UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TESIS

MANUAL DE BUENAS PRÁCTICAS PARA EL DISEÑO DE UNA RED ZIGBEE

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTA:

DANIEL PÉREZ CERVANTES

DIRECTORA DE TESIS: M.C. CINTIA QUEZADA REYES

CIUDAD UNIVERSITARIA.

Agradecimientos

Quiero agradecer a Dios por brindarme la oportunidad de estar aquí y darme a los mejores padres y hermanos del mundo, la bendición más grande que alguien puede recibir es su familia, familia los amo.

A mi mamá Anita Cervantes Estrada que sin ti este trabajo de tesis no existiría, gracias por darme la vida por ese esfuerzo diario, por todo el tiempo que me dedicas, por todas tus enseñanzas, por hacer que todo lo bueno que yo pueda ser es gracias a ti. Este trabajo de tesis es tuyo porque me enseñaste a perseverar, a ser paciente, a terminar lo que empiezo, a ser responsable y sobre todo a disfrutar cada día y no conformarme con algo sino a seguir creciendo como persona y como profesional. Nunca podré terminar de agradecer todo lo que haces por mí.

A mi papá Eliseo Pérez Estrada por tu esfuerzo diario, por siempre estar al pendiente de que nunca falte nada, por tus llamadas de atención que me han ayudado a tomar mejores decisiones y gracias por darme la oportunidad de seguir creciendo. Gracias por apoyarme en todo momento y darme ánimos en cada nuevo proyecto, este trabajo de tesis tiene mucho de ti, tú y mi mamá son mi ejemplo a seguir.

A mis hermanos Quique y Cheo que siempre me demuestran que nunca se deja de aprender y que siempre cuento con ustedes ya sea para un partido de futbol, videojuegos o solo platicar y reír por un muy buen rato. He disfrutado cada momento desde el día que los conocí.

A mi mamá Lala Estrada, a mi papá Juvenal Cervantes, a mi abuelita Virginia Estrada, a mi abuelito Pedro Pérez (en paz descanse) y todos mis familiares que siempre me han apoyado, me han dedicado un poco de su tiempo gracias por todo y por abrirme la puerta de su casa siempre con gran entusiasmo.

A mi gran amigo Joan Méndez por las ocurrencias de cada día, por hacer que las clases fueran muy amenas y divertidas, por las grandes tardes de videojuegos en casa de Mayra, las buenas charlas y ante todo por ser un gran amigo.

A Mayra y Marisol que siempre tienen otra forma de ver las cosas que abren panoramas y muchas opciones.

A Denisse gracias por ser una gran amiga y por aconsejarme elegir esta carrera y al final opté por la mejor opción.

A Laura García, Diego Hernández, Alejandra González, Nancy Acalco, Guillermo Reyes, Arturo Jiménez, Verónica Pérez, Paola Velázquez, Alma Vargas, Ana y Juan que cada que nos vemos, aunque no sea muy seguido, son grandes momentos. A los Ingenieros, Gabriela Camacho, Francisco Montoya y Sergio Cruz por darme la oportunidad de empezar de alguna forma mi vida profesional en UNICA y que me ha servido de enseñanza para la vida laboral fuera de la UNAM.
Es difícil mencionarlos a todos pero gracias a cada uno por su aportación, he aprendido algo bueno de cada uno.

Agradecimientos

Un agradecimiento especial a la M.C. Cintia Quezada Reyes por toda su dedicación para este trabajo, toda su paciencia y tiempo. ¡¡¡Gracias!!!

CONTENIDO

INTRODUCCIÓN

A través de la historia, la humanidad ha buscado la forma de comunicarse entre sí de diversas formas y permitirle ampliar sus conocimientos para poder sobrevivir ante posibles adversidades. En la actualidad esta comunicación se ha vuelto indispensable sobre todo con los avances en la ciencia que permiten que dos personas que están a una gran distancia puedan comunicarse entre sí en tan solo unos segundos, todo esto, gracias al surgimiento de las redes de datos que son un medio que permite entablar comunicación con cualquier persona de todo el mundo.

Con el desarrollo de las comunicaciones fueron creciendo las opciones como lo es la invención del telégrafo utilizando clave Morse aunque la limitante principal era el hecho de que sólo se podían mandar mensajes cortos por lo que únicamente se comunicaba lo más relevante, tiempo después surgió el teléfono, uno de los inventos que más ha ayudado a la humanidad a comunicarse y uno de los más usados hoy en día ya que se puede establecer comunicación de persona a persona en tiempo real hablando y después escuchando a través de un dispositivo electrónico.

Un poco más adelante se dio el surgimiento de una de las tecnologías más importantes para los habitantes del planeta, la computadora y las redes de computadoras son el parte aguas de la comunicación actual la cual es indispensable en los días modernos, hay quien dice que sin estas herramientas no se sabría qué hacer en la actualidad. Si se remonta al inicio de las redes de datos todo era a través de cables con los cuales aunque eran muy lenta la transferencia de la información, era un buen inicio para lo que venía ya que se desarrollaron estándares que permitieron acelerar este envío de información de una manera rápida y eficaz.

Pero no todo quedo ahí ya que ahora surge la gran necesidad de ahorrar energía y materiales puesto que se produce año tras año un gran desperdicio de energía y se tiran grandes cantidades de basura por lo que se buscan tecnologías que no requieran tanto material y que ahorren gran cantidad de energía surgiendo así las redes sin cables mejor conocidas como “Wireless”(término en inglés refiriéndose a “sin cables”) las cuales cada día que pasa traen nuevos beneficios inigualables como la posibilidad de poder comunicarse no importando dónde se esté sin la necesidad de tener cableado tan extenso instalado.

Una de esas tecnologías es ZigBee, por medio de ella es posible implementar nuevas formas de enseñanza y creación de nuevas herramientas de trabajo que ayuden a estudiar de una manera formidable todo tipo de conceptos aunados a practicar lo que se acaba de aprender en el aula.

Con esta tesis se busca proporcionar un manual completo en el que se explica qué es la tecnología ZigBee, qué ofrece, principales características, qué se debe tomar en cuenta para el diseño de una red, seguridad en este tipo de redes y recomendaciones importantes que se deben tomar en cuenta al momento de diseñarla e implementarla.

Este trabajo puede servir como base para trabajos futuros para alguien que quiera realizar la implementación de una red ZigBee siguiendo los estándares y normas necesarias para su correcto funcionamiento por lo que es un buen documento para consultar en todo momento y tomar en cuenta los puntos importantes como lo es el análisis, el diseño, funcionamiento y la implementación de la seguridad y de esta manera no haya un desorden al momento de interactuar con otras redes ya sea inalámbricas o cableadas asegurando que la información llegue a su destino final íntegra, disponible y sea confidencial.

OBJETIVOS

a) Dar a conocer una nueva tecnología inalámbrica que permita el ahorro de energía y la intercomunicación entre una gran cantidad de dispositivos electrónicos.

b) Ofrecer un manual de referencia en el que se puedan consultar las bases para poder implementar una red inalámbrica ZigBee.

Para lograrlos, este documento se divide en 5 capítulos:

a) CAPÍTULO I. CONCEPTOS BÁSICOS:

Se describen los conceptos básicos de redes desde los modelos OSI, TCP/IP y sus protocolos de servicio más utilizados, se mencionan también los principales conceptos de seguridad informática, amenazas, vulnerabilidades, servicios, mecanismos de seguridad y políticas de seguridad. Aunado a lo anterior se describe el espectro radio eléctrico.

b) CAPÍTULO II. REDES ZIGBEE (IEEE 802.15.4):

Se da una descripción completa del protocolo usado por las redes ZigBee, el protocolo IEEE 802.15.4, abarcando desde su panorama general así como su arquitectura, tipos de dispositivos usados, características principales, tipo de tráfico, modelos de red y comparación con otras tecnologías.

c) CAPÍTULO III. APLICACIONES PARA REDES ZIGBEE:

Se detallan las principales aplicaciones que tiene la implementación de una red o redes ZigBee describiendo sus principales beneficios.

d) CAPÍTULO IV. SEGURIDAD EN REDES ZIGBEE:

Se analizan las principales amenazas y vulnerabilidades de una red ZigBee y qué herramientas de seguridad se pueden implementar para su protección así como políticas de seguridad que permiten garantizar el correcto uso de la información que se transmite a través de ella.

e) CAPÍTULO V. BUENAS PRÁCTICAS PARA EL DISEÑO DE UNA RED ZIGBEE:

Tomando las bases descritas en los 4 capítulos anteriores se proveen buenas prácticas para el diseño de una red ZigBee desde sus principales requerimientos, así como su estructura, el tipo de espacio que ocupará, qué hardware y software es conveniente usar y las condiciones necesarias de seguridad para que la red sea funcional y evitar posibles ataques.

CAPÍTULO 1.

CONCEPTOS BÁSICOS

1.1Definiciones de redes de computadoras

En realidad no existe una definición específica para lo que es una red de computadoras, dependiendo de cada autor, existe una definición de acuerdo con su experiencia profesional, por lo que se verán algunas definiciones:

a) Las redes de computadoras son un conjunto de computadoras autónomas interconectadas que pueden intercambiar información no importando qué medio se utilice para que se lleve a cabo dicha interconexión[1].

b) Las redes de datos tienen como objetivos compartir recursos, información y programas que se encuentran localmente en todo el mundo, brindando confiabilidad a la información, disponiendo de alternativas de almacenamiento, teniendo una buena relación costo/beneficio y transmitiendo información entre usuarios distantes de manera más rápida y eficiente posible[2].

c) Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico. Una red de computadoras comienza cuando son dos o más dispositivos y/o computadoras conectadas. Para conectarse entre sí en una red el sistema de red utiliza protocolos de red[3].

Tomando en cuenta las definiciones anteriores, se define una red de computadoras como un conjunto de dispositivos autónomos interconectados entre sí, capaces de intercambiar información a través de diferentes medios como puede ser cableado o inalámbrico, además de utilizar protocolos de comunicación para garantizar que los datos lleguen con éxito de una forma segura, respetando la confidencialidad, integridad y disponibilidad de la información. Dicho intercambio se lleva a cabo entre los usuarios a través de un dispositivo y/o computadora, no importando a qué distancia se encuentren; en la figura 1.1 se observa un esquema sencillo de una red de computadoras.

[1] Redes de Computadoras, Andrew S. Tanenbaum, cuarta edición, Pearson educación
[2] Documento pdf, Redes de Datos, Ing José Joskowicz, Instituto de Ingeniería Eléctrica, Facultad de ingeniería Universidad de la República de Montevideo, Uruguay.
[3] http://www.lawebdelprogramador.com/diccionario/mostrar.php?letra=R&pagina=2

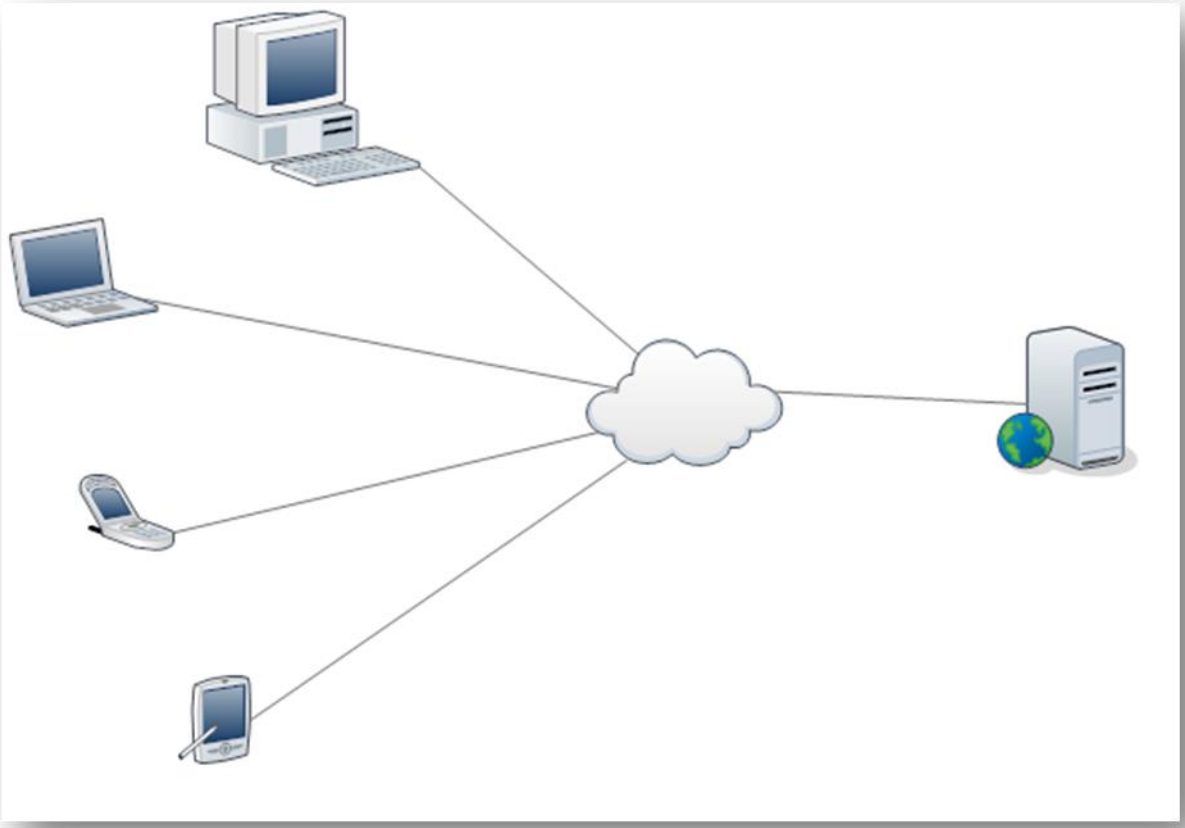


Figura 1.1 Red Básica de Computadoras.

1.2.7 Elementos de una red de computadoras

Para que exista comunicación entre dos o más computadoras y se garantice el envío seguro de la información, se consideran varios elementos que deben existir en cualquier red de computadoras es por esto que a continuación se describirán de manera general:

1. Protocolo de Red. Para que dos o más equipos o dispositivos se puedan comunicar, es necesario que cuenten con ciertas reglas que les permitan entablar dicha comunicación, por lo tanto, en el contexto de las redes de datos se dice que un protocolo es un conjunto de reglas formales, convenciones y estructuras de información que indican cómo es que las computadoras y otros dispositivos de red intercambian datos a través de la red. En otras palabras, un protocolo es un procedimiento estándar o formato que dos dispositivos de intercambio de información pueden entender, aceptar y usar para ser capaces de comunicarse unos con otros.

