los jefes de conjunto reciben todos los mensajes con la información de los nodos que desean estar en el conjunto. En base a número de nodos en el conjunto, el jefe crea una calendarización por medio de códigos de acceso múltiple por división de tiempo (TDMA, Time Division Multiple Access) informando a cada nodo cuando puede realizar sus transmisiones (la calendarización se radiodifunde de vuelta a los nodos).

El protocolo de ruteo LEACH, se emplea en arquitecturas de conjuntos, con el propósito de minimizar el consumo global de energía, distribuyendo la carga a todos los nodos en diferentes instantes de tiempo. El protocolo es completamente distribuido y no requiere de un control de información de un nodo central. Además, no es necesario que los nodos tengan un conocimiento amplio de la arquitectura de la red para poder ejecutarlo.

No existe una solución definitiva para el enrutamiento en ambientes inalámbricos. En la actualidad las redes ad-hoc siguen bajo investigación ya que ofrecen un ambiente teórico con mucho por estudiar y por su parte las redes de sensores revisten interés dada su diversidad de aplicaciones comerciales y de seguridad, sin embargo queda mucho por desarrollar con respecto al enrutamiento para ambientes inalámbricos y también queda mucho por desarrollar sobre modelos teóricos para redes inalámbricas.

3. ACCESO Y CONTROL

3.1 Acceso y control en las Redes Inalámbricas y de Arquitectura Ad-Hoc:

El encaminamiento en un entorno cooperativo es de gran importancia debido al hecho de que es indispensable establecer rutas multisaltos con el fin de hacer posible la conectividad extremo a extremo, esto es un aspecto relevante a la hora de definir los criterios de admisión.

Por ser de un medio compartido, es de gran importancia establecer una serie de políticas que rijan de una manera eficiente y ordenada el acceso al medio.

Una decisión de encaminamiento basada en una métrica que refleje adecuadamente la disponibilidad real de los recursos brinda la oportunidad hallar la capacidad del sistema para proporcionar la QoS demandada, claro está que, esta medida depende directamente de la gestión de recursos realizada por el nivel de enlace y los protocolos de control de acceso al medio (Medium Access Control – MAC)²².

La razón de ser de los protocolos MAC en entornos inalámbricos es el de gestionar de una manera eficaz recursos disponibles, tiene como objetivo principal el de optimizar el uso del canal radio, ya que el espectro de frecuencia disponible es limitado y el número de usuarios crece diariamente al igual que también lo hacen los requerimientos de dichos usuarios.

La creciente demanda de información multimedia, la combinación de voz, datos, al igual que el envío de video y audio, exige nuevos y más estrictos requisitos en

²² GALLEGO, J.R., et al. *Control de admisión distribuido para redes móviles ad-hoc basado en un diseño cross-layer*. IEEE Latin America Transactions, vol. 5, No. 6, October 2007. Universidad Politécnica de Cataluña. Marzo, 2004.

términos de grandes anchos de banda necesarios para cada usuario y, en muchos casos, con exigencia de calidad asegurada (QoS)²³.

El estándar 802.11 utiliza como mecanismo de acceso básico el método CSMA (Carrier Sense Multiple Access) el cual funciona de la siguiente manera, cuando la estación que desea transmitir escucha el canal de transmisión, si el medio está ocupado es porque otra estación está transmitiendo y por lo tanto debe esperar para realizar la transmisión, si el medio está libre durante un tiempo específico, llamado DIFS (Distributed InterFrame Space) en el estándar, la estación está habilitada para transmitir.

Este tipo de métodos de acceso al medio, denominados como protocolos de acceso por contienda, son muy efectivos si la carga de uso del medio no es muy alta, debido a que esto le permitirá a las estaciones transmitir con un retardo mínimo, de igual forma hay que tener en cuenta que pueden producirse colisiones por la posibilidad de que 2 estaciones “escuchen” el medio simultáneamente, detectando que está libre e iniciando su transmisión al mismo tiempo.

El método de acceso más conocido en redes cableadas es el CSMA/CD, utilizado por el estándar IEEE 802.3 (Ethernet); este método no puede aplicarse a redes inalámbricas debido a dos razones:

- Para implementar un mecanismo de detección de colisiones, se necesitarían dispositivos de radio full duplex capaces de transmitir y recibir simultáneamente, lo cual incrementaría significativamente el coste de los equipos.

²³ ZÁRATE, Jesús Alonso. *Estudio y Análisis de Técnicas de Acceso y Algoritmos de Adaptación Dinámica de Topología de Redes Inalámbricas Ad Hoc Autoconfigurables*

- En una red cableada cualquier estación pueden “escuchar” al resto, mientras que en redes inalámbricas esto puede no cumplirse (nodo escondido).

El método que más se utiliza en redes inalámbricas es el CSMA/CA, este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio, en este protocolo cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, con el fin de disminuir así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI. Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares. El estándar proporciona otra opción CCA que puede comprobarse independientemente o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido).

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión.

Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC.

3.1.1 Mecanismo de Intercambio de Mensajes con Reconocimiento Positivo (Reservation-Based Protocol)²⁴:

Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS - "request to send") quien difunde el NAV (Network Allocation Vector) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan); y cuál va a ser la duración de la transmisión.

Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS - "clear to send") que permite al solicitante enviar su trama (datos). Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo.

Después de que se reciba la trama de los datos, se devuelve una trama de reconocimiento (ACK - ACKnowledged) notificando al transmisor que se ha recibido correctamente la información (sin colisiones).

²⁴ GARCÍA FERNÁNDEZ, Nestor. Tesis Doctoral: *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo*. Universidad de Oviedo, marzo de 2006

Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto.

Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

3.1.2 Protocolo CSMA/CA:

La norma IEEE 802.11 especifica que el algoritmo a utilizar en este nivel y para este tipo de tráfico es el denominado CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

En la figura 12 se ilustra el procedimiento que siguen un conjunto de estaciones que operan bajo el algoritmo de acceso CSMA/CA²⁵.

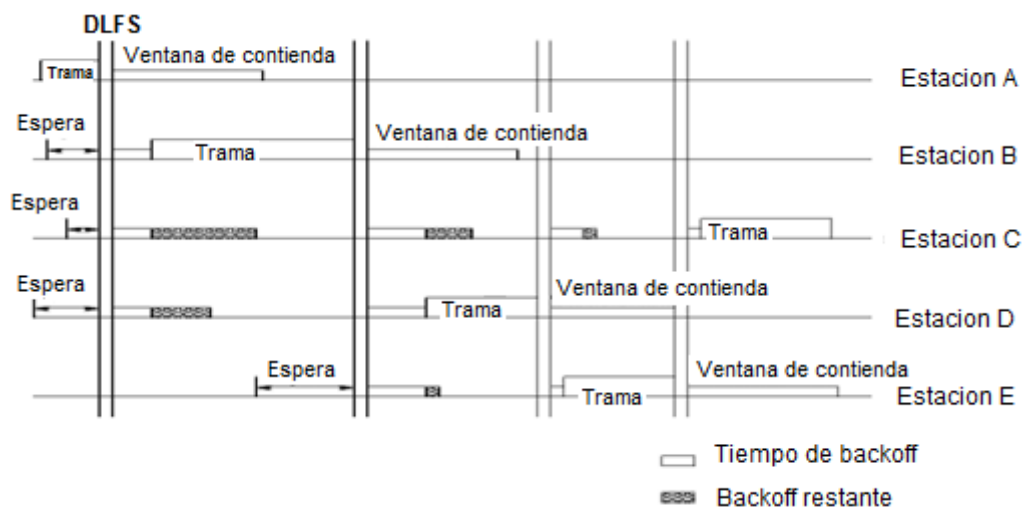


Figura 12 algoritmo de acceso CSMA/CA Tomada de WLAN Red inalámbrica de área local pág. 8

²⁵ ESCUDERO QUESADA, Ana; OLIVER RIERA, Miquel. *Estudio del rendimiento del algoritmo CSMA/CA IEEE 802.11 con diferentes niveles físicos*. Departamento de Matemática Aplicada y Telemática. <http://nmg.upc.es/intranet/qos/9/9.3/9.3.15.pdf>

Según el algoritmo de acceso CSMA/CA una estación que está preparada para transmitir un paquete de información debe testear el medio antes de hacerlo para determinar si el medio está libre, si el medio está desocupado la estación puede empezar el proceso de transmisión, por el contrario, si el medio se determina ocupado la estación espera un tiempo aleatorio, medido en slots time antes de volver a intentar transmitir, este número aleatorio es seleccionado de manera uniforme en un intervalo definido por los valores 0 y CW, donde CW es la denominada ventana de contienda, y el parámetro CW varía en función del número de intentos que contabiliza una estación para la transmisión de un paquete determinado.

3.1.3 Funcionamiento de una Red Inalámbrica:

Las dos funciones operativas más importantes que se producen en el una Red Inalámbrica, en especial las de Área Local, son el método utilizado por una estación para conectarse a una celda y el soporte de roaming entre APs.

Conexión a una celda:

Existen 3 momentos en que una estación necesitará acceder a un BSS: después del encendido, al finalizar el sleep-mode o cuando entra en el área del BSS.

La estación precisa obtener información de sincronización del AP (configuración en modo infraestructura) o de otra estación (configuración en modo independiente). La estación puede utilizar dos métodos para obtener esta información:

1. Active Scanning: En este método la estación trata de localizar el AP transmitiendo tramas de petición de sondeo, quedando a la espera de paquetes de respuesta de sondeo desde el AP.

2. **Passive Scanning:** En este método la estación se queda a la espera de recibir una trama Beacon del AP. La trama Beacon contiene la información de sincronización y proporciona a la estación la información que necesita.

El método utilizado por la estación dependerá de su consumo de energía y su propia operativa.

Proceso de autenticación y asociación:

Una vez que la estación ha localizado un AP y decide unirse a su BSS, debe iniciar un proceso de autenticación. Este proceso consiste en un intercambio de información entre el AP y la estación donde cada extremo prueba el conocimiento de una contraseña predefinida.

Realizado el proceso de autenticación, se inicia el proceso de asociación. La estación y el BSS intercambian información acerca de sus propias capacidades y el DSS toma conocimiento de la posición actual de la estación. Una estación no puede transmitir o recibir tramas de datos sin que el proceso de asociación haya concluido.

Itinerancia o Roaming:

Siempre que la red inalámbrica disponga de más de una celda es posible para los clientes inalámbricos desplazarse entre las áreas de cobertura de cada uno de ellos sin perder la conexión. Se entiende por Roaming el proceso de movimiento desde una celda o BSS a otra, sin pérdida de conexión.

El 802.11 no define explícitamente cómo debe ser implementado el roaming, pero define los métodos básicos para hacerlo posible. Esto incluye active/passive scanning y el proceso de reasociación; donde la estación que hace roaming desde un AP a otro, pasa a estar asociada al nuevo.

Para que el Roaming sea posible, todas las estaciones base deben utilizar el mismo nombre de red SSID y las mismas claves de encriptación WEP.

Sincronización

Mantener la sincronización del sistema con las estaciones es muy importante para llevar a cabo saltos sincronizados además de otras funciones como el ahorro de consumo energético. Esto se logra actualizando el reloj de las estaciones con arreglo al reloj de los APs, mediante las tramas Beacon, las cuales contienen el valor de reloj del AP en el momento de su transmisión.

Cabe resaltar que los protocolos de acceso y control que trabajan en el funcionamiento y administración de las redes inalámbricas, pueden estar implementados sobre cualquiera de las arquitecturas de estas redes, es decir, arquitectura peer-to-peer (Ad Hoc), o de infraestructura.

3.2 Acceso y Control en las Redes Sensoriales²⁶:

En comparación a las redes tradicionales cableadas, la comunicación punto a punto en enlaces de comunicación, da como resultado que al momento de enviar información las decisiones se hagan de forma local, empleando técnicas de ruteo y descubrimiento de enlaces entre el origen y los destinos.

La localización de la información de sensores, implica que cada nodo debe saber su posición geográfica y que pueda éste ser localizado en base a la información que este transmite en los mensajes. Para ello, es deseable contar con un

²⁶ UNIVERSIDAD DE CASTILLA LA MANCHA. *B-Mac y otros Protocolos de Acceso al Medio*. <https://www.dsi.uclm.es/descargas/thechnicalreports/DIAB-06-09-2/TRBMAC.pdf>

mecanismo de bajo costo, mínimo consumo de potencia y que brinde confiabilidad para el descubrimiento de nodos dentro de una red²⁷.

La subcapa MAC la cual pertenece a la capa de enlace de datos, es la encargada del control de acceso al medio y a la vez es la responsable de transmitir los paquetes, de igual manera incluye dentro de sus funciones las labores de validar las tramas que recibe, comprobación de errores en la comunicación y confirmar la recepción de tramas al emisor.

Esta subcapa tiene funciones menos relevantes que las anteriormente mencionadas pero también tienen su importancia en el proceso entre estas tenemos la fragmentación de paquetes, control de flujo, tasa de transmisión y funciones relacionadas con la gestión de la batería; En síntesis esta capa es la encargada de controlar un medio de comunicación compartido por una serie de dispositivos que se comunican a través de él. Entre las restricciones de este tipo de redes, es el ahorro de energía es uno de las más importantes tanto así que influyen directamente en el diseño de estos protocolos (MAC). Estos protocolos se pueden agrupar en dos clases, los protocolos basados en slots o ranurados y los basados en muestreo.

Protocolos Basados en Slots o Ranuras:

En los protocolos ranurados, los nodos dividen el tiempo en intervalos discretos “ranuras o slots”, y los planifican dependiendo del estado en que se encuentra el radio “modo recepción, modo transmisión o apagada”. La sincronización de los slots con los vecinos permite que los nodos enciendan la radio solamente cuando sea necesario, con lo que se reduce considerablemente la escucha ociosa. A menudo estos protocolos se convierten en estáticos después de que se planifique un determinado horario o sincronización para los slots, un nodo solo puede

²⁷TAPIA, José Luis, Tesis: *Tutorial de redes de sensores ad hoc con eficiencia en energía*. Capítulo 6 http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/tapia_z_jl/capitulo6.pdf

comunicarse con otros nodos dentro del mismo periodo de slots previamente establecido, los periodos cortos de comunicación pueden conducir a un aumento de la contención, y los costes de la sincronización y mantenimiento penalizan el consumo energético y el ancho de banda. Estos protocolos incluyen los protocolos TDMA, IEEE 802.15.4, S-MAC, T-MAC y TRAMA, entre otros.