Se utiliza el término PDU (Protocol Data Unit-Unidad de Datos del Protocolo) para especificar las unidades de información de los protocolos que se utilizan para que se lleve el intercambio de datos de igual forma tanto del lado del dispositivo de origen así como del destino.

2. **Medios de transmisión o canal de comunicación[4].** Es el medio mediante el cual viajan las señales por las que se traslada la información, estos medios pueden ser terrestres o aéreos.

3. **Tecnología de transmisión.** Se refiere a la forma en que se envía la información de un lugar a otro a través de algún medio de comunicación, en las redes de datos existen dos muy importantes:

a) Enlaces de difusión. En este tipo de enlace solo existe un canal de comunicación, por lo que todos los dispositivos de red comparten este medio al intercambiar información. Una máquina envía un *paquete* a todas las computadoras, éste tiene una dirección de destino, por lo que si no va dirigido a ese equipo, lo ignora y no lo recibe, a este enlace se le conoce como difusión (broadcasting). Ahora, si lo que se quiere es transmitir solo a un subconjunto de máquinas, existe la multidifusión (multicasting), en donde los paquetes llegarán a todos aquellos equipos que estén inscritos en el grupo de este enlace de transmisión, en caso contrario, si no está dentro del grupo, no recibirá dichos paquetes.

b) Enlaces punto a punto. En este caso se tienen muchas conexiones entre pares individuales de máquinas, es decir, este tipo de enlace se lleva a cabo de un sola máquina a otra de forma individual, por lo que si quiere acceder a una tercera máquina requeriría de una máquina intermedia para poder establecer una comunicación, primero enviaría información a la máquina a la que está conectada, la máquina dos recibe la información y la envía a la tercera, la respuesta sería algo similar. Como una regla general, con muchas excepciones, redes pequeñas en una misma región utilizan la difusión mientras que las más grandes suelen ser de punto a punto. A este tipo de redes se les conoce como unidifusión (unicasting) que a diferencia de la difusión y multidifusión, la comunicación se lleva a cabo de un solo dispositivo a un solo dispositivo. En la Figura 1.2 se ve un ejemplo de cada tipo de transmisión.

[4] Para mayor información véase apéndice A “Medios de transmisión”

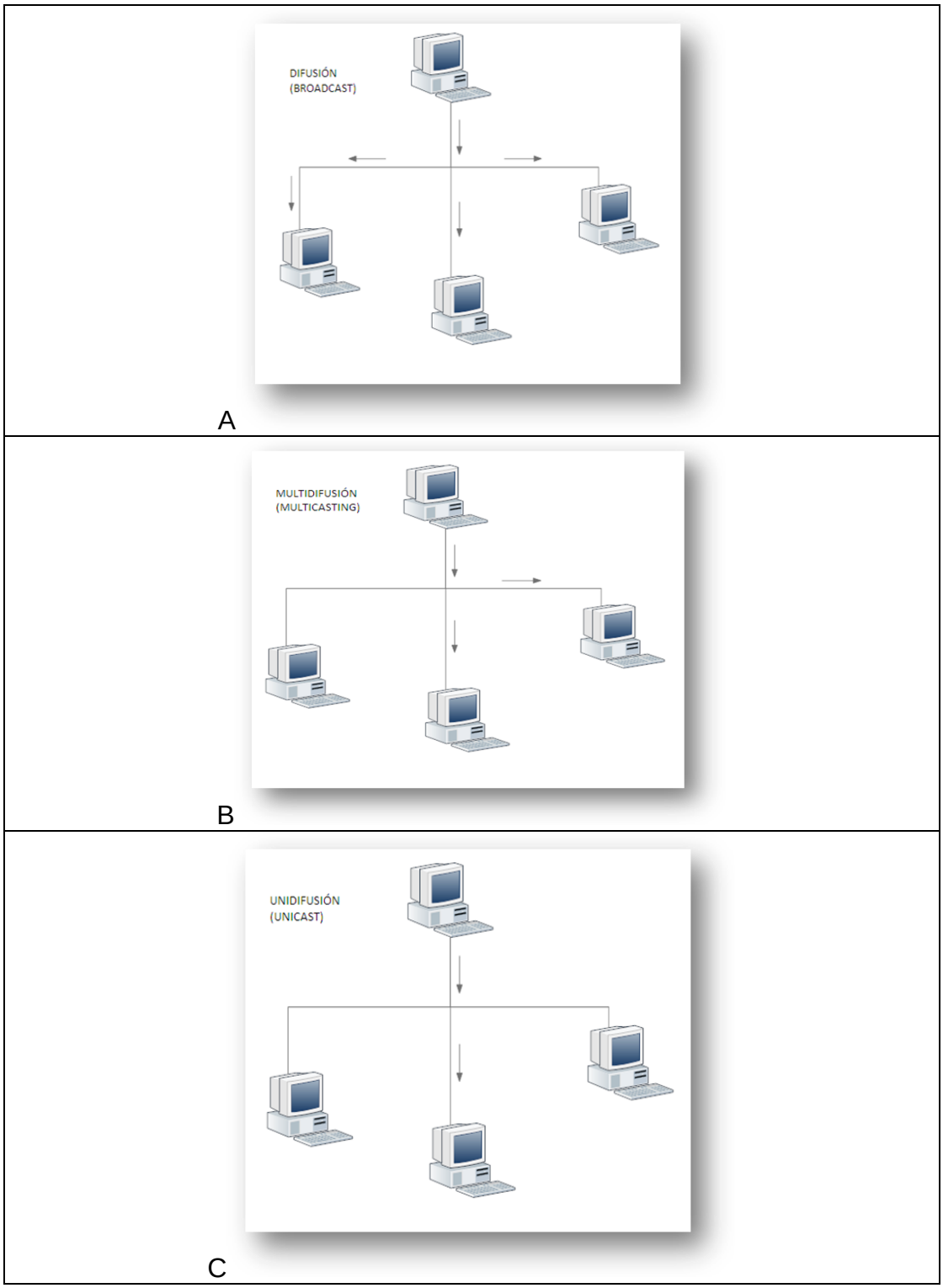


Figura 1.2 Tipos de Transmisión. A-Difusión, B-Multidifusión, C-Unidifusión.

4. **Escala de las redes.** Las redes de datos también tienen una clasificación según su alcance y su tamaño, a esto se le conoce como la escala de una red, la cual se divide de la siguiente forma:

a) Redes de Área Personal (PAN-Personal Area Network). Estas redes están destinadas para una sola persona, abarcan un área de un metro cuadrado aproximadamente, como por ejemplo una pequeña red inalámbrica en donde se conecta una computadora con su ratón, teclado e impresora.

b) Redes de Área Local (LAN-Local Area Network). Son redes de propiedad privada que se encuentran en un campus universitario, en uno o en varios edificios cercanos de pocos kilómetros de longitud. Su principal función es conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos e intercambiar información. Este tipo de redes son diferentes en tres aspectos importantes: tamaño, tecnología de transmisión y topología. Son redes restringidas por su tamaño, por lo que el tiempo de transmisión, en el peor de los casos, es limitado y conocido de antemano, aun así este límite permite utilizar ciertos tipos de diseño simplificando la administración. Una LAN tradicional se ejecuta a una velocidad de 10 a 100Mbps, tiene un retardo bajo (microsegundos o nanosegundos) y cometen muy pocos errores. Las LAN actuales funcionan hasta 10Gbps.

c) Redes de Área Metropolitana (MAN-Metropolitan Area Network). Son redes con cobertura urbana concebidas para vincular distintas redes LAN entre ellas, formando lo que se denomina internet. Se dice que son de cobertura urbana ya que pueden llegar, en ciudades grandes, a segmentos de 50km. Transportan señales a velocidades de 10^2 Mbps utilizando para ello fibra óptica. Prestan servicios de transporte para interconexión de redes, telefonía entre otros servicios y pueden ser de conmutación de paquetes con servicios orientados o no a la conexión.

d) Redes de Área Extensa (WAN-Wide Area Network). Estas redes son de cobertura ilimitada debido a que encadenan diferentes redes de cobertura menor. Para poder hacerlo, se valen generalmente de redes públicas y privadas, utilizando todo tipo de vínculos: no tangibles, como satélites y radio enlace, y tangibles, como pares de cobre, coaxiales y fibras. Son utilizadas para poder comunicarse más allá de un edificio.

5. Topologías de red.

a) *Topología en Malla*. En una topología en malla cada dispositivo tiene un enlace punto a punto; por tanto, una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada y salida. Dentro de sus varias ventajas, en primer lugar se puede mencionar que el uso de los enlaces dedicados garantiza que cada conexión solo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos. En segundo lugar, una topología en malla es robusta, si un enlace falla no inhabilita todo el sistema. Otra gran ventaja es la privacidad o la seguridad. Una de sus grandes desventajas es el costo de instalación ya que requiere mucho cable, a no ser que sea inalámbrica (Vea Figura 1.3)

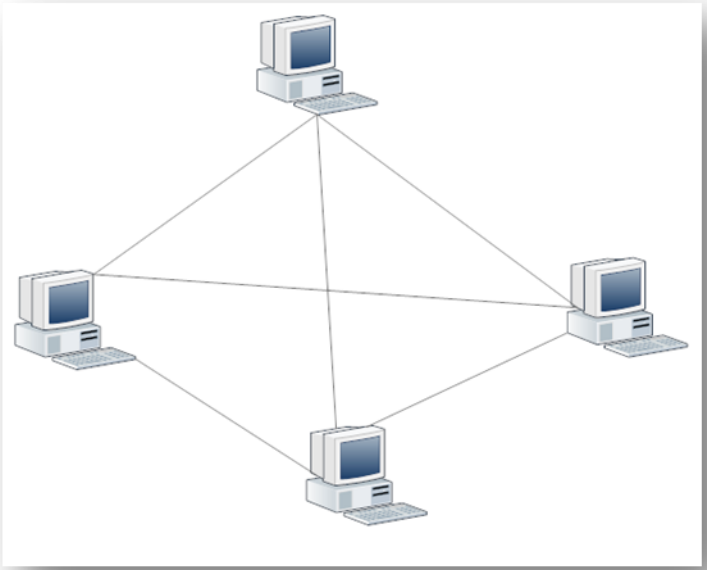


Figura 1.3 Topología en Malla.

b) *Topología en Estrella*. Cada dispositivo solamente tiene un enlace punto a punto dedicado a un controlador central, comúnmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí. A diferencia de la topología en malla, la topología en estrella no permite el tráfico directo de dispositivos. El dispositivo central actúa como un intercambiador: si un dispositivo quiere enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final. Es una topología barata y cada dispositivo necesita solo un enlace y un puerto de entrada y salida para conectarse a cualquier número de dispositivos. Es de fácil instalación y no se requiere de tanto material, el único inconveniente es que si falla el dispositivo central se pierde la comunicación entre los demás equipos. (Vea Figura 1.4)

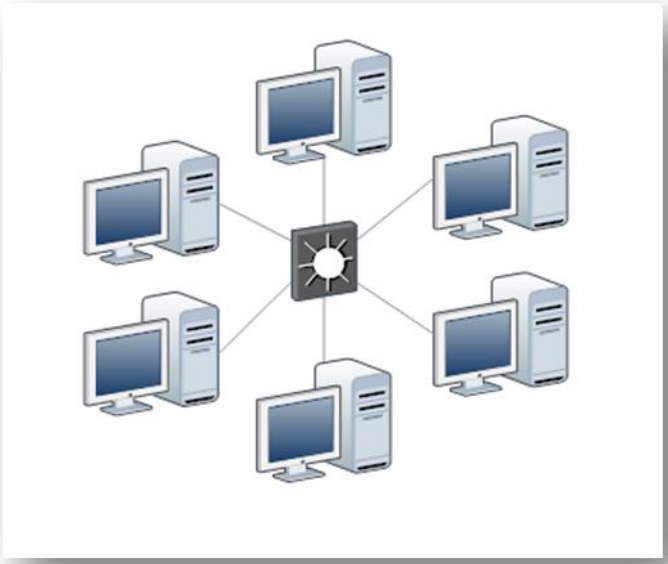


Figura 1.4 Topología en Estrella.

c) *Topología en árbol*. Es una variante de la estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al dispositivo central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central. El concentrador central del árbol es un concentrador activo, el cual contiene un repetidor que regenera los patrones de bits

recibidos antes de retransmitidos. Retransmitir las señales de esta forma amplifica su potencia e incrementa la distancia a la que puede viajar la señal. Como desventajas de esta topología se observa la medida de cada segmento viene determinada por el tipo de cable utilizado, si se viene abajo el segmento principal todo el segmento se viene abajo y es más difícil de configurar. (Vea Figura 1.5)

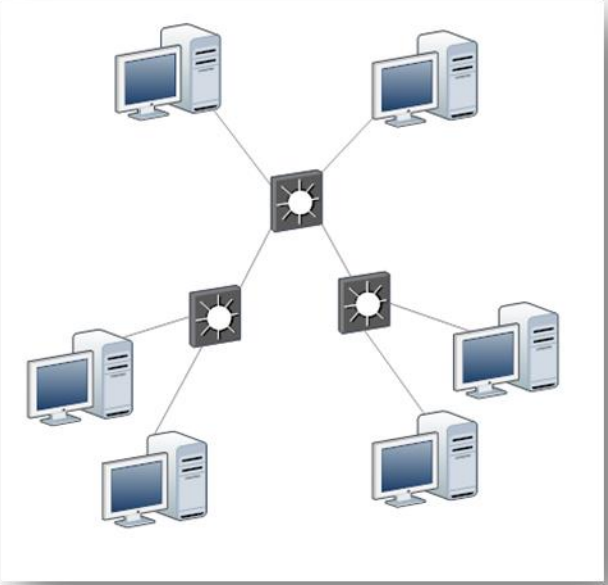


Figura 1.5 Topología en Árbol.

d) *Topología en bus.* Una topología de bus es multipunto, por lo que pueden estar conectadas muchas máquinas a la vez. Un cable largo actúa como eje central llamado comúnmente backbone que conecta todos los dispositivos en la red. De esta forma todos los dispositivos conectados comparten el mismo canal para comunicarse entre sí y para conectar cada terminal al backbone se utilizan cables llamados drop que son conectados con conectores tipos t. Dentro de sus ventajas es de fácil instalación, facilidad de crecimiento y su simplicidad en la arquitectura.