Protocolos Basados en Muestreo:

A diferencia del protocolo de ranura en vez de coordinar las ranuras de tiempo, los nodos cambian a estado activo en cierto periodo de tiempo buscando de actividad en el canal de radio, si se detecta actividad en el canal, se inicia la recepción de los datos. Dependiendo de la capa física, esta detección se puede basar en el nivel de energía del canal o en la detección de portadora. El muestreo periódico del canal permite que un nodo ahorre energía manteniendo su radio apagada la mayor parte del tiempo. En comparación con los protocolos ranurados, estos son muy flexibles ya que un nodo puede comunicarse con otro cualquiera dentro del alcance de la radio. Pero la flexibilidad tiene un coste, mientras que los protocolos ranurados envían los paquetes de datos regularmente, en muestreo hay que enviar mensajes largos y costosos para despertar a un vecino. Dentro del tipo de protocolos basados en muestreo encontramos: Aloha, B-MAC, WiseMAC, transceiver de Chipcon CC2500, y la plataforma mica de Berkeley.

3.2.1 Protocolos Utilizados²⁸:

Protocolo ranurado IEEE 802.15.4 :

Este protocolo fue considerado como estándar en el 2003 y surge por la necesidad de tener un protocolo estándar de bajo consumo y bajo ancho de banda para

²⁸ UNIVERSIDAD DE CASTILLA LA MANCHA, *B-MAC y otros Protocolos de Acceso al Medio*. Departamento de Sistemas Informáticos. <https://www.dsi.uclm.es/descargas/technicalreports/DIAB-06-09-2/TRBMAC.pdf>

redes de sensores, estableciendo dos topologías de red como lo son la topología tipo estrella y la topología “Peer-to-Peer”. Cuando se quiere determinar la topología que se va a utilizar, se debe tener en cuenta la aplicación en la que se va a desempeñar la red de sensores, pero sabiendo de antemano que en periféricos e interfaces de PC se pueden implementar conexiones tipo estrella, y en aplicaciones para la monitorización de terrenos que despliegan la red por un área de terreno considerable se implementa una red Peer-to-Peer con el fin de controlar los problemas de cobertura. Existen tres tipos de nodos dependiendo de la topología, el RFD, FFD y el controlador de red; cada uno con funciones específicas de la topología de red.

Este estándar establece tres clases de funcionamiento, utilizando beacons, no utilizando beacons y utilizándolos, pero con un tiempo de acceso garantizado (GTS), dependiendo de la topología y la aplicación en la que va a funcionar la red.

- IEEE 802.15.4 con beacons:

En este mecanismo que utiliza beacons, es aquel en que un nodo determinado manda unas señales, de manera periódica y va marcando unas divisiones de tiempo entre dos beacons. En concreto lo que se hace es establecer 16 slots los cuales serán utilizados cuando los nodos que quieran transmitir lo haciéndolo por cada uno de estos slots. En el estándar IEEE 802.15.4 con beacons hay una señal que le indica al un nodo que puede transmitir y si no tiene nada para transmitir este se apaga, en el caso contrario que si tenga algo para transmitir, espera un periodo de contención aleatorio, de varios slots, Tras ese periodo, si el medio está libre, el nodo retransmitirá alineado con el siguiente slot de tiempo. La sincronización permite que varios nodos puedan transmitir al mismo tiempo, reduciendo las colisiones e intentos de retransmisión.

El PAN coordinator se el encargado de transmitir beacons cada cierto periodo tiempo; entre beacon y beacon se establece una supertrama compuesta de 16 slots "slots de backoff". Al periodo que ocupan los 15 slots libres que hay entre beacons se les llama CAP (Contention Access Period), en ellos los dispositivos pueden transmitir de forma coordinada, como se ve en la figura 13:

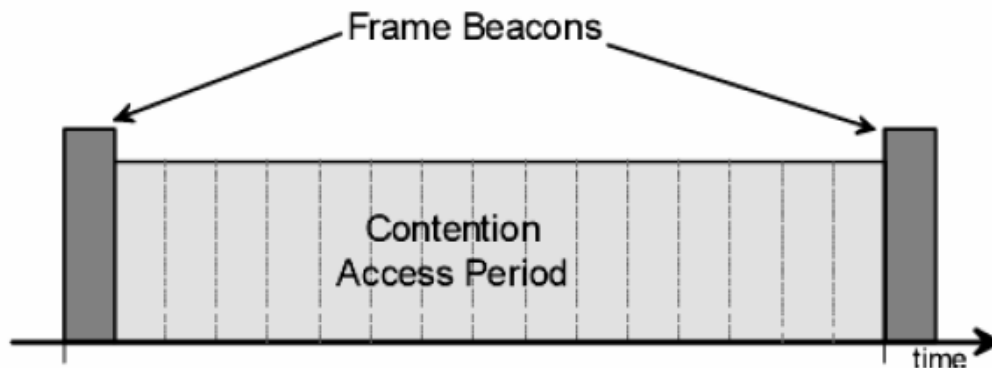


Figura 13 IEEE 802.15.4 Trasmisión con beacons Tomada de b-mac y otros protocolos de acceso al medio pág. 7

Para este mecanismo se utiliza CSMA-CA ranurado para el acceso al medio, en donde las ranuras de backoff están alineadas con el comienzo de un beacon, cada vez que un nodo desea realizar una transmisión, tiene primero que alinearse con el siguiente slot de backoff y entonces tiene que esperar un número aleatorio de ranuras de backoff. Si el canal está libre, el siguiente slot comenzaría a transmitir, sino dejará pasar otro número aleatorio de ranuras de backoff. Los únicos paquetes que no están sometidos a CSMA-CA son los ACK's y los beacons.

- IEEE 802.15.4 sin beacons:

El mecanismo de acceso al medio en este estándar es CSMA-CA no ranurado, es decir que los dispositivos transmiten en el momento que es

necesario sin esperar ningún beacon de ningún PAN coordinator, su mecanismo de funcionamiento establece que cada vez que un dispositivo va a transmitir, espera un tiempo aleatorio, si encuentra el canal libre espera un tiempo de backoff, pasado este tiempo intenta transmitir, si el canal se encuentra ocupado después del periodo de backoff volverá a esperar otro periodo aleatorio de tiempo y otro de backoff, hasta que realice la transmisión.