Desventajas de la topología en bus son: toda la red dejaría de funcionar si hubiera una ruptura en el cable principal, se requieren unos dispositivos llamados terminadores, es difícil detectar un error cuando toda la red cae y no se debe utilizar como única solución en un gran edificio. (vea Figura 1.6)

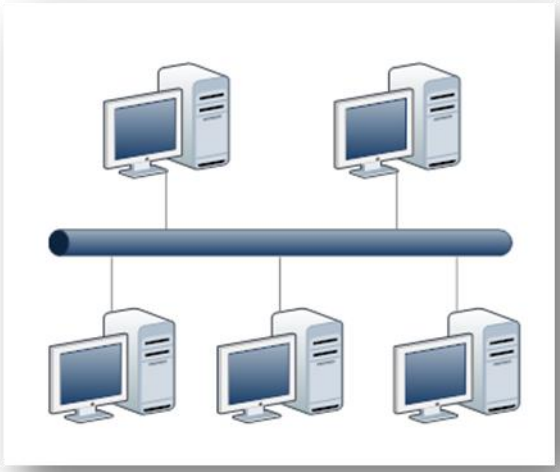


Figura 1.6 Topología en bus.

e) *Topología en anillo.* Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia. Dentro de sus ventajas se tiene la simplicidad en la arquitectura y facilidad de fluidez de datos y dentro de sus desventajas la longitud de sus canales y el canal se degrada a medida que la red se expande. (Vea Figura 1.7)

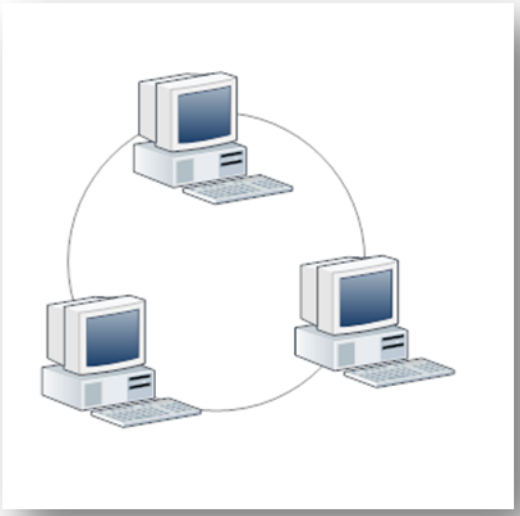


Figura 1.7 Topología en Anillo.

6. **Dispositivos de una red.**

En una red de computadoras es de suma importancia una variedad de componentes que gracias a sus funciones permiten materializar los conceptos de interconexión de dispositivos, a continuación se mencionan los más importantes:

a) **NIC (Network Interface Card-Tarjeta de Interfaz de Red).**Una tarjeta de interfaz de red comúnmente conocida como NIC, es un dispositivo que permite a las computadoras conectarse a una red LAN (Local Area Network-Red de Área Local). Las máquinas en red se comunican unas con otras usando un protocolo o un lenguaje en común para transmitir paquetes de datos entre diferentes máquinas, conocidas como nodos. Las tarjetas de red actúan como enlace entre una PC y una red para recibir y enviar información (Figura 1.8).

Figura 1.8 Tarjeta de red.

b) Switch. Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI (Open System Interconnection-Interconexión de Sistema Abierto) y reenvía los paquetes con base en la dirección MAC (Media Access Control-Control de acceso al medio) (Figura 1.9).

Figura 1.9 Switch.

c) Router. Un router es un dispositivo de propósito general diseñado para segmentar la red con la idea de limitar tráfico broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN. El router opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el router distingue entre los diferentes protocolos de red (Figura 1.10).

Figura 1.10 Router.

d) Host o nodo. Es el dispositivo final que está conectado en una red y posee una dirección IP para que se lleve a cabo el intercambio de información como lo es la transferencia de archivos, de voz, de datos, video etcétera. El usuario utiliza este dispositivo como interfaz con la red y para que se comunique con otros usuarios. (Vea la Figura 1.11)

Figura 1.11 Computadora Personal (Host).

1.2.8 Principales Estándares

La ISO (International Organization for Standardization-Organización Internacional de normalización) define a los estándares de la siguiente forma “Son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito”. Por lo tanto, un estándar de telecomunicaciones es un conjunto de normas y recomendaciones técnicas que regula la transmisión en los sistemas de comunicaciones. Los estándares deben ser documentados para que sean difundidos y captados de igual manera por las entidades o personas que los vayan a utilizar.

Existen tres tipos de estándares: de facto, de jure y los propietarios. Los estándares de facto son aquellos que tienen una alta penetración y aceptación en el mercado, pero aún no son oficiales. Un estándar de jure es definido por grupos u organizaciones oficiales. Y los propietarios que son propiedad absoluta de una corporación o entidad y su uso todavía no logra introducirse en el mercado.

Hay dos tipos de organizaciones que definen estándares: las organizaciones oficiales y los consorcios de fabricantes. El primer organismo está integrado por consultores independientes, integrantes de departamentos o secretarías de estado de diferentes países. Los consorcios de fabricantes están integrados por compañías fabricantes de equipo de comunicaciones o desarrolladores de software que conjuntamente definen estándares para que sus productos entren al mercado de las telecomunicaciones y redes.

Dentro de las organizaciones de estándares están:

a) ITU (International Telecommunication Union-Unión Internacional de Telecomunicaciones). Es el organismo especializado de la Organización de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

b) IEEE (Institute of Electrical and Electronics Engineers-Instituto de Ingenieros Eléctricos y Electrónicos). Fundada en 1884, es una sociedad establecida en los Estados Unidos de Norteamérica que desarrolla estándares para las industrias eléctricas y electrónicas, particularmente en el área de redes de datos.

c) ISO. Es una organización no gubernamental establecida en 1947, tiene representantes de organizaciones importantes de estándares alrededor del mundo y actualmente conglomera a más de 100 países. La misión de ISO es promover el desarrollo de la estandarización y actividades relacionadas con el propósito de facilitar el intercambio internacional de bienes y servicios y para desarrollar la cooperación en la esfera de la actividad intelectual, científica, tecnológica y económica.

Día con día las organizaciones oficiales y los consorcios de fabricantes están gestando estándares con el fin de optimizar la vida diaria. En la industria global de redes, los fabricantes que puedan adoptar los estándares a sus tecnologías serán los que predominen en el mercado. Los fabricantes tienen dos grandes razones para invertir en estándares. Primero, los estándares crean un nicho de mercado; segundo, los fabricantes que puedan estandarizar sus propias tecnologías podrán entrar más rápido a la competencia.

La tecnología Ethernet es relativamente barata, razonablemente rápida y popular en tecnologías LAN. Bob Metcalfe y D.R. Boggs integrantes de Xerox PARC fueron los encargados de diseñar esta tecnología a principios de 1972 y las especificaciones basadas en este trabajo aparecieron en el estándar 802.3 de la IEEE en 1980.

Especificada en el estándar IEEE 802.3, una LAN Ethernet usa típicamente cable coaxial o categorías especiales de cables de par trenzado. Ethernet también es utilizado en LAN's inalámbricas. Ethernet usa el método de acceso CSMA/CD para el manejo de peticiones simultáneas. El sistema Ethernet más comúnmente instalado es el llamado 10BASE-T y provee una velocidad de transmisión de 10 Mbps. Los dispositivos en una red Ethernet son conectados al cable y compiten por el acceso usando el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection-Acceso Múltiple por Detección de Portadora con Detección de Colisiones). Fast Ethernet o 100BaseT proporciona velocidades de transmisión a 1000 Mbps y es típicamente usada para un sistema de cableado vertical, con soporte para estaciones

de trabajo con tarjetas 10BASE-T. Gigabit Ethernet proporciona aun un nivel más alto de soporte de backbone a una velocidad de 1000megabits por segundo. 10-Gigabit Ethernet trabaja a una velocidad de 10 billones Mbps. Además de Ethernet, existen otros estándares que surgen del estándar 802 de la IEEE que se muestran en el siguiente apartado.

Estándares IEEE

IEEE desarrolló un grupo de estándares, los cuales se muestran en la tabla 1.1

Tabla 1.1 Estándares 802.x.

Estándar	Uso
IEEE 802.1	Estándar relacionado a la administración de la red
IEEE 802.2	Estándar general para la capa de enlace de datos en el modelo de referencia OSI. La IEEE divide esta capa en dos subcapas- Control de enlace lógico (LLC - logical link control) y la capa de acceso al medio (MAC– Media Acces Control). La capa MAC varía para diferentes tipos de redes y es definida por los estándares IEEE 802.3 a través del IEEE 802.5
IEEE 802.3	Define la capa MAC para redes de tipo bus que usan CSMA/CD. Este protocolo es la base de este estándar
IEEE 802.4	Define la capa MAC para redes de tipo bus que usan el mecanismo de envío de tokens
IEEE 802.5	Define la capa MAC para redes Token Ring
IEEE 802.6	Estándar para redes de Area Metropolitana (MAN)

1.1.3 Modelo de Referencia OSI

El Modelo de Sistema de Interconexión Abierto (OSI-Open System Interconnection) es un modelo de referencia desarrollado por ISO en 1984 como una estructura conceptual de estándares para la comunicación en la red entre diferentes equipos y aplicaciones. Es considerado el modelo principal para el intercambio de información entre redes de computadoras y cualquier elemento de una red de datos.

La gran mayoría de los protocolos de comunicación de red usados en la actualidad tiene una estructura basada en este modelo, el cual define el proceso de comunicación en 7 capas, dividiendo tareas complicadas de traslado de información entre máquinas en red en siete pequeñas, permitiendo grupos de tareas más manejables. Una tarea o grupo de ellas están asignados en cada una de estas siete capas del modelo OSI. Cada capa está razonablemente definida por sí misma, por lo que cada tarea asignada a cada capa puede ser implementada independientemente, lo que permite ofrecer una solución de encapsulamiento a cada capa, de manera que al ser actualizada o modificada no afecte al funcionamiento de las demás capas.

Los principales beneficios del Modelo OSI son:

a) Ayuda a los diseñadores de red a entender la gran estructura de una red.

b) Ayuda a los diseñadores de red para que los elementos de hardware y software trabajan de manera conjunta y se lleve a cabo el intercambio de información.

c) Facilita la resolución de problemas separando la red en partes pequeñas que son más manejables.

d) Define reglas que los profesionales de computación pueden usar para comparar las relaciones de funcionamiento básico en diferentes redes.

e) Ayuda a los usuarios a entender nuevas tecnologías mientras son desarrolladas.

El modelo OSI se divide en 7 capas como se ve en la figura 1.12, las cuales se explican a continuación:

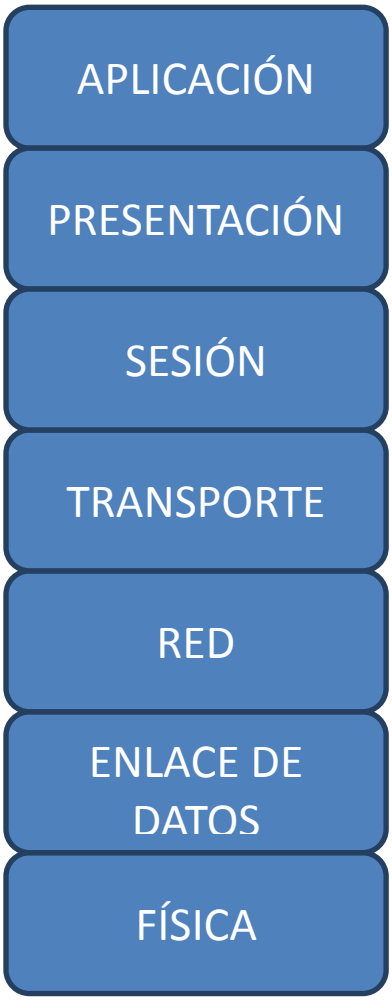


Figura 1.12 Capas del Modelo OSI.

1. **Capa Física**. Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (cable coaxial, cable de par trenzado, fibra óptica, radio, microondas); características del medio (tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria).

2. **Capa de Enlace de Datos.** Es la capa responsable de la transferencia fiable de información a través de un circuito de transmisión de datos.El objetivo del nivel de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a conexión). Para lograr este objetivo tiene que montar bloques de información (llamados tramas en este nivel), dotarles de una dirección de nivel de enlace, gestionar la detección o corrección de errores, y ocuparse del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento).Cuando el medio de comunicación está compartido entre más de dos equipos es necesario arbitrar el uso del mismo. Esta tarea se realiza en el subnivel de acceso al medio.

3. **Capa de Red.** Es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

4. **Capa de Transporte.** Encargada de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo. La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina destino.

5. **Capa de Sesión.** Esta capa establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

6. **Capa de Presentación.** El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible. Esta capa es la primera en trabajar más en el contenido de la comunicación que en cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras, es un traductor.

7. **Capa de Aplicación.** Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones, el número de protocolos crece sin parar. Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

Modelo TCP/IP

La arquitectura TCP/IP (Transmission Control Protocol/Internet Protocol-Protocolo de control de Transmisión/Protocolo de Internet) no sigue exactamente el modelo de referencia OSI. Desafortunadamente no existe un acuerdo universal de cómo describir TCP/IP en un modelo de capas. En TCP/IP se tienen menos capas comparado con el modelo de referencia OSI, en total se tienen 4 capas para el modelo TCP/IP.

La arquitectura TCP/IP omite algunas características que se encuentran en el modelo de referencia OSI, combina características de algunas capas adyacentes de OSI y deja otras capas aparte. La estructura de la capa 4 de TCP/IP incorporada como información es transmitida a las aplicaciones de la capa física de red. Cuando la información es enviada, cada capa trata toda la información recibida de las capas superiores como datos, agrega una cabecera de control de información y la pasa a la capa inferior. Cuando los datos son recibidos, se efectúa el procedimiento contrario, cada capa procesa y retira las cabeceras antes de pasar la información a las capas superiores.

La función de cada capa del modelo TCP/IP se muestra a continuación:

1. **Capa de Aplicación.** La capa de aplicación TCP/IP agrupa las funciones de la capa de aplicación, presentación y sesión del modelo de referencia OSI. Es por ello que cualquier proceso en la capa superior de la arquitectura TCP/IP es llamada aplicación. En TCP/IP sockets y puertos son usados para describir el camino por el cual las aplicaciones se comunican. La mayoría de los niveles de protocolos son asociados con uno o más puertos.

2. **Capa de Transporte.** En TCP/IP existen dos protocolos de la capa de transporte que son TCP (Transmission Control Protocol–Protocolo de Control de Transmisión) que garantiza el envío de información y UDP (User Datagram Protocol–Protocolo de Datagrama de Usuario) que envía datagramas sin esperar respuesta de transferencia de información correcta. Ambos protocolos son de gran importancia y tienen múltiples aplicaciones.

3. **Capa de red.** El protocolo de internet (IP-Internet Protocol) es el protocolo principal en la capa de red de TCP/IP, las comunicaciones tanto en las capas superiores como las capas inferiores deben viajar a través de IP, así como recorrer la pila de protocolos TCP/IP. En esta capa también existen varios protocolos de red como ICMP (Internet Control Message Protocol-Protocolo de Mensajes de Control de Internet) que facilitan la administración del proceso de encaminamiento.

4. **Capa de acceso a la red.** En la arquitectura TCP/IP la capa de enlace de datos y la capa física están normalmente agrupadas para formar una sola capa llamada capa de acceso a la red. La capa física, la cual define las propiedades de la comunicación con el hardware aunque no muy a menudo interactúa directamente con los protocolos TCP/IP en la capa superior (Capa de red).

Después de haber conocido el modelo de referencia OSI y el modelo TCP/IP Se muestra un diagrama comparativo entre los dos modelos que se ven en la Tabla 1.4.

Tabla 1.4 Comparación entre el modelo OSI y el modelo TCP/IP.

MODELO DE REFERENCIA OSI	MODELO TCP/IP
APLICACIÓN	APLICACIÓN
PRESENTACIÓN	
SESIÓN	
TRANSPORTE	TRANSPORTE
RED	RED
ENLACE DE DATOS	ACCESO A LA RED
FÍSICA	

1.1.4 Redes Inalámbricas.

Las redes inalámbricas (redes wireless en inglés, que se refiere a sin cables) como su nombre lo indica, son redes que funcionan sin la necesidad de usar algún tipo de cableado, su funcionamiento se basa en ondas de radio que viajan a través del aire. Esta tecnología es muy utilizada en lugares de difícil acceso, zonas rurales o en edificios antiguos en donde no es posible o no se tiene permitido cablear. Este tipo de redes permite a los usuarios estar conectados en cualquier lugar sin la necesidad de muchas configuraciones y sin la necesidad de algún cable, esta tecnología es una de las más usadas para dispositivos móviles como tabletas-PC, celulares, netbooks y notebooks.

Algunas tecnologías de redes inalámbricas son:

a) **Wireless:** En inglés su significado es sin cables y se denomina así a los dispositivos que no utilizan cables para realizar el envío y la recepción de datos.

b) **Wi-Fi:** Abreviatura del término inglés Wireless Fidelity. Es el término que se refiere también a una LAN inalámbrica (WLAN) de alta frecuencia[5].

c) **WLAN (Wireless Local Area Network):** Es una red LAN que utiliza ondas de radio de alta frecuencia en lugar de cables para comunicar y transmitir datos.

d) **Bluetooth:** Tecnología y protocolo de conexión entre dispositivos inalámbricos. Incluye un chip específico para comunicarse en la banda de frecuencia comprendida entre 2402 y 2480 GHz con un alcance máximo de 10m y tasas de transmisión de datos de hasta 721 Kbps[6].

e) **Zigbee:** Es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal area network, WPAN). Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

Aun con las grandes ventajas que las tecnologías proporcionan, las redes cableadas no alcanzan a cubrir todos los requerimientos nuevos que han surgido con los avances de la tecnología, como es poder obtener información al instante a través de algún dispositivo mientras se viaja o si se está en una obra civil.

[5] Para mayor información véase apéndice B Tecnologías inalámbricas.
[6] Para mayor información véase el apéndice B Tecnologías inalámbricas

Es por ello que para poder cubrir esa parte surgieron las redes inalámbricas que dentro de su principal ventaja es precisamente la movilidad. Esto permite que muchos usuarios y empleados de alguna empresa accedan de forma remota a sus archivos, trabajos y recursos sin la necesidad de permanecer en todo momento en una ubicación fija como una oficina.

Las redes inalámbricas tienen como principales características:

a) Instalación más simple.

b) Alta escalabilidad.

c) Facilidad de Administración.

d) Al no tener cables se pueden adaptar a cualquier estructura como edificios antiguos.

e) No existen cruces de oficinas con cableado innecesario.

f) Se pueden usar en cualquier lugar donde esté habilitado el servicio.

Dentro de las desventajas se pueden enumerar las siguientes:

a) La velocidad de conexión está limitada ya que no superan los 54Mbps mientras que las redes cableadas ya rebasan los 100Mbps.

b) Otro punto débil es la seguridad debido a que muchas redes inalámbricas en la actualidad no ofrecen mecanismos adecuados que permitan el envío seguro de la información, ocasionando pérdida de la misma así como robo.

c) Las redes inalámbricas son susceptibles o propensas a interferencias y esto es debido al rango de señal a la que trabajan (en su mayoría 2.4 MHz) suelen ser interferidas por dispositivos de uso común en cualquier casa y oficina, como teléfonos inalámbricos que utilicen el mismo rango.

Para establecer una conexión de tipo inalámbrica es necesario realizar dos cosas de manera global: instalar placas de red inalámbricas en cada una de las PC y configurar un punto de acceso (Access point) (Figura 1.13). Un access point es un dispositivo que permite ampliar el alcance de una señal entre dos o más dispositivos interconectados repitiéndola para que se lleve a cabo la transmisión de la información. Por lo general se coloca en un espacio en donde se tenga cobertura de ondas de radio deseadas por medio de las cuales se accede a una red WLAN a través de un adaptador que no es otra cosa que una tarjeta de red muy similar a una NIC, con la diferencia que trabaja

con señales de radio, esta tarjeta debe estar conectada al dispositivo para poder recibir las señales que provienen del exterior y funcionar como una interfaz entre el sistema operativo y las ondas que contienen la información mediante una antena.

En una WLAN los Access point (switches inalámbricos) reciben información, la almacenan y la transmiten entre los dispositivos que acceden a él. Si solo se tiene un Access point, éste soportará un pequeño grupo de usuarios y funcionará en un rango de 30 a varios cientos de metros también, dependiendo si se cuenta con antenas amplificadoras o no.

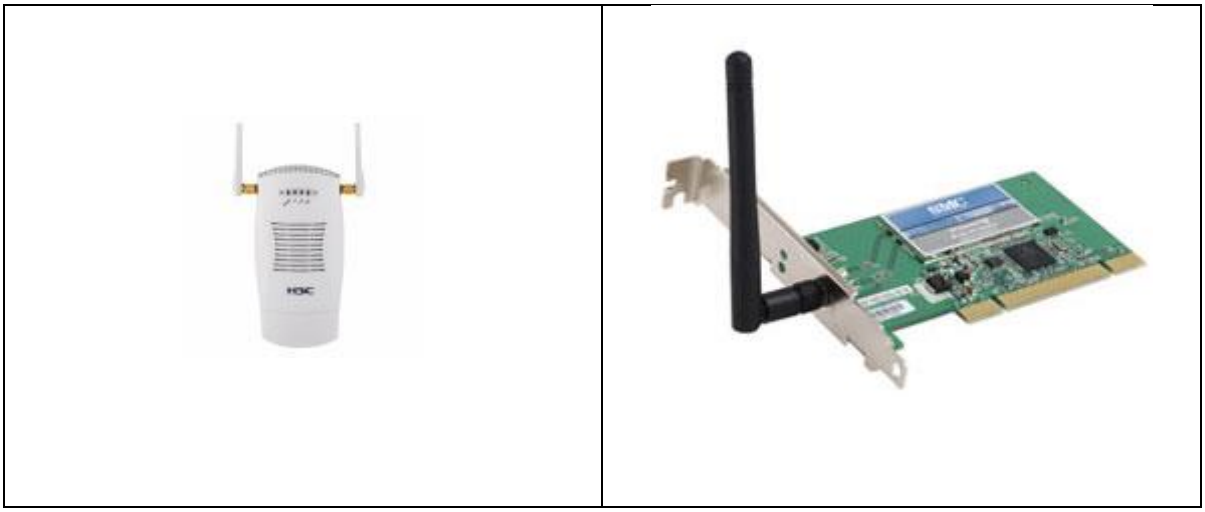


Figura 1.13 Izquierda-Access Point, Derecha-Tarjeta de red Inalámbrica.

1.3 Seguridad Informática

Con los avances de la tecnología en las redes de datos ha aumentado la preocupación del resguardo de un activo muy preciado para el ser humano ya sea en el hogar o en el trabajo y refiriéndose a grandes empresas donde tienen la responsabilidad del resguardo de la misma, se trata de la tan preciada información.

1.2.1 Definición de Seguridad Informática

El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a los que haga referencia. La seguridad es un estado de ánimo, una sensación, una cualidad intangible. Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria. En cuanto a la seguridad de la información son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la

información, buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. Por último, la seguridad informática son todas aquellas actividades, técnicas, aplicaciones y dispositivos que buscan proteger la integridad, confidencialidad y disponibilidad de la información (Figura 1.14).

1.14 Seguridad Informática.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático no tomando en cuenta otros factores que existan alrededor como algún fallo eléctrico, efectos de la naturaleza o personas no autorizadas en el lugar de trabajo. A continuación se muestran aspectos importantes que hay que tomar en cuenta en la seguridad informática para poder proteger la información.

1.2.2 Amenazas

Con la definición anterior surge una pregunta muy importante ¿Qué podría afectar la información? De aquí surge el concepto de amenaza. Una amenaza es todo aquello que intenta, puede o pretende destruir y proviene de diversas fuentes:

a) Humanos. Es cuando una amenaza surge de la ignorancia en el manejo de la información, por descuido, negligencia, inconformidad.

b) Errores de Hardware. Se refiere a un mal funcionamiento de los dispositivos donde se almacena la información y donde podría haber una falla eléctrica, sobrecalentamiento de algún componente o un maltrato físico al equipo de cómputo.

c) Errores en la red. Una amenaza se presenta de manera física cuando no se calcula bien el flujo de información que va a circular por el canal de comunicación o cuando de repente se desconecte el cable por alguna razón y de manera lógica algún software diseñado para monitorear, obtención de contraseñas, espionaje etcétera, falle.

d) Problemas de tipo lógico. Cuando un diseño bien elaborado de un mecanismo de seguridad se implementa mal por lo que no cumple con las especificaciones del diseño.

e) Desastres. Es una amenaza que no se puede erradicar y es muy difícil de controlar debido a que es demasiado variable y sus efectos pueden ser los mínimos o pueden a llegar a ser devastadores, provienen de las fuerzas naturales que son altamente o completamente impredecibles.

1.2.3 Vulnerabilidades

Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo, es decir, las vulnerabilidades representan las debilidades o aspectos atacables en el sistema informático. Por ejemplo, una vulnerabilidad muy común es usar una contraseña no segura, poniendo palabras que están en algún diccionario, nombres de artistas, películas o alguna palabra conocida.

Las vulnerabilidades de forma similar a las amenazas se pueden clasificar en:

a) Físicas. Debilidad en el entorno de trabajo.

b) Natural. La afectación que puede haber ante algún desastre natural.

c) Hardware. No darle el mantenimiento adecuado a los equipos de cómputo desde el mantenimiento preventivo así como el correctivo.

d) Software. No tener las herramientas adecuadas de protección además de bajar las actualizaciones críticas de las mismas y del sistema operativo.

e) De red. Al crecer el uso de la red, se corre el riesgo de que alguien pueda acceder al equipo de trabajo con mayor facilidad.

f) Humana. Una de las vulnerabilidades más comunes, es aquí donde se comenten más errores debido a la desinformación o a la poca ética de alguna persona, es una de las vulnerabilidades que se debe cubrir lo más que se pueda.

1.2.4 Servicios de seguridad

Algo que debe tomarse en cuenta para garantizar la seguridad son los ataques, es importante analizar de dónde provienen, qué vulnerabilidad aprovecharon y qué efectos tienen o pueden llegar a tener.

Un ataque es la consumación de una amenaza aprovechando una o varias vulnerabilidades. Un ataque puede ser activo, en el cual se modifica o borra la información o pasivo, cuando el atacante solo ve la información sin modificarla, únicamente observa, escucha, obtiene o monitorea dicha información, este tipo de ataque es el más difícil de detectar.

Una vez analizado esto, es necesario aplicar una mejora de seguridad a un sistema de información y el flujo de la misma en la organización, es aquí donde surgen los servicios de seguridad que utilizan uno o más mecanismos de seguridad para resguardar la información.

Formalmente un servicio de seguridad "es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismo de seguridad para proveer el servicio"[7].

Una clasificación muy utilizada de los servicios de seguridad es la siguiente:

a) Confidencialidad. La confidencialidad en la información se refiere a que alguien que no esté autorizado pueda ser capaz de tener acceso a la misma, los servicios de confidencialidad buscan que no se lea, copie, descubra o se modifique la información sin autorización y que nadie pueda interceptar las comunicaciones entre entidades. Todo esto lo hace a través de métodos cifrados basados en la criptografía que aseguren que el descubrimiento no autorizado de la información sea computacionalmente imposible.

b) Autenticación. Se refiere a la acción de verificar la identidad de alguien a través de una contraseña, una firma o una huella digital que permita saber que la persona está autorizada a tener acceso a la información. El servicio de autenticación trata de asegurar que una comunicación sea auténtica, que las entidades que quieran comunicarse sean las correctas y que no haya una tercera entidad no autorizada.

[7] Definición obtenida del libro Fundamentos de seguridad informática de la Maestra María Jaquelina López Barrientos y la Maestra Cintia Quezada Reyes

c) Integridad. El tener la información tal y como se diseñó o elaboró es la parte fundamental de la integridad y si es necesario hacer alguna modificación, solo las personas autorizadas pueden hacerlo. Es por ello que el servicio de integridad ayuda a detectar cuando la información sufre un cambio malintencionado o por entidades no autorizadas. Existen dos tipos de servicios de integridad: el de contenido que provee pruebas de que el contenido no ha sido alterado o modificado por inserción o supresión y de secuencia del mensaje en donde se proporcionan pruebas de que el orden de una secuencia de mensajes ha sido mantenida durante su transmisión.

d) No repudio. Previene a los emisores o a los receptores de negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. El servicio de no repudio permite hacer este tipo de comprobaciones como lo es el no repudio de origen, no repudio de envío, no repudio de presentación, no repudio de transporte y no repudio de recepción.

e) Control de acceso. Es la forma en que se limitan los recursos de una red para que solo las personas autorizadas tengan acceso directo a la información. El servicio de control de acceso proporciona los diferentes niveles de seguridad necesarios para garantizar el correcto uso de la información.

f) Disponibilidad. La información puede accederse en el momento que se requiera y tantas veces como sea necesario por lo que el servicio de seguridad de la disponibilidad se encarga de que haya los respaldos necesarios en diferentes lugares por si ocurre algún imprevisto.