- IEEE 802.15.4 con beacons y GTS:

Por su parte, este modelo proporciona una latencia mínima para aquellos dispositivos que necesiten tener este parámetro garantizado, por tal motivo implementa los GTS (Guaranteed Time Slot), estos se definen como la trama de beacon y se sitúan dentro del periodo de libre contención CFP (Contention Free Period), que es un espacio reservado para que en caso de haber mucho tráfico, ciertos dispositivos tengan siempre prioridad de utilizarlo con el fin de minimizar la latencia ver figura 14:

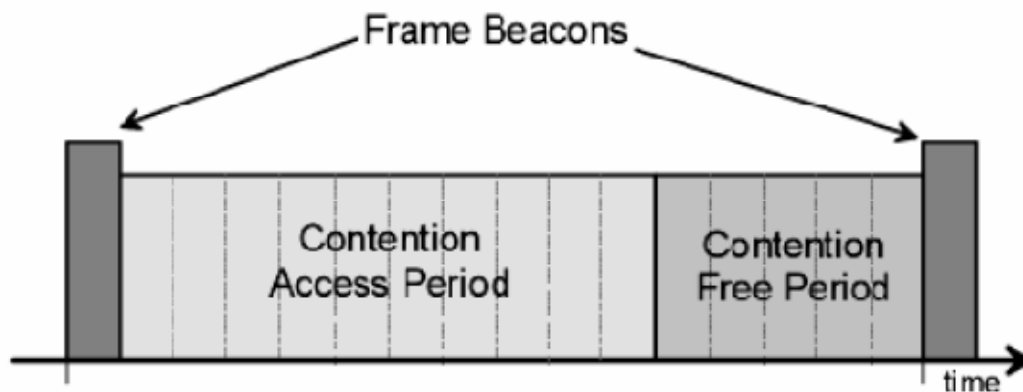


Figura 14 IEEE 802.15.4 Trasmisión con beacons y GTS

El PAN o coordinador tiene una función muy importante en este modelo con lo es la de encarga de la organización de los nodos de la red, los nodos RFD's se asocian a un coordinador en las dos topologías, por otra parte los nodos FFD's pueden asociarse y comunicarse con otros coordinadores, pero no pueden asociarse a nodos no coordinadores o RFD's. Al momento que un dispositivo coordinador se despierta, pone en marcha el mecanismo de beacons y envía una señal de red o beacon, el cual le informa a los nodos cuánto tiempo va a estar despierto, la duración del superframe, cuándo va a volver a mandar otro beacon, y la duración del beacon.

De esta manera se establece tres posibilidades de acceso al medio en el estándar IEEE 802.15.4 el mecanismo de señalizaciones (beacons) para el establecimiento de topologías en estrella, un mecanismo de acceso al medio CSMA/CA para las topologías punto a punto y, para conseguir que ciertos nodos tengan prioridad, un mecanismo de contención que asegura un periodo de tiempo para estos dispositivos.

Protocolo ranurado S-MAC (Sensor Medium Access Control):

Para hacer frente al medio radioeléctrico gran parte de los protocolos diseñados, o "protocolos de control de acceso" proponen una serie de tramas de control que arbitren el acceso, claro está que en un medio con innumerables posibilidades de variación en la infraestructura de la red original es posible que se presente una saturación al medio con este tipo de tramas de control, y también hay un alto incremento en la probabilidad de tener que procesar paquetes que no estaban destinados al nodo que permanece a la escucha.

Este protocolo es un poco similar al 802.15.4 pero diferenciados notablemente en sus mecanismos; por su parte S-MAC está basado en un esquema RTS-CTS de

bajo consumo de energía para redes de sensores, periódicamente duerme, despierta, escucha el canal, y después vuelve a dormir, utilizando lo que se conoce como duty cycle. Este protocolo fue diseñado para trabajar como caja negra ya que no tiene ningún tipo de interfaz que permita alterar el duty cycle; pero a cambio de esto, el encaminamiento, organización, sincronización y servicios de fragmentación de paquetes forman parte de él y todos estos servicios están disponibles para los protocolos de red.

En S-MAC el periodo de actividad es fijo, 115ms, a diferencia del periodo en el que duerme, este es variable y la longitud de este dictamina el duty cycle. La red se divide en celdas, y cada nodo perteneciente a una celda intercambia información necesaria para la sincronización de sus envíos, pero si los nodos pertenecen a más de una celda deben mantener la información de sincronización de ambas celdas; en la Figura 15 se muestra el comportamiento de este protocolo:

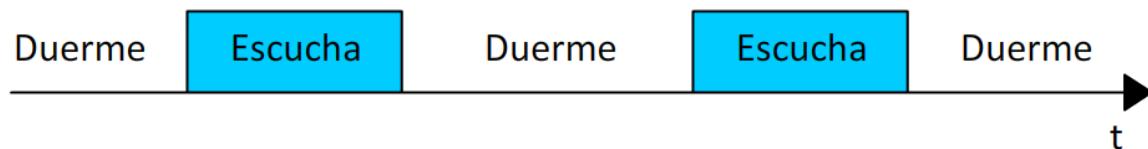


Figura 15 Estados del protocolo S-MAC b-mac y otros protocolos de acceso al medio pág. 10

Por otro lado, hay un protocolo que mejora el uso de la energía con respecto al ya mencionado S-MAC, es T-MAC, el cual trabaja usando un preámbulo muy corto para escuchar en el principio de cada período activo; después de la sincronización de cada período activo, envía o recibe los paquetes RTS-CTS a través de una ventana muy corta y si no hay ninguna actividad en este período, el nodo cambia a estado dormido. Este protocolo T-MAC, aún con cargas de trabajo variables utiliza un quinto de la energía de la que gasta S-MAC, con lo que se ha conseguido la mayor mejora al momento de realizar una comparación con el antes mencionado S-MAC.

Cuando se trabaja con cargas homogéneas, T-MAC y S-MAC se comportan igual, al punto que el protocolo T-MAC llega a sufrir de los mismos problemas de complejidad y escalabilidad que generalmente son de S-MAC.

Protocolo de muestreo B-MAC:

B-MAC (Berkeley Medium Access Control), es un protocolo capaz de reducir la denominada escucha ociosa, que es el tiempo que el nodo escucha sin recibir transmisión. Este protocolo propone que cada estación se active cada cierto período de tiempo para comprobar la actividad en el canal, en el caso de detectar alguna actividad permanece a la escucha y en caso contrario vuelva a dormir, a dicho período se le ha denominado wake-up time. El tiempo entre periodos wake-up se fija mediante el denominado check interval. B-MAC define 8 check intervals, y cada uno de ellos se corresponde a un listening mode diferente. La figura 16 representa la forma de trabajo del protocolo B-MAC para dos nodos:

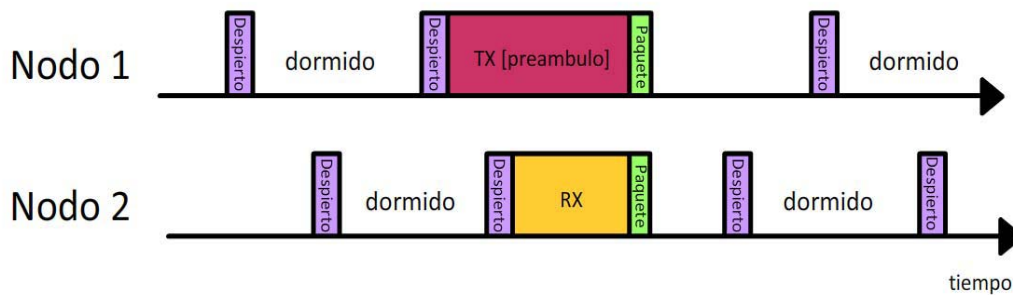


Figura 16 Modo de trabajo de B_MAC b-mac y otros protocolos de acceso al medio pág. 11

Como método para garantizar que todos los paquetes son recibidos, los paquetes se envían con un preámbulo cuya longitud de transmisión es superior al check interval, este protocolo define ocho tamaños diferentes para los preámbulo, cada uno relacionado con un diferente modo de transmisión, lo que B-MAC denomina transmit mode.

Dentro de las ventajas de B-MAC también se puede resaltar su modularidad y flexibilidad, ya que proporciona interfaces accesibles a las capas superiores, para que desde estas capas se pueda fijar los modos de listening y transmit, ajustándose a las necesidades del momento. Se asegura que utilizando las interfaces, y realizando las modificaciones oportunamente como atender al estado instantáneo del nodo, se pueden llegar a conseguir grandes ahorros de energía en la red.

Protocolo de muestreo WISE-MAC:

Es un protocolo orientado a redes de sensores basadas en infraestructura y está diseñado especialmente para funcionar con el sistema WiseNet del CSEM, cuyo mecanismo incorpora un transceiver de radio FSK, con dos bandas de trabajo 434 y 869 Mhz. Además este protocolo se basa en la idea de tener dos modos de comunicación, una la comunicación entre el nodo y la estación base, y la otra es desde ésta a los nodos.

Tenemos por una parte las comunicaciones downlink, que van de la estación base al nodo y tiene como principal característica que los nodos escuchan el medio durante un tiempo aleatorio, y si este está ocupado esperan por si llegan paquetes para ellos o si el medio se desocupa; mientras la estación base al solicitar los datos, debe asegurarse de que el nodo esté en modo de recepción al momento que ella quiera transmitir, para que la comunicación sea sincronizada, por lo que añade un preámbulo a sus tramas que alarga la duración hasta igualarla al periodo de muestreo del nodo receptor. Por lo tanto, la clave de la comunicación está en reducir este periodo haciendo que la estación base conozca exactamente cuánto dura y así también cuándo ocurrirá el siguiente periodo de escucha.

Por otro lado, La solución que plantea WiseMAC para las comunicaciones de nodo a estación base se basa en tener en cuenta que la energía en la estación base es

ilimitada, por lo que esta puede escuchar al canal continuamente. El protocolo de acceso al medio que se utilizará no necesita de ningún esquema de wake-up, entonces nos queda resolver el problema de los accesos múltiples a un medio compartido como el canal de radio. Pero teniendo en cuenta que si las comunicaciones entre los nodos y la estación base provocan un nivel de tráfico próximo a la máxima capacidad del medio, este problema se vuelve muy complejo. Sin embargo, si el nivel de tráfico es relativamente moderado, solamente utilizando el mecanismo CSMA podemos acercarnos al caso ideal, en el que no se produce idle listening, overhearing sino solamente algunas colisiones.

4. FUTURO DE ESTAS TECNOLOGÍAS

4.1 Futuro de las Redes Inalámbricas:

Las redes inalámbricas brindan la posibilidad de integrar conectividad y movilidad para usuarios tanto corporativos como domésticos, mediante tecnologías como Wi-Fi y Wimax, de las que se vislumbra el desarrollo de nuevos estándares como el 802.11n para redes Wi-Fi que podrá funcionar a una velocidad de unos 300 Mbps, unas cuarenta veces más rápido que el actual utilizado, el 802.11b²⁹.

Por este motivo compañías como Broadcom cabecilla de éste proyecto dice que ya tiene preparados los chips que serán compatibles con ésta nueva Wi-Fi, mientras que otras empresas como Marvell pretenden imponer una fuerte competencia a Broadcom y aseguran que también tienen sus propios chips preparados y listos para funcionar.

En cuanto a la arquitectura, sin embargo, se puede hablar de la mezcla de las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” para poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo, logrando que el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Sabiendo de antemano que las topologías utilizadas por la tecnología Wi-Fi son las siguientes:

²⁹Artículo: *EL FUTURO DE LA WIFI, PREPARÁNDOSE*. <http://xataka.com/2006/01/25-el-futuro-de-la-wifi-preparandose>.

- Topología Ad-Hoc: Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red *Peer to Peer* o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos, y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A medida que haya más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, sin la necesidad de que lleguen a verse entre sí.

- Topología Infraestructura: En esta existe un nodo central AP (Punto de Acceso WiFi) que sirve de enlace para todos los demás TR (Tarjetas de Red Wifi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación entre los nodos, estos deben estar dentro de la zona de cobertura del AP.

Surge entonces, un caso especial de topología de redes inalámbricas, es el caso de las redes MESH, o redes en malla, que son aquellas redes en las que se mezclan las dos topologías de las redes WiFi.

Los inicios de las redes MESH o acopladas son militares. Inicialmente se usaron para comunicarse con aquellas unidades de militares que aún estando lejos de las zonas de cobertura de sus mandos estaban lo suficientemente cerca entre si como para formar una cadena a través de la cual se pudiese ir pasando los mensajes hasta llegar a su destino (los mandos).

Las redes MESH son aquellas en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de

cobertura de los AP están dentro del rango de cobertura de algún TR que directamente o indirectamente está dentro del rango de cobertura del AP³⁰.

También permiten que las TR se comuniquen independientemente del AP entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al AP sino que pueden pasárselos a otras Tarjetas de Red para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (Hops en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno.

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

- Modo Managed: Es el modo en el que el TR se conecta al AP para que éste último le sirva de "concentrador". El TR sólo se comunica con el AP.

- Modo Master: Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW³¹.

³⁰ Curso: *REDES INALÁMBRICAS. WI-FI, EL FUTURO DE LA COMUNICACIÓN*. Capítulo 12: MESH Networks. <http://www.mailxmail.com/curso/informatica/wifi/capitulo12.htm>

4.1.1 Características de las Redes MESH³²:

Ajustes reales:

En la realidad la topografía raramente viene en forma de anillo, línea recta o estrella; En terrenos difíciles, sean remotos, rural o urbano, donde no todos los usuarios ven uno o algunos puntos centrales, lo más posible es que el usuario solo vea a uno o más usuarios vecinos.

Precio:

El que cada nodo MESH funciona tanto como cliente y como repetidor potencialmente significa ahorro en el número de radios necesarios, y por consiguiente en el presupuesto total. Mientras este punto pierde relevancia con la caída de los precios de radios, la cercanía de las redes MESH puede reducir la necesidad de torres centrales (costosas y vulnerables) y otras infraestructuras centralizadas.

Organización y modelos de negocio:

La naturaleza descentralizada de las redes MESH se presta muy bien para un modelo de propiedad en donde cada participante de la red posee y mantiene su propio hardware, el cual simplifica significativamente los aspectos financieros y comunales del sistema.