1.2.5 Mecanismos de seguridad

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático, éstos permiten implementar uno o varios servicios de seguridad.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

1. Clasificación según su función:
   a) Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
   b) Detectores: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.
   c) Correctivos: Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.
   d) Disuasivos: Reducen la probabilidad de un ataque deliberado.

2. Clasificación según el servicio que implementan:
   a) Integridad.
   b) Confidencialidad.
   c) Autenticación.
   d) No repudio.
   e) Disponibilidad.
   f) Control de acceso.

3. Clasificación con base en su necesidad:
   a) Requeridos. Todos los controles en esta categoría pueden ser definidos con base en una o más reglas escritas. La clasificación de los datos almacenados y procesados en un sistema o red y su modo de operación determinan qué reglas aplicar, y éstas indican cuáles son los controles requeridos.
   b) Discrecionales. Este tipo de controles es elegido por los administradores. En muchos casos los controles requeridos no reducen el nivel de vulnerabilidad a un nivel aceptable, por lo que se deben elegir e implementar este tipo de controles para ajustar el nivel de vulnerabilidad a un nivel aceptable.

1.2.6 Políticas de seguridad

La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

La política define la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. La política especifica qué propiedades de seguridad el sistema debe proveer. De manera similar, la política define la seguridad informática para una organización, especificando tanto las propiedades del sistema como las responsabilidades de seguridad de las personas.

De aquí surgen los principios fundamentales que a través de leyes, reglas y prácticas reflejan las metas y situaciones de la organización, a continuación se mencionan cuáles son esos principios.

Principios fundamentales:

1. Responsabilidad individual. Las personas son responsables de sus actos.
2. Autorización. Son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.
3. Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.
4. Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.
5. Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros, donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.
6. Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

7. Reducción de Riesgo: esta estrategia debe reducir el riesgo a un nivel aceptable, haciendo que el costo de la aplicación sea proporcional al riesgo.

CAPÍTULO 2
REDES ZIGBEE
(IEEE 802.15.4)

2.1 Panorama general (IEEE 802.x y 802.15).

Las redes inalámbricas de corto alcance permiten la comunicación entre diferentes dispositivos sin la necesidad de algún tipo de instalación especial, todo esto está especificado en el estándar 802.15 que se utiliza para redes WPAN (Wireless Personal Area Network-Red Inalámbrica de Área Personal) como lo es bluetooth, que es una especificación industrial para este tipo de redes que posibilita la transmisión de voz y datos mediante un enlace por radiofrecuencia en la banda ISM (Industrial, Scientific and Medical-Industrial –Industrial, Científica y Médica Industrial) de los 2.4GHz, por lo que solo basta que el dispositivo cuente con esta tecnología para poder habilitar una red pequeña de acuerdo con las necesidades que se tengan en ese momento. Es por ello que este tipo de tecnología en redes inalámbricas ha ido creciendo y han sido desarrollados otros apartados de este estándar como lo es el apartado 802.15.4 que surge de la necesidad de tener una gran cantidad de dispositivos conectados en red para distancias cortas y para dispositivos electrónicos que consumen poca energía y no se transmita demasiada información.

ZigBee se basa en este estándar, su nombre se deriva de los patrones erráticos comunicativos que hacen muchas abejas entre las flores durante la recolección de polen por lo que este término se refiere a redes invisibles en un entorno totalmente inalámbrico.

ZigBee se ha desarrollado para satisfacer la creciente demanda de capacidad de red inalámbrica entre varios dispositivos de baja potencia. En la industria, ZigBee se está utilizando para la próxima generación de fabricación automatizada, con pequeños transmisores en cada dispositivo, lo que permite la comunicación entre dispositivos a una computadora central.

Para llevar a cabo este sistema, un grupo de trabajo llamado Alianza ZigBee (ZigBee Alliance) formado por varias industrias sin fin de lucro, como lo son Invensys, Mitsubishi, Philips y Motorola están desarrollando el estándar conjuntamente con la IEEE para asegurar una integración completa y operativa al formar un sistema estándar de comunicaciones que utilice ondas de radio y que sea bidireccional, para usarlo dentro de dispositivos de automatización hogareña (domótica), de edificios (inmótica), control industrial, periféricos de PC y sensores médicos. Los miembros de esta alianza justifican el desarrollo de este estándar para cubrir el vacío que se produce por debajo de bluetooth[8].

Para conocer un poco más cómo está constituido este estándar se verá a continuación su arquitectura y cómo es que transfiere información en las diferentes capas que maneja.

[8] Para mayor información véase el apéndice B tecnologías Inalámbricas

2.2 Arquitectura

ZigBee está basado en una arquitectura que se asemeja al modelo de referencia OSI con la excepción de que solo define aquellas capas relevantes que proporcionan la funcionalidad para el ámbito de este tipo de redes. En la Figura 2.1 se muestra la arquitectura de ZigBee y cómo es que se basa en el estándar 802.15.4.

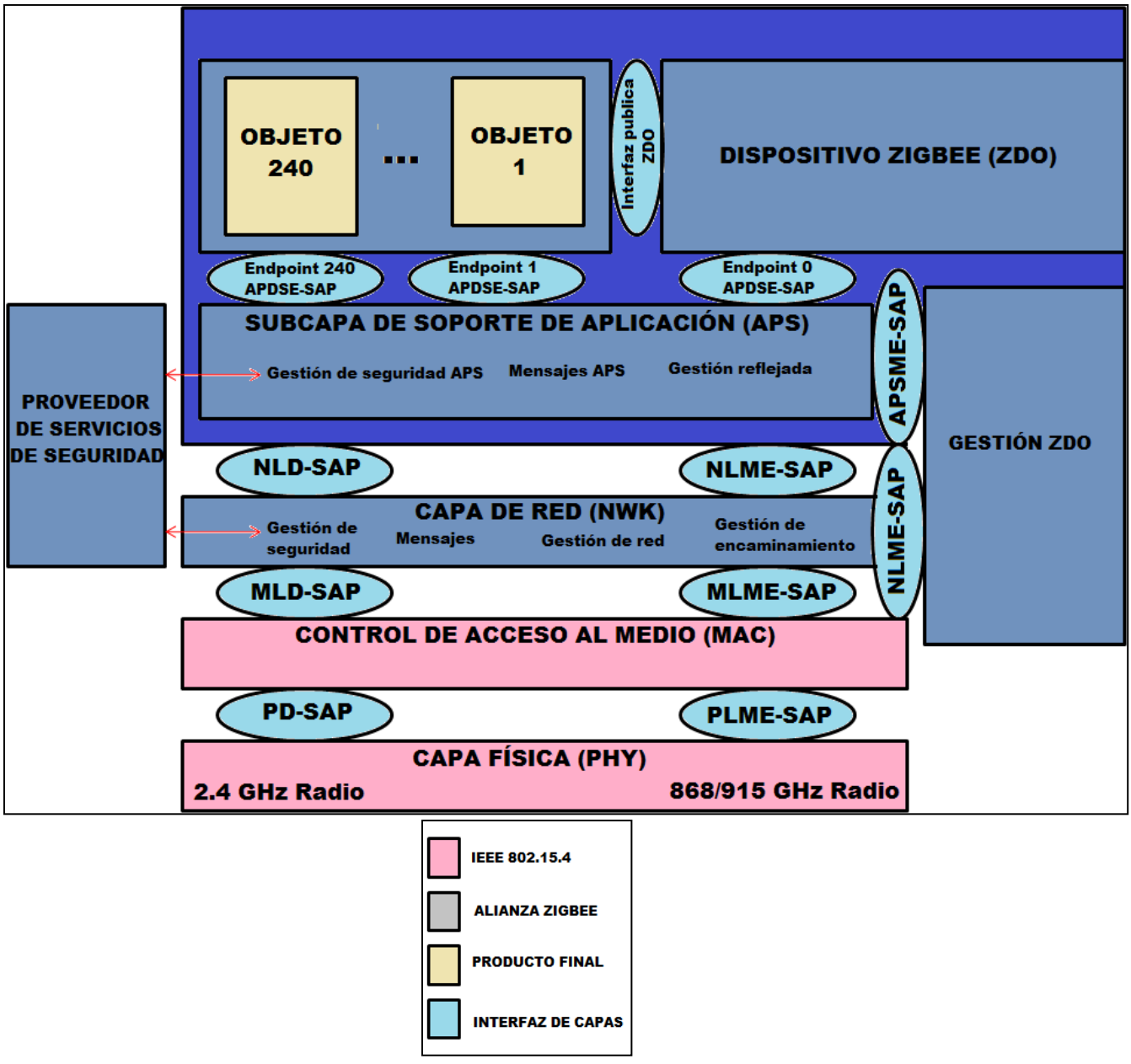


Figura 2.1 Modelo de la arquitectura ZigBee.

La pila ZigBee está formada por un grupo de bloques llamado capas. Cada capa utiliza un grupo específico de servicios de capas superiores: una entidad de datos provee un

servicio de transmisión y una entidad de administración que proporciona los servicios restantes. Cada entidad de servicio muestra una interfaz a la capa superior a través de un SAP (Service Access Point - Punto de Acceso de Servicio), y cada SAP soporta un cierto número de primitivas de servicio para alcanzar la funcionalidad requerida. El estándar IEEE 802.15.4 define las dos capas inferiores: la capa física (PHY - Physical Layer) y la subcapa de control de acceso al medio (MAC).

Este estándar se enfoca principalmente en el desarrollo de estándares para redes tipo PAN (Personal Area Network - Redes de Área Personal) o HAN (Home Area Network - Redes de Área Doméstica) que son redes inalámbricas de corta distancia. Al igual que bluetooth o ZigBee, el 802.15 permite que dispositivos inalámbricos portátiles como PCs, PDAs (Personal Digital Assistant - Asistente Digital Personal), teléfonos, sensores y otros dispositivos puedan comunicarse e interoperar uno con el otro. El estándar 802.15.4, por su parte, es un estándar que define el nivel físico y el control de acceso al medio de redes inalámbricas de área personal con tasas bajas de transmisión de datos (LR-WPAN - Low Rate Wireless Personal Area Network - Red de Área Personal Inalámbrica de Bajo Consumo). El propósito del estándar es definir los niveles de red básicos para dar servicio a un tipo específico de red inalámbrica de área personal (WPAN) centrada en la habilitación de comunicación entre dispositivos con bajo costo y velocidad. Se enfatiza el bajo costo de comunicación con nodos cercanos y sin infraestructura o con muy poca, para favorecer aún más el bajo consumo. A continuación se presentan los valores característicos del estándar en la tabla 2.1.

Tabla 2.1 Valores característicos de ZigBee.

Bandas de Frecuencia – Rango de Transmisión de Datos	868MHz – 20kb/s 915MHz – 40kb/s 2.4 GHz – 250kb/s
Alcance	10 - 20 m
Latencia	<15 ms
Canales	868/915 MHz: 11 Canales 2.4 GHz: 16 Canales
Modos de direccionamiento	64bits IEEE
Canal de acceso	CSMA-CA
Seguridad	128 AES
Red	Hasta 2^{64} dispositivos
Rango de Temperatura	-40 a 85°C

Para comprender un poco más el estándar es necesario definir más detalladamente las capas que lo componen y se tiene las siguientes capas:

a) Capa física. La capa física es la capa de red más básica, proporcionando únicamente los medios para transmitir bit a bit sobre un enlace de datos físico conectado a nodos de red. Las cadenas de bits pueden ser agrupadas en palabras codificadas o símbolos y convertidas a señales físicas, que son transmitidas sobre un medio de transmisión físico. La capa física proporciona una interfaz eléctrica, mecánica y procedimental para el medio de transmisión. En este nivel se especifican las características de los conectores eléctricos, sobre qué frecuencias retransmitir, qué esquema de modulación usar y parámetros de bajo nivel similares.
   El IEEE 802.15.4 ofrece dos opciones de nivel físico (PHY) que se combinan con el Control de Acceso al Medio (MAC) para permitir un amplio rango de aplicaciones en red. Ambas opciones se basan en métodos de secuencia directa de espectro extendido (DSSS - Direct Squence Spread Spectrum) que representan bajos costos de implementación digital en IC (Integrated Circuits - Circuitos Integrados) y ambas comparten la misma estructura básica de paquetes low duty-cycle (ciclo de trabajo) con operaciones de bajo consumo de energía. La principal diferencia entre ambas capas físicas radica en la banda de frecuencias. La PHY de los 2.4 GHz especifica la operación en la banda ISM que está disponible a nivel mundial, mientras que la PHY de los 868/915 MHz especifica operaciones en la banda de 865 MHz en Europa y 915M Hz en la banda ISM en Estados Unidos. Mientras que la movilidad entre países no se emplea para la mayoría de las aplicaciones de redes en las casas, la disponibilidad internacional de la banda de los 2.4 GHz ofrece ventajas en términos de mercados más amplios y costos de fabricación más bajos. Por otro lado, las bandas de 868 MHz y 915 MHz ofrecen una alternativa a la congestión creciente y demás interferencias (como por ejemplo los hornos de microondas) asociadas a la banda de 2.4 GHz además de mayores rangos por enlace debido a que existen menores pérdidas de propagación.

   Una segunda distinción de las características de la PHY es la velocidad de transmisión. La PHY de 2.4GHz permite una velocidad de transmisión de 250 kb/s, mientras que la PHY de los 868/915 MHz ofrece velocidades de 20 kb/s y 40 kb/s respectivamente. Este rango superior de transmisión en la PHY de los 2.4GHz es debido principalmente a un mayor orden en la modulación. Los diferentes regímenes de bits se pueden elegir según la aplicación. Por ejemplo, la baja densidad de datos en la PHY de los 868/915 MHz se puede utilizar para lograr mayor sensibilidad y mayores áreas de cobertura, con lo que se reduce el

número de nodos requeridos para cubrir un área geográfica, mientras que el rango superior de transmisión en la PHY de los 2.4 GHz se puede utilizar para conseguir salidas superiores y de poca latencia.

- Estructura de paquete de Capa Física.

  Para mantener una interfaz común con la MAC, ambas capas PHY comparten una sola estructura de paquete (Figura 2.2).