Facilidad y simplicidad:

Para un artefacto que este pre instalado con software de MESH inalámbrico y usa protocolo estándar como el 802.11b/g, el montaje es extremadamente simple. Ya

³¹ Curso: *REDES INALÁMBRICAS. WI-FI, EL FUTURO DE LA COMUNICACIÓN*

Capítulo 11: Topología y Modos de funcionamiento de los dispositivos.

<http://www.mailxmail.com/curso/informatica/wifi/capitulo12.htm>

³² BÜTTRICH, Sebastian. *Redes MESH*. Capítulo 13. www.wilac.net/tricalcar – Octubre 2007

que las rutas son configuradas dinámicamente, es suficiente con ubicar la caja en la red y juntar cualquier antena requerida para alcanzar uno o más nodos vecinos.

Red robusta:

Las características de la topología de una red MESH y del enrutamiento AdHoc prometen gran estabilidad en cuanto a condiciones variables o en alguna falla de algún nodo en particular, la cual va a estar bajo duras condiciones experimentales.

Potencia:

Los nodos de una red MESH, pueden ser construidos con bajísimos requerimientos de energía, es decir, pueden ser desplegados como unidades completamente autónomas con energía solar, eólica, hidráulica, celdas combustibles (derivados del petróleo) o generada por tracción de sangre; exceptuando posiblemente aquellos nodos que mantienen un enlace directo con Internet.

Integración:

El hardware de las MESH tiene todas las ventajas de una tecnología firme y simple: típicamente pequeño, no hace ruido y fácilmente encapsuladas en cajas a prueba de agua. Esto significa que integra agradablemente a la intemperie así como también para usar dentro de los hogares.

Entornos urbanos y rurales:

En sus principios, las redes MESH fueron propuestas para redes urbanas y redes municipales, sin embargo, hay un gran potencial para redes MESH en zonas de conectividad rurales.

Tópicos y limitaciones:

Como cualquier tecnología existen limitaciones y tópicos para las redes MESH, la mayoría de estos están basados alrededor de los límites del ancho de banda, escalabilidad y las dificultades de garantizar calidad de servicio.

Es importante estar al tanto del hecho que las estructuras organizacionales y comunicacionales de un proyecto no son necesariamente reflejados uno a uno por la estructura técnica de una red. Ellos pertenecen a dominios diferentes.

Un escenario típico MESH en una zona urbana puede verse así, conectando mayormente antenas en techos. Pero potencialmente incluyendo muchas otras ubicaciones, como torres de antenas, árboles, nodos móviles (vehículos, laptop).

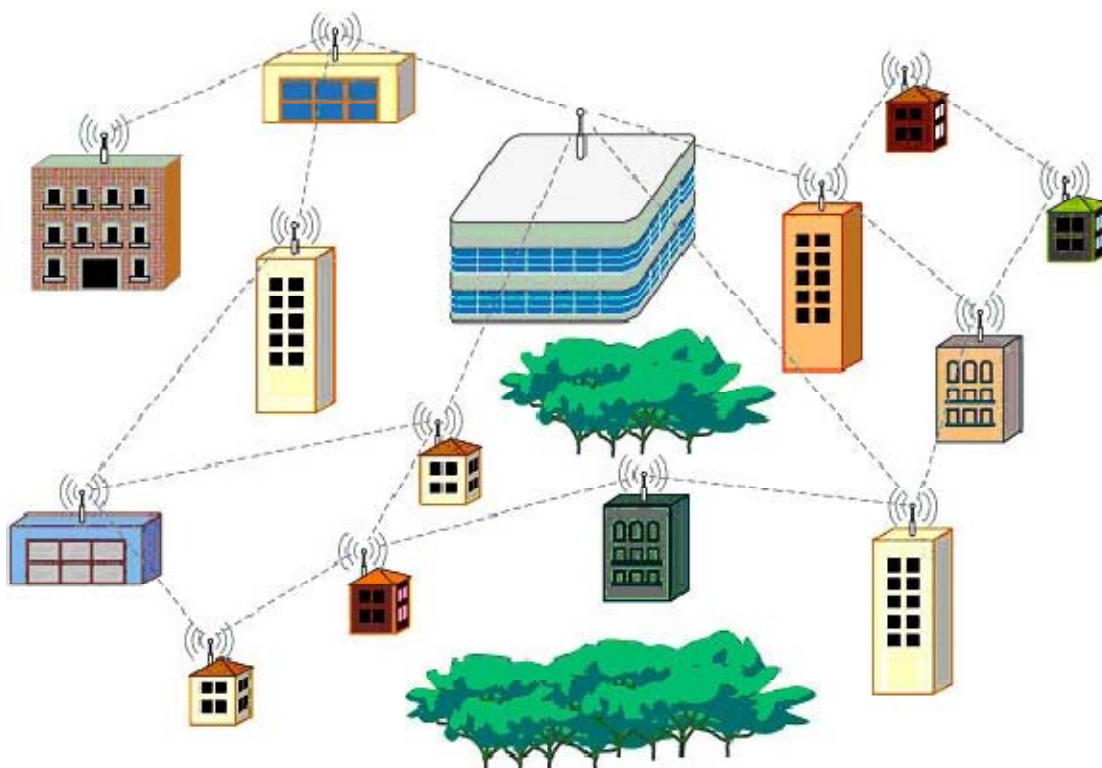


Figura 17 Escenario típico de MESH Tomada de www.wilac.net/tricalcar

Los avances que esta tecnología ha representado en el tema de las telecomunicaciones han dado pie a un sinnúmero de experimentos exitosos que permiten vislumbrar el interés de muchas comunidades sobre él y de la cual ya se han adelantado algunas investigaciones con resultados satisfactorios.

4.2 Futuro de las Redes Sensoriales:

Muy a la par de las redes Ad-Hoc, las WSNs han atraído la atención de la comunidad de investigación académica e industrial, en los últimos años un número de prototipos de sensores inteligentes han sido diseñados e implementados por la comunidad de investigación académica, entre estos tenemos los famosos Berkeley Motes y Smart Dust, pero después de muchos proyectos académicos interdisciplinarios actualmente están siendo financiados varios proyectos con el fin de desplegar y utilizar realmente las redes sensoriales. Uno de estos proyectos es Great Duck Island, en el cual una WSN ha sido desplegada para monitorear el hábitat de los nesting petrels sin alguna interferencia humana con animales.

Los nodos de sensores inteligentes en nuestros días ya siendo producidos y comercializados por algunos fabricantes electrónicos como Citemos Crossbow, una compañía que produce a gran escala los nodos de sensor Motes desarrollado en UC Berkeley y otras compañías importante como Intel, Philips, Siemens, están interesados en la tecnología WSN desarrollando sus propias plataformas de nodos de sensores inteligentes.

También se ha iniciado una considerable actividad de estandarización en el campo de las WSNs; tal vez uno de los impulsos más evidente en este ámbito es el de el estándar IEEE 802.15.4, en el cual se define los protocolos de la capa física y de la capa MAC para monitoreo remoto y control, así como también para aplicaciones de redes de sensores ZigBee que es un consorcio de industrias (actualmente

involucra a más de 100 miembros, representando a 22 países en 4 continentes) con el objetivo de promover el estándar IEEE 802.15.4.

En la actualidad, esta tecnología se encuentra lista implementarse puesto que se encuentra relativamente madura, pero aplicaciones basadas en redes de sensores no han sido completamente definidas; algunas industrias se esfuerzan por encontrar mercados importantes para aplicaciones WSN, trayendo esto algunas promesa como parece ser el control del hogar, la automatización de edificios, la automatización industrial, y las aplicaciones automotoras³³.

Otros de los campos de implementación de este tipo de redes, que promete revolucionar las comunicaciones es la inclusión de las redes sensoriales a la Internet, creando lo que ya se denomina “Internet Sensorial”.

Un grupo de investigadores de la Queen’s University de Belfast (Irlanda del Norte) se ha dado a la tarea de desarrollar un revolucionario programa informático para Internet capaz de transmitir y recibir señales sensoriales en la Red. Su objetivo es introducir en los mundos virtuales, hasta ahora dominados casi exclusivamente por el sentido del oído y de la vista, una tercera variable: el tacto.

Este proyecto tiene como finalidad que cualquier usuario pueda “tocar” objetos virtuales manipulando un “brazo mecánico” que responde a señales electrónicas.

Se cree que con esta investigación estamos a punto de entrar en una segunda etapa en Internet, en la que se debería ser capaz de facilitar una comunicación multimodal, incluidas sensaciones adicionales. Esto, gracias a la llamada tecnología Haptic o “del tacto”, la cual conecta al usuario con un sistema automatizado a través del sentido del tacto aplicando fuerzas, vibraciones,

³³ SANTI, Paolo. *Topología y Control en Redes Inalámbricas y Redes de Sensores*.
<http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct06Marzo07/ComInalam/TRabajos/TRABAJO3/G1/PROYECTO%203%20-%20GRUPO%201.doc>

presiones y movimientos. Esta estimulación mecánica se usará para crear objetos virtuales táctiles en un mundo virtual táctil.

En la actualidad, algunos ejemplos de la aplicación de esta tecnología, a un nivel todavía muy básico, pueden encontrarse en los teléfonos móviles, cuyas vibraciones avisan al usuario de una llamada o un mensaje, o en la popular videoconsola Wii de Nintendo.

Las áreas que se van a ver mejor beneficiadas con este tipo de tecnología, serán los videojuegos, el campo de la medicina, en donde se prevé un futuro no muy lejano en el que los cirujanos puedan impartir clases de formación a través de la Red. Otro uso de esta tecnología cambiaría para siempre la relación con Internet de las personas con deficiencias visuales.

En la actualidad las investigaciones sobre este tema, están siendo adelantadas por un grupo de científicos norirlandeses y están siendo conducidas en cooperación con las multinacionales British Telecom (BT, Reino Unido), Inmersion (EU) y HandshakeVR (Canadá); logrando obtener, hasta el momento, el primer apretón de manos online, entre dos personas, una de la Queen's University (universidad gestora del proyecto) y un funcionario de la British Telecom, con la ayuda de los brazos mecánicos³⁴.

³⁴ EL UNIVERSAL de México, *Internet sensorial, el futuro del mundo virtual*.
<http://www.el-universal.com.mx/articulos/42409.html>

CONCLUSIÓN

Mediante la realización de este trabajo hemos logrado determinar la funcionalidad y aplicabilidad de tecnologías tan importantes en esta era como lo son las inalámbricas, al igual que los esquemas y arquitecturas sobre las cuales trabajan, consiguiendo así definir de manera clara los objetivos de cada una; también hemos podido concluir:

- ❖ La IEEE como entidad encargada de la estandarización, ha dado validez y funcionalidad comercial a las tecnologías inalámbricas, ad hoc y sensoriales para lograr la implementación de estas y la inclusión en dispositivos que permitan hacer más fácil la vida del hombre.
- ❖ Las arquitecturas y los protocolos con los que trabajan estas redes, hacen que sean más funcionales y se desenvuelvan mejor en cualquier entorno.
- ❖ La seguridad es un tema esencial en las redes, por lo cual se han creado protocolos como el WEP, en el caso de las redes inalámbricas, que permiten la transmisión de información de manera segura y que a su vez ellos mismos han ido evolucionando de acuerdo a las necesidades y requerimientos de los usuarios.
- ❖ La investigación sobre estos temas es muy extensa y se pueden encontrar contenidos que aún requieren de mayor profundización, como lo es el tema de la seguridad en donde todavía no se tiene la última palabra y se hace necesario generar más proyectos de desarrollo que ayuden a enriquecer el conocimiento que se tiene sobre estos.

RECOMENDACIONES

Durante el desarrollo de esta monografía al momento de la búsqueda de la información para formar las bases de este proyecto, nos encontramos con algunas dificultades debido a que no se encontraba información de procedencias confiables sobre algunos temas a desarrollar en este trabajo, entre estos temas están las redes sensorial, y los protocolos que se utilizan en las tecnologías inalámbricas desarrolladas en esta monografía; por este motivo una de nuestras recomendaciones para la institución es que adquieran textos con información relacionada con todo lo referente a las tecnologías inalámbricas en general, ya la información con que se cuenta es muy pobre y antigua puesto que este tema está en constante evolución y a tenido un gran aceptación en los últimos años.

Por último, otra de nuestras recomendaciones va dirigida así todos aquellos estudiantes con espíritu investigativo y en general para toda la comunidad universitaria interesada en temas de telecomunicaciones y con proyección hacia el futuro; quienes en las redes inalámbricas MESH y sensoriales pueden encontrar un gran potencial temático para un excelente desarrollo investigativo.

GLOSARIO

802.11 Es un familia de estándares de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.11x definen la tecnología de redes de área local.

802.11a Especificación sobre una frecuencia de 5 Ghz que alcanza los 54 Mbps.

802.11b Especificación con velocidades de hasta 11 Mbps, trabaja en la frecuencia de 2,4 GHz.

802.11g Especificación con velocidades de 54 Mbps en la frecuencia de 2.4 GHz. Ultima aprobada.

802.11n Especificación en estado de desarrollo que se espera alcance velocidades de hasta 200 Mbps.

AD-HOC Un tipo de topología de WLAN en la que sólo existen dispositivos clientes, sin la participación de ningún Access Point, de forma que los clientes se comunican de forma independiente punto a punto, peer-to-peer.

AP *Access Point*. Estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.

Bluetooth Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia con una velocidad máxima de 11Mbps a la frecuencia ISM de 2'4 GHz.

BPSK *Biphase Shift Keying*

BSS *Basic Service set*.

CSMA/CA *Carrier Sense Multiple Access with Collision Avoidance*.

CSMA/CD *Carrier Sense Multiple Access with Collision Detect*

dBm Corresponde a la unidad de medida de la potencia de emisión en redes inalámbricas, en donde cuanto mayor (positivo) sea el valor obtenido, más intensidad de campo se estaría recibiendo.

DIFS Distributed InterFrame Space, es el espacio distribuido entre marcos en el protocolo csma/ca.