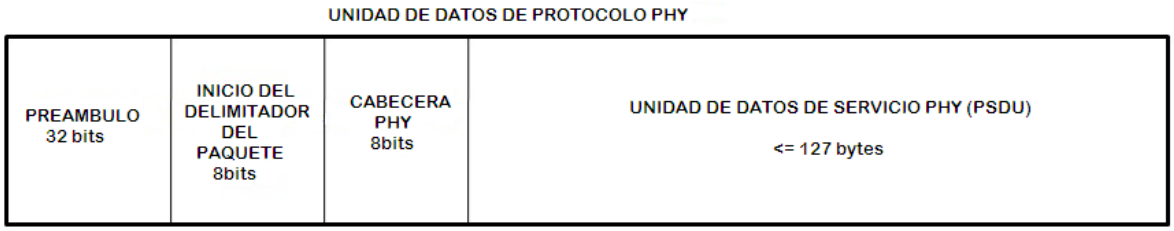


Figura 2.2 Trama PPDU.

Cada paquete o Unidad de Datos de Protocolo de capa física PHY (PPDU), empieza con un encabezado de sincronización (SHR - Synchronization Header - Encabezado de Sincronización), seguido de un encabezado de capa física para indicar la longitud del paquete (PHR - Phy Header), y de la capa física de la unidad de servicio de datos (PSDU- Phy Service Data Unit).

El preámbulo, de 32 bits, está diseñado para la adquisición de símbolos y tiempos de chip y en algunos casos se utiliza para ajustes repentinos en la frecuencia. No se requiere una ecualización en el canal de la capa física debido a la combinación de pequeñas áreas de cobertura con rangos de transmisión bajos. Típicamente el retardo RMS (Root Mean Square-Valor Medio Cuadrático) de propagación en casas residenciales es de 25 ns, que corresponde al 2.5% del periodo del espectro extendido utilizando el estándar IEEE 802.15.4.

Dentro del encabezado de la capa física se utilizan 7 bits para especificar la longitud de la carga de datos (en bytes). La longitud de paquetes va de 0 a 127 bytes. El tamaño típico de los paquetes para la mayoría de las aplicaciones domóticas, tales como el monitoreo y control de dispositivos de seguridad, iluminación, aire acondicionado y otras aplicaciones va de 30 a 60 bytes, mientras que las aplicaciones como juegos interactivos y periféricos de PC, requerirán paquetes más largos. La duración máxima

de paquetes es de 4.25ms para la banda de 2.4 GHz, y de 26.6ms para la banda de 915 MHz y de 53.2 ms para la banda de 868MHz.

- Canalización.
  En el IEEE 802.15.4 se definen 27 canales de frecuencia entre las tres bandas (Figura 2.3). La PHY de los 868/915 MHz soporta un solo canal entre los 868 y los 868.6MHz y diez canales entre los 902 y 928 MHz. Debido al soporte regional de esas dos bandas de frecuencias, es muy improbable que una sola red utilice los 11 canales. Sin embargo, las dos bandas se consideran lo suficientemente cercanas en frecuencia que se puede utilizar el mismo hardware para ambos y así reducir costos de manufactura.

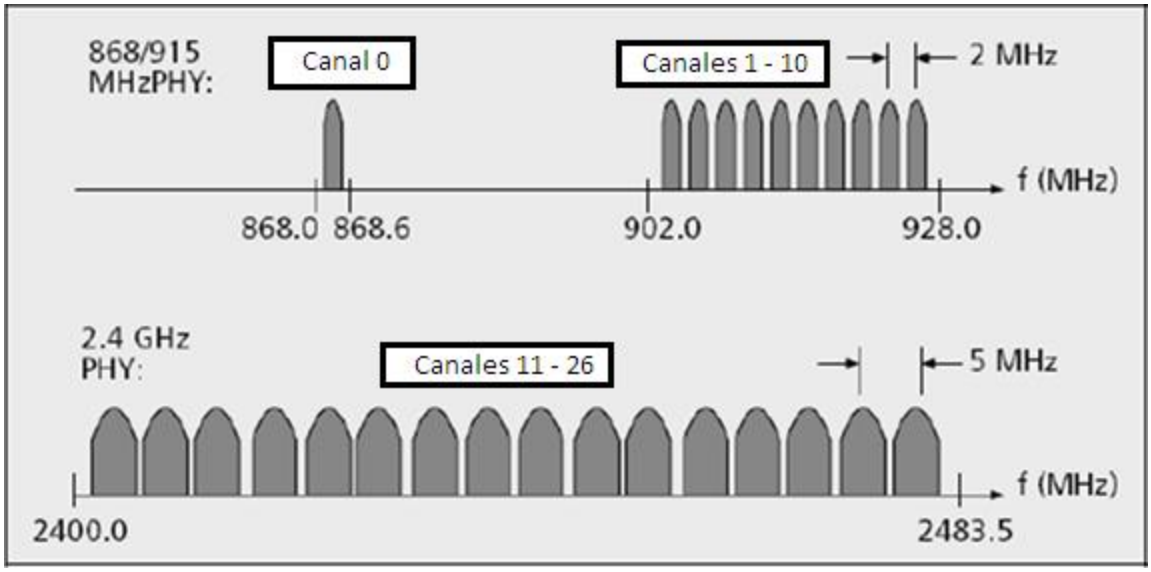


Figura 2.3 Canales de frecuencia del estándar 802.15.4.

La PHY de los 2.4 GHz soporta 16 canales de 2 MHz entre los 2.4 y los 2.4835 GHz con un amplio espacio entre canales (5 MHz) y esto con el objetivo de facilitar los requerimientos de filtrado en la transmisión y en la recepción (Tabla 2.2).

Tabla 2.2 Relación canales-frecuencia.

Número de Canales	Frecuencia central del Canal (MHz)
k = 0	868.3
k = 1, 2, … 10	906 + 2(k-1)
k = 11, 12, … 26	2405 + 5(k-11)

Dado que el hogar es propenso a tener múltiples redes inalámbricas trabajando en las mismas bandas de frecuencias, así como una interferencia no intencionada de las diferentes aplicaciones, la capacidad de relocalización dentro del espectro será un factor importante en el éxito de las redes inalámbricas dentro del hogar.

El estándar fue diseñado para implementar una selección dinámica de canales, a través de una selección específica de algoritmos, la cual es responsabilidad de la capa de red. La capa MAC incluye funciones de búsqueda que sigue paso a paso a través de una lista de canales permitidos en busca de una señal guía, mientras que la PHY contiene varias funciones de bajo nivel, tales como la detección de los niveles de energía recibidos, indicadores de calidad en el enlace así como de conmutación de canales, lo que permite la asignación de canales y agilidad en la selección de frecuencias. Estas funciones son utilizadas por la red para establecer su canal inicial de operación y para cambiar canales en respuesta a una pausa muy prolongada.

- Modulación.

  La PHY en los 868/915 MHz utiliza una aproximación simple DSSS en la cual cada bit transmitido se representa por un chip de máxima longitud de secuencia (secuencia m). Los datos binarios son codificados al multiplicar cada secuencia m por +1 o -1 y la secuencia de chip que resulta se modula dentro de la portadora utilizando BPSK (Binary Phase Shift Keying - Transmisión por Desplazamiento Binario de Fase). Antes de la modulación se utiliza una codificación de datos diferencial para permitir una recepción diferencial coherente de baja complejidad (Tabla 2.3).

Tabla 2.3 Modulación.

PHY	Banda	Parámetros de los Datos			Parámetros del chip	
		Velocidad de bits (kbps)	Velocidad de símbolos (Kbaud)	Modulación	Velocidad de chip (Mchip s/s)	Modulación
868/915 MHz	868-868.6 MHz	20	20	BPSK	0.3	BPSK
	902.0-928 MHz	40	40	BPSK	0.6	BPSK
2.4 GHz PHY	2.4-4.4835 GHz	250	62.5	16-ary ortogonal	2	O-QPSK

La capa física de 2.4GHz emplea una técnica de modulación semi-ortogonal basada en métodos de DSSS. Los datos binarios son agrupados en símbolos de 4 bits, y cada símbolo especifica una de las 16 secuencias de transmisión semi-ortogonales de código de pseudo-ruido (PN - Pseudo Noise). El uso de símbolos casi ortogonales simplifica la implementación a cambio de un desempeño ligeramente menor.

b) Control de Acceso al Medio. El control de acceso al medio transmite tramas MAC usando para ello el canal físico. Además del servicio de datos, ofrece una interfaz de control y regula el acceso al canal físico y al balizado de la red. También controla la validación de las tramas y las asociaciones entre nodos, y garantiza intervalos de tiempo. Por último ofrece puntos de enganche para servicios seguros.

El formato general de las tramas MAC se diseñó para ser muy flexible y que se ajustara a las necesidades de las diferentes aplicaciones con diversas topologías de red al mismo tiempo que se mantenía un protocolo simple. El formato general de una trama MAC se muestra en la figura 2.4. A la trama MAC se le denomina Unidad de Datos de Protocolos MAC (MPDU - MAC Protocol Data Unit) y se compone del encabezado MAC (MHR - MAC Header), unidad de servicio de datos MAC (MSDU - MAC Service Data Unit) y pie de MAC (MFR - MAC Footer). El primer campo del encabezado de trama es el campo de control. Éste indica el tipo de trama MAC que se pretende transmitir, especifica el formato y la dirección de campo y controla los mensajes de enterado. En pocas

palabras, la trama de control especifica cómo es el resto de la trama de datos y que es lo que contiene.

El tamaño de las direcciones puede variar entre 0 y 20 bytes. Por ejemplo, una trama de datos puede contener información de la fuente y del destinatario, mientras que la trama de enterado no contiene ninguna información de ninguna dirección. Por otro lado, una trama de guía solo tiene información de la dirección de la fuente. Esta flexibilidad en la estructura ayuda a incrementar la eficiencia del protocolo al mantener los paquetes lo más reducido posible.

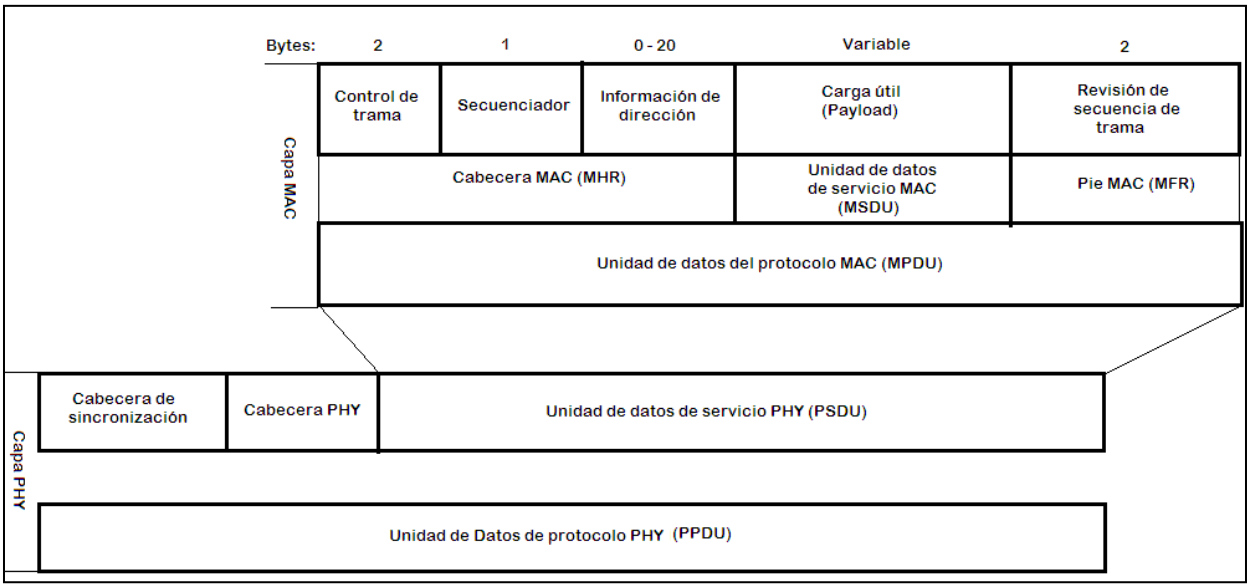


Figura 2.4 Trama MAC.

El campo llamado payload (carga útil) es variable en longitud; sin embargo, la trama completa de MAC no debe exceder los 127 bytes de información. Los datos que lleva el payload dependen del tipo de trama. El estándar IEEE 802.15.4 tiene cuatro diferentes tipos de tramas. Éstos son la trama de guía, de datos, tramas de enterados y tramas de comando MAC. Solo la trama de datos y de guía contienen información proveniente de capas superiores; las tramas de mensajes de enterado y la de comandos MAC originados en el MAC, son usadas para comunicaciones MAC punto a punto. Otros campos en la trama MAC son una secuencia de números al igual que tramas de revisión (FCS - Frame Checksum). La secuencia de números en los encabezados enlaza a las tramas de reconocimiento o acuse de recibo (acknowledgment o ACK) con transmisiones anteriores. La transmisión se considera exitosa solamente cuando la trama de enterado contiene la misma secuencia de números que la secuencia anterior transmitida. Las FCS ayudan a verificar la integridad de las tramas MAC.

El estándar IEEE incluye esta subcapa que añade las etiquetas estándar de 8-bit DSAP (Destination Service Access Point - Servicio de Destino del Punto Acceso) y SSAP (Source Service Access Point - Servicio Fuente del Punto de Acceso) a los paquetes del tipo de conexión. También hay un campo de control de 8 o 16 bits usado en funciones auxiliares como Control de flujo. Hay sitio para 64 números SAP globalmente asignados.

c) Estructura de la trama de Datos (Data Frame). La trama de datos se origina en capas superiores. La carga útil de datos es enviada a la subcapa MAC y se la denomina MSDU, es limitada por una trama MHR al inicio y por una trama MFR al final. El MPDU es enviado a la capa física como carga útil de datos de la capa física (PSDU), el cual junto con una trama SHR y una trama PHR forman el paquete de datos de la capa física PHY (PPDU) (Figura 2.5).

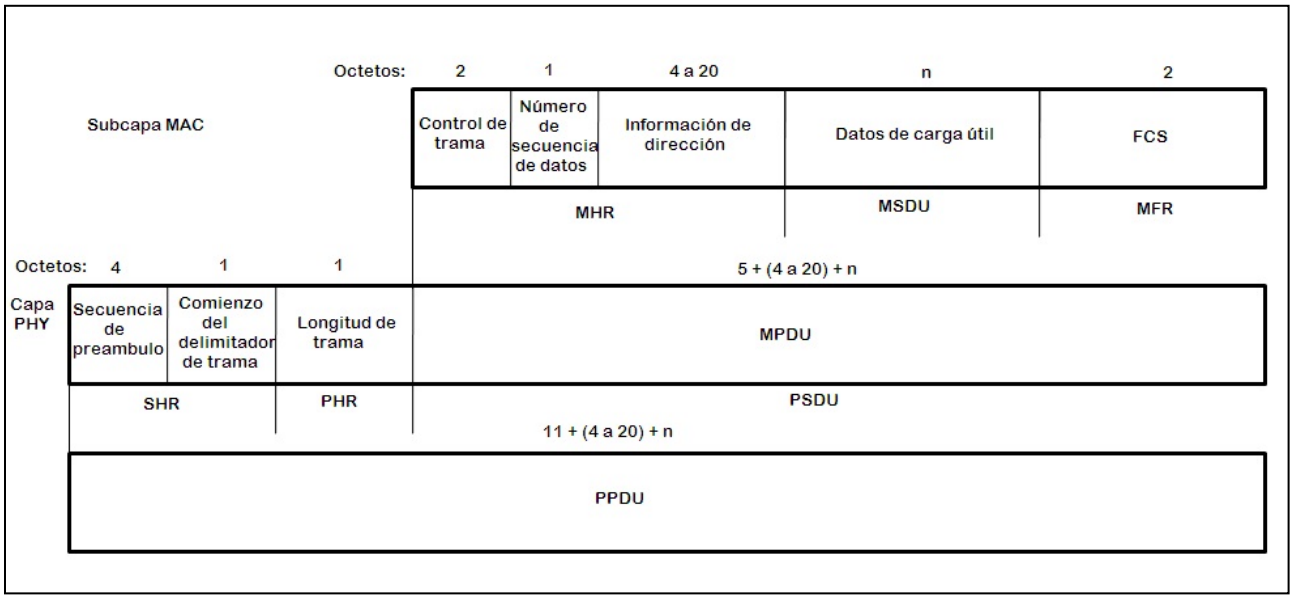


Figura 2.5 Subcapa MAC.

d) Estructura de la trama ACK (Acknowledgment Frame - Trama de reconocimiento) La trama ACK proporciona el intercambio de información activa desde el receptor para indicarle al emisor que el paquete fue recibido sin error. Este paquete corto aprovecha el tiempo de silencio (quiet time), especificado por la norma, inmediatamente después de la transmisión del paquete de datos se origina en la subcapa MAC (Figura 2.6).

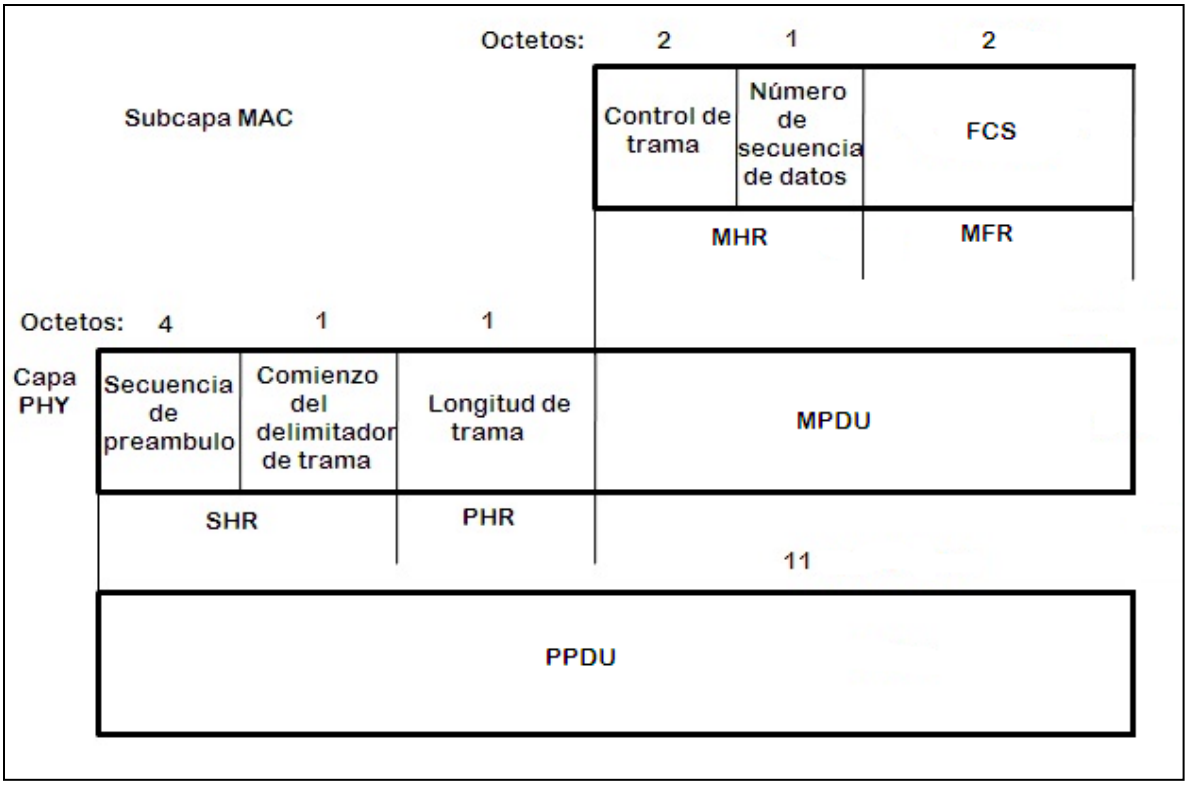


Figura 2.6 Trama Acknowledgment.

- Estructura de la trama de comandos MAC (MAC Command Frame).
  La trama de Comandos MAC es un mecanismo para el control o configuración a distancia de los dispositivos de los nodos. Permite que un director centralizado de la red pueda configurar a los dispositivos individualmente sin importar lo grande que sea la red. En la estructura se puede ver que solo se añade el campo “Command Type” a la estructura de Datos (Figura 2.7).

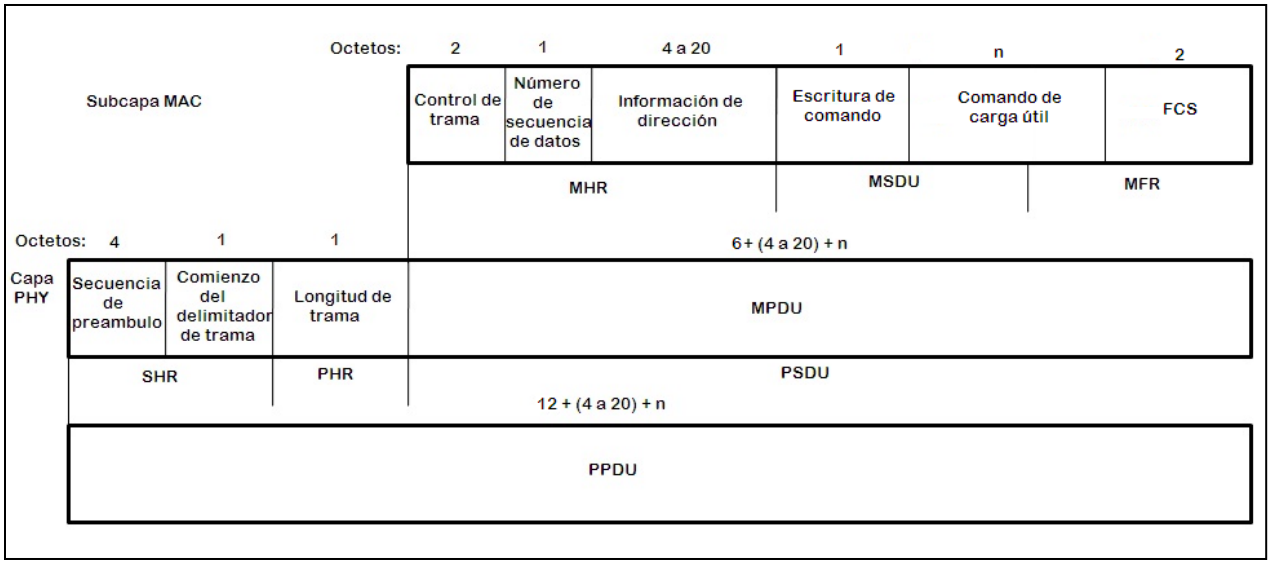


Figura 2.7 Trama de comandos MAC.

- Estructura de la trama Baliza (Beacon Frame).
  La trama Baliza (Figura 2.8) añade un nuevo nivel de funcionalidad a la red. Los dispositivos de los nodos pueden despertarse solamente cuando es transmitida una señal guía “beacon”, escuchar su dirección y volver al estado dormido, con el consecuente ahorro de energía. Las tramas baliza son importantes en las redes malla y de árbol para mantener todos los nodos sincronizados sin requerir que los nodos consuman energía de la batería, escuchando durante largos periodos de tiempo. Esta estructura de balizas contienen supertramas.

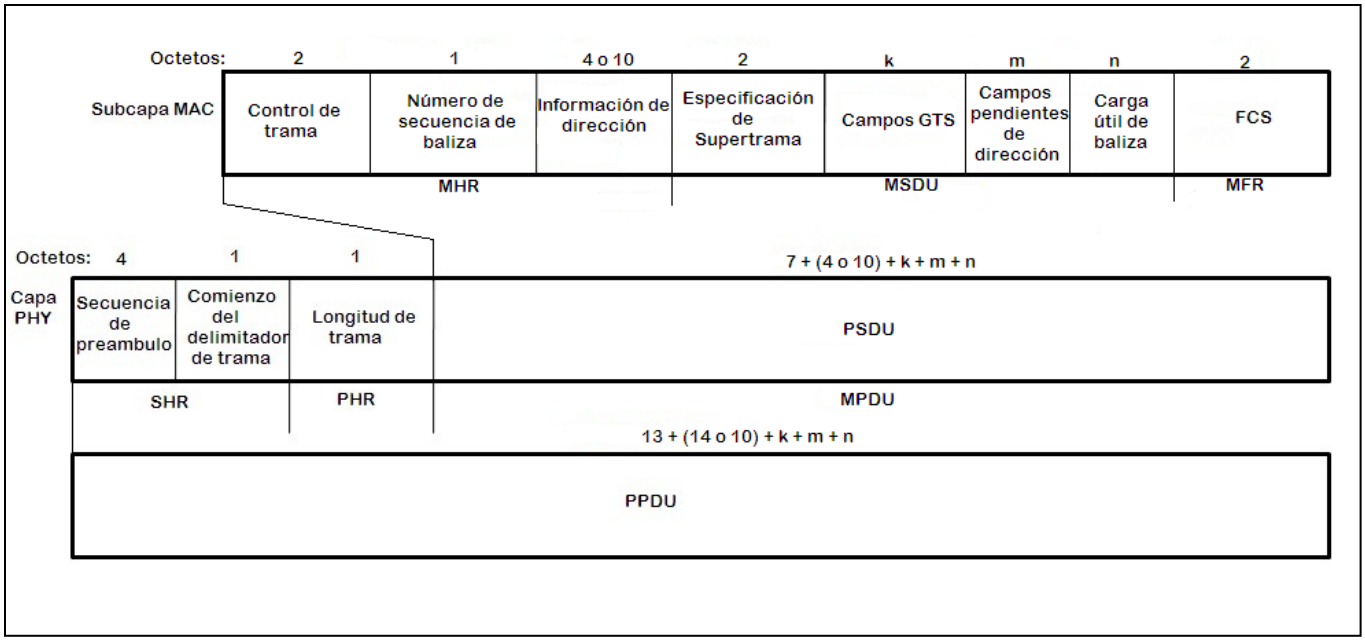


Figura 2.8 Trama Beacon.

- Estructura de supertramas.
  Algunas aplicaciones requieren anchos de banda dedicados para lograr estados de espera para un consumo de baja potencia. Para lograr dichos estados de espera el estándar IEEE 802.15.4 puede operar en un nodo opcional llamado supertrama (superframes) (Figura 2.9).

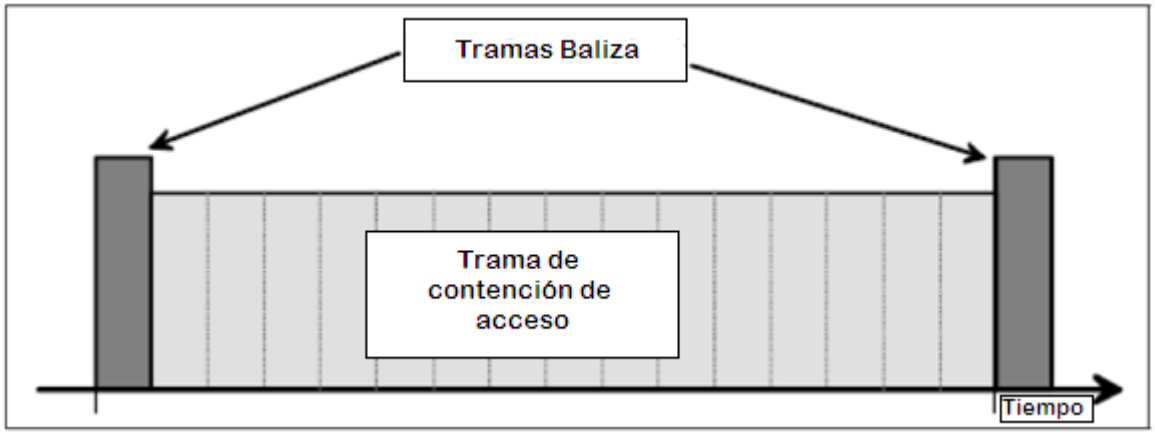


Figura 2.9 Supertrama.

El formato de una supertrama es definido por el coordinador de red. La supertrama está limitada por la baliza (guía de red), que es enviada por el coordinador y está dividida en 16 intervalos de tiempo de igual duración. La baliza de trama es transmitida en el

primer intervalo de tiempo de cada supertrama. Si un coordinador no desea usar la estructura de supertrama, puede deshabilitar la transmisión de guías. Las balizas son usadas para sincronizar los dispositivos vinculados, para identificar la PAN y para describir la estructura de las supertramas.

La supertrama puede tener un periodo activo y un periodo inactivo. Durante el periodo inactivo el coordinador puede no interactuar con su PAN y entrar en un modo de bajo consumo de energía.