DSSS *Direct Sequence Spread Spectrum*. Técnica de transmisión

ESS *Extended Service Set*.

ESSID *Extended Service Set Identification*. Uno de los dos tipos de SSID, el que se emplea en redes wireless en modo infraestructura.

FHSS *Frequency Hopping Spread Spectrum*. Espectro expandido mediante saltos de frecuencial.

Hot-Spot Es un lugar donde se puede acceder a una red wireless pública.

IBSS *Independent Basic Service Set*.

IEEE *Institute of Electrical and Electronics Engineers*.

IrDA *Infrared Data Association*.

LAN *Local Area Network*. Red de Área Local

MAC *Media Access Control*. Corresponde al nivel de enlace (nivel 2) en el modelo OSI.

OFDM *Orthogonal Frequency Division Multiplexing*. División de frecuencia por multiplexación ortogonal,

On World Revista de publicación internacional de sistemas informáticos.

PCS *Personal Communications Systems*.

Peer to Peer modo de comunicación Punto a Punto.

QoS La calidad de servicio consiste en ofrecerle al usuario, de acuerdo a la aplicación, los recursos de red necesarios y suficientes para cumplir con los requerimientos por él establecidos.

QPSK *Quaternary Phase Shift Keying*.

SSID *Service Set Identification*. Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan

comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

TR Tarjeta de Red

Wi-Fi *Wireless Fidelity*, la organización comercial que prueba y certifica que los equipos cumplen el conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11x.

WLAN *Wireless Local Area Network*, es un sistema de redes de area local inalámbricas muy flexible y utilizado como alternativa a la LAN cableada o como una extensión de ésta

WiMax *Worldwide Interoperability for Microwave Acces*, es un estándar de transmisión inalámbrica de datos (**802.16d**) diseñado para ser utilizado en el área metropolitana o MAN proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.

WSN *Wireless Sensor Network* es un tecnología de tipo inalámbrica basada en sensores de alta percepción y desempeño.

REFERENCIAS

BIBLIOGRÁFICAS:

- CORTÉS GRAJALES, Miguel Ángel; ALVIS LARA, Maryori Tatiana. *Redes Móviles Inalámbricas Ad Hoc*. Universidad Tecnológica de Bolívar, Facultad de Ingeniería Electrónica, noviembre de 2004.
- PÉREZ BECERRA, Gianncarlo; FAJARDO SUÁREZ, Kenny. *Estudio de Redes Inalámbricas Basadas en Tecnología Wimax*. Universidad Tecnológica de Bolívar, Minor en Telecomunicaciones, Facultad de Ingeniería Eléctrica y Electrónica, noviembre de 2005.
- UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR, *Medios de Transmisión* Minor de Comunicaciones y Redes, Módulos de Fundamentos..

ENLACES:

- GONZÁLEZ VELASCO, Jorge Antonio; CAÑIZARES ORMAZA, Luis Vinicio. *Redes De Sensores*. Escuela Politécnica Nacional. <http://clusterfie.epn.edu.ec/ibernal/>
- VIDAL, Iván et. al. *Servicios de Valor Añadido en Redes Móviles Ad-hoc*. Universidad Carlos III, Madrid, España. http://www.it.uc3m.es/ividal/articulos/telecom03_adhoc.pdf
- UNIVERSIDAD INCCA DE COLOMBIA. Artículo: *Redes Locales Inalámbricas* <http://www.unincca.edu.co/boletin/indice.htm>
- GARCÍA FERNÁNDEZ, Nestor. *Modelo de Cobertura de Redes Inalámbricas*. Universidad de Oviedo. Marzo de 2006.
- HERNÁNDEZ CARDOSA, Amaterazú. Tesis: *Operación de una radio base celular cuando coexisten GSM & IS-54, IS-136*, Universidad de Las Américas. Puebla, México http://caterina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/capitulo4.pdf
- BLAT, Fernando, *Wimax a Fondo*. <http://www.xataka.com>
- CABAÑAS H., Adriana, *Tecnología Wifi en todos lados*, MICROASIST: Soluciones Humanas a problemas técnicos <http://microasist.com.mx/noticias/internet/achin201205.shtml>
- LEDESMA Karen, CASTELLAR Israel. *Diseño de una PAN Basada en Tecnología Bluetooth*. Universidad Tecnológica de Bolívar. Monografía Minor de Comunicaciones y Redes. Facultad de Ingeniería de Sistemas.

- SANTI, Paolo, *Topología y Control en Redes Inalámbricas y Redes de Sensores*
- TAPIA ZURITA, José Luis; Tesis: *Redes Inalámbricas de Sensores Ad Hoc*
http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/tapia_z_jl/capitulo2.pdf
- GARAIZAR SAGARMINAGA, Pablo Estándar 802.15 802.11 www.e-ghost.deusto.es
- BARAJAS, Saulo. Tesis Doctoral: *Protocolos de Seguridad en Redes Inalámbricas*. Universidad Carlos III de Madrid.
<http://www.saulo.net/pub/inv/SegWiFi-art.htm>
- GALLEGO, J.R., et al. *Control de admisión distribuido para redes móviles ad-hoc basado en un diseño cross-layer*. IEEE Latin America Transactions, vol. 5, No. 6, October 2007. Universidad Politecnica de Cataluña. Marzo, 2004.
- ZÁRATE, Jesús Alonso. *Estudio y Análisis de Técnicas de Acceso y Algoritmos de Adaptación Dinámica de Topología de Redes Inalámbricas Ad Hoc Autoconfigurables*
- ESCUDERO QUESADA, Ana; OLIVER RIERA, Miquel. *Estudio del rendimiento del algoritmo CSMA/CA IEEE 802.11 con diferentes niveles físicos*. Departamento de Matemática Aplicada y Telemática.
<http://nmg.upc.es/intranet/qos/9/9.3/9.3.15.pdf>
- UNIVERSIDAD DE CASTILLA LA MANCHA. *B-Mac y otros Protocolos de Acceso al Medio*. <https://www.dsi.uclm.es/descargas/technicalreports/DIAB-06-09-2/TRBMAC.pdf>
- Artículo: *EL FUTURO DE LA WIFI, PREPARÁNDOSE*.
<http://xataka.com/2006/01/25-el-futuro-de-la-wifi-preparandose>.
- Curso: *REDES INALÁMBRICAS. WI-FI, EL FUTURO DE LA COMUNICACIÓN*. Capítulo 12: MESH Networks.
<http://www.mailxmail.com/curso/informatica/wifi/capitulo12.htm>
- Curso: *REDES INALÁMBRICAS. WI-FI, EL FUTURO DE LA COMUNICACIÓN* Capítulo 11: Topología y Modos de funcionamiento de los dispositivos.
<http://www.mailxmail.com/curso/informatica/wifi/capitulo12.htm>
- BÜTTRICH, Sebastian. *Redes MESH*. Capítulo 13. www.wilac.net/tricalcar – Octubre 2007
- EL UNIVERSAL de México, *Internet sensorial, el futuro del mundo virtual*.
<http://www.el-universal.com.mx/articulos/42409.html>