Para aplicaciones de bajo retardo que requieran un ancho de banda específico o para que en caso de haber mucho tráfico ciertos dispositivos tengan siempre prioridad para lograr mínima latencia, el coordinador PAN puede dedicar partes de una trama activa para esas aplicaciones. Esas porciones son llamadas Intervalos de Tiempo Garantizados (GTS - Guaranteed Time Slots).

El GTS forma el periodo libre de contención (CFP - Contetion Free Period), el cual siempre aparece al final de una supertrama activa, inmediatamente luego del periodo de contención de acceso (CAP - Contention Access Period) que está después de una baliza. El coordinador PAN puede asignar hasta siete GTS y un GTS puede ocupar más de un periodo de tiempo. Sin embargo, una pequeña porción del CAP puede sobrar para el acceso de nuevos dispositivos que deseen unirse a la red. Todas las transacciones basadas en contención de acceso deben completarse antes que el CFP comience. También cada dispositivo transmitiendo en un GTS debe asegurarse de que su transacción se completó antes de que ocurra el próximo GTS o el fin del CFP (Figura 2.10).

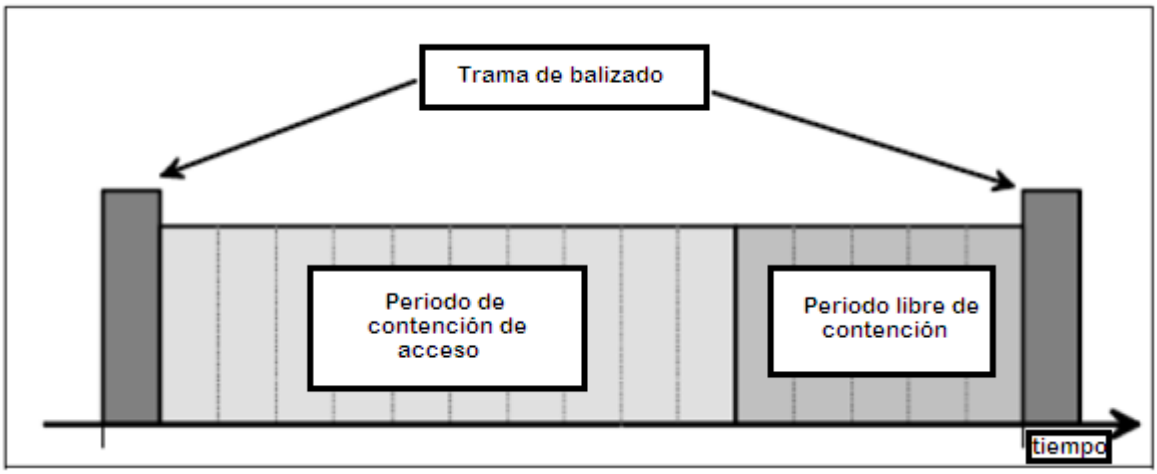


Figura **2.10 Supertrama con CFP.**

Resumiendo, el estándar 802.15.4 LR-WPAN es una red de comunicación de bajo costo que permite conexión inalámbrica en aplicaciones de bajo consumo de energía y baja tasa de transferencia de información. Los objetivos principales de una LR-WPAN son: su fácil instalación, transferencia de información confiable, un rango corto de operación, un muy bajo costo y una vida útil de batería razonable, mientras mantiene un protocolo flexible y simple.

Algunas de las características de una LR-WPAN son:

- Las velocidades de transferencia de información son 250kb/s, 100kb/s, 40kb/s y 20kb/s.
- Operación en estrella o peer to peer.
- Asigna direcciones de 16 bits o 64 bits extendido.
- Asignación especial en espacios de tiempo garantizados (GTSs).
- Canales de acceso CSMA/CA.
- Un protocolo completo de acuse de recibo para una transferencia confiable.
- Bajo consumo de energía.
- Detección de energía (ED - Energy Detection).
- Indicador de calidad de conexión (LQI - Link Quality Index).
- 16 canales en la banda de 2450MHz, 30 canales en la banda de 915 MHz y 3 canales en la banda de 868MHz.

Dos tipos de dispositivos distintos pueden participar en una red IEEE 802.15.4, un dispositivo de función completa (FFD - Full Function Device) que es el que toma la función de un router y un dispositivo de función reducida (RFD - Reduced Function Device) utilizado en los dispositivos finales. El FFD puede operar en tres modos sirviendo como un coordinador de red de área personal (PAN), un coordinador o un

dispositivo. Un FFD puede comunicarse con RFDs u otros FFDs, mientras un RFD puede comunicarse solo con un FFD. Un RFD está previsto para aplicaciones que son extremadamente simples, como un interruptor de luz o un sensor infrarrojo pasivo debido a que no tienen la necesidad de enviar grandes cantidades de datos y podría solo asociarse con un único FFD a la vez. Por consiguiente, el RFD puede ser implementado usando pocos recursos y poca capacidad de memoria.

La PHY provee dos servicios: el servicio de datos PHY y el servicio de administración de interconexión con la capa física de la entidad de gestión (PLME - Physical Layer Management Entity) y servicio de access point (SAP conocido como PLME-SAP). El servicio de datos de la PHY habilita la transmisión y recepción de las PDU a través del canal físico de radio.

La capa de red tiene como objetivo principal permitir el correcto uso del subnivel MAC y ofrecer una interfaz adecuada para su uso por parte de la capa de aplicación. En esta capa se brindan los métodos necesarios para iniciar la red, unirse a la red, enrutar paquetes dirigidos a otros nodos en la red, proporcionar los medios para garantizar la entrega del paquete al destinatario final, filtrar paquetes recibidos, cifrarlos y autentificarlos. Se debe tomar en cuenta que el algoritmo de enrutamiento que se usa es el enrutamiento de malla, el cual se basa en el protocolo vector de ruteo bajo demanda (Ad Hoc On-Demand Vector Routing – AODV). Cuando esta capa se encuentra cumpliendo la función de unir o separar dispositivos a través del controlador de red, implementa seguridad y encamina tramas a sus respectivos destinos; además, la capa de red del controlador de red es responsable de crear una nueva red y asignar direcciones a los dispositivos de la misma. En esta capa se implementan las distintas topologías que una red ZigBee soporta (árbol, estrella y malla).

La siguiente capa es la de soporte a la aplicación que es el responsable de mantener el rol que el nodo juega en la red, filtrar paquetes a nivel aplicación, mantener la relación de grupos y dispositivos con los que la aplicación interactúa y simplificar el envío de datos a los diferentes nodos de la red. La capa de red y de soporte a la aplicación son definidas por la Alianza ZigBee.

En el nivel conceptual más alto se encuentra la capa de aplicación que no es otra cosa que la aplicación misma y de la que se encargan los fabricantes. En esta capa es donde se encuentran los ZDO (ZigBee Device Objects - Objetos de Dispositivo ZigBee) que se encargan de definir el papel del dispositivo en la red, si el actuara como coordinador, ruteador o dispositivo final.

Cada capa se comunica con sus capas subyacentes a través de una interfase de datos y otra de control, las capas superiores solicitan servicios a las capas inferiores y éstas reportan resultados a las superiores. Además de las capas mencionadas, a la

arquitectura se integra otro par de módulos: módulo de seguridad, que es quien provee los servicios para cifrar y autentificar los paquetes, y el módulo de administración del dispositivo ZigBee, que es quien se encarga de administrar los recursos de red del dispositivo local, además de proporcionar a la aplicación funciones de administración remota de la red.

Las distintas interfaces entre las capas ayudan a definir las conexiones lógicas que son descritas en este estándar (Figura 2.11).

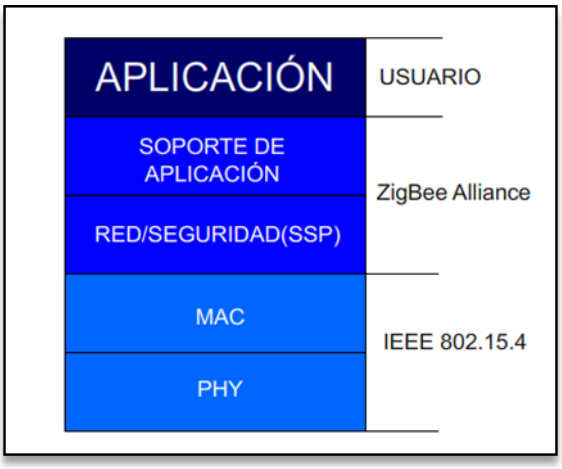


Figura 2.11 Capas de la pila de protocolos ZigBee.

2.3 Tipos de Dispositivos

Para una red ZigBee se definen tres tipos diferentes de dispositivos ZigBee según su función:

a) Coordinador ZigBee (ZC - ZigBee coordinator). El tipo de dispositivo completo puede actuar como un director de una red en árbol así como servir de enlace a otras redes. Existe exactamente un coordinador por cada red, que es el nodo que la comienza en principio. Puede almacenar información sobre la red y actuar como su centro de confianza en la distribución de claves de cifrado (Figura 2.12).

2.12 Coordinador ZigBee.

b) Router ZigBee (ZR - ZigBee Ruter). Además de ofrecer un nivel de aplicación para la ejecución de código usuario, puede actuar como router interconectando dispositivos separados en la topología de la red (Figura 2.13).

2.13 Router ZigBee.

c) Dispositivo Final (ZED - ZigBee End Device). Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o un router), pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías. Un ZED tiene requerimientos mínimos de memoria y es por tanto significativamente más barato (Figura 2.14).

2.14 Dispositivo final.

Con base en su funcionalidad puede plantearse una segunda clasificación:

1. Dispositivo de funcionalidad completa (FFD). Es capaz de recibir mensajes en formato del estándar 802.15.4. Gracias a la memoria adicional y a la capacidad de cómputo, puede funcionar como coordinador o router o puede ser usado en dispositivos de red que actúen de interface con los usuarios.

2. Dispositivo de funcionalidad reducida (RFD). Tiene capacidad y funcionalidad limitadas con el objetivo de conseguir un bajo costo y una gran simplicidad. Básicamente, son los sensores/actuadores de la red.

2.4 Características de las redes ZigBee

Las principales características de ZigBee son:

- ✓ ZigBee opera en las bandas libres ISM de 2.4 GHz, 868 MHz (Europa) y 915 MHz (Estados Unidos).

- ✓ Tiene una velocidad de transmisión de 250 Kbps y un rango de cobertura de 10 a 75 m.

- ✓ Aunque coexiste en la misma frecuencia con otro tipo de redes como WiFi o Bluetooth se desempeño no se ve afectado, esto debido a su baja tasa de transmisión y a características propias del estándar IEEE 802.15.4.

- ✓ Capacidad de operar en redes de gran densidad, esta característica ayuda a aumentar la confiabilidad de la comunicación, ya que entre más nodos existan dentro de una red, entonces, mayor número de rutas alternas existirán para garantizar que un paquete llegue a su destino.

- ✓ Cada red ZigBee tiene un identificador de red único, lo que permite que coexistan varias redes en un mismo canal de comunicación sin ningún problema. Teóricamente pueden existir hasta 16000 redes diferentes en un mismo canal y cada red puede estar constituida por hasta 65000 nodos.

- ✓ Es un protocolo de comunicación multi-salto, es decir, que se puede establecer comunicación entre dos nodos aún cuando éstos se encuentren fuera del rango de transmisión, siempre y cuando existan otros nodos intermedios que los interconecten, de esta manera se incrementa el área de cobertura de la red.

- ✓ Su topología de malla permite a la red auto recuperarse de problemas en la comunicación aumentando su confiabilidad.

2.5 Tipo de tráfico

En ZigBee, el empaquetamiento se realiza en cuatro tipos diferentes de paquetes básicos, los cuales son: Datos, ACK, MAC y Baliza. El paquete de datos tiene una carga de datos de hasta 104 bytes. La trama está numerada para asegurar que todos los paquetes llegan a su destino. Un campo asegura que el paquete se ha recibido sin errores. Esta estructura aumenta la fiabilidad en condiciones complicadas de transmisión.

La estructura de los paquetes ACK, llamada también paquete de reconocimiento, es donde se realiza una realimentación desde el receptor al emisor, de una manera se confirma que el paquete se ha recibido sin errores. Se puede incluir un tiempo de silencio entre tramas para enviar un pequeño paquete después de la transmisión de cada paquete.

El paquete MAC se utiliza para el control remoto y la configuración de dispositivos/nodos. Una red centralizada utiliza este tipo de paquetes para configurar la red a distancia.

El paquete baliza se encarga de despertar los dispositivos que escuchan y luego vuelven a dormirse si no reciben nada más. Estos paquetes son importantes para mantener todos los dispositivos y los nodos sincronizados, sin tener que gastar una gran cantidad de batería estando todo el tiempo encendidos.

Por otra parte, el direccionamiento es, a su vez, parte del nivel de aplicación. Un nodo está formado por un transceptor de radio compatible con el estándar 802.15.4 donde se implementan dos mecanismos de acceso al canal y una o más descripciones de dispositivo. El transceptor es la base del direccionamiento, mientras que los dispositivos dentro de un nodo se identifican por medio de un dispositivo final numerado entre 1 y 240.

Los dispositivos se direccionan empleando 64-bits y un direccionamiento corto opcional de 6 bits. El campo de dirección incluido en MAC puede contener información de direccionamiento de ambos orígenes y destinos. Este doble direccionamiento es usado para prevenir un fallo en la red.

Los dos mecanismos de acceso al canal que se implementan en ZigBee corresponden a redes “con balizas” y “sin balizas”. Para una red “sin balizas”, un estándar ALOHA CSMA/CA envía reconocimientos positivos para paquetes recibidos correctamente. En esta red, cada dispositivo es autónomo, pudiendo iniciar una conversación, en la cual los otros pueden interferir. A veces ocurre que el dispositivo destino puede no oír la petición o que el canal esté ocupado.

Este sistema se usa típicamente en los sistemas de seguridad, en los cuales sus dispositivos (sensores, detectores de movimiento o de rotura de cristales), duermen prácticamente todo el tiempo (99.99%). Para que se les tome en cuenta, estos elementos se “despiertan” de forma regular para anunciar que siguen en la red. Cuando se produce un evento, el sensor “despierta” instantáneamente y transmite la alarma correspondiente. Es en ese momento cuando el coordinador de red recibe el mensaje enviado por el sensor y activa la alarma correspondiente. En este caso, el coordinador de red se alimenta de la red principal durante todo el tiempo.

En cambio, en una red “con balizas”, se usa una estructura de supertrama para controlar el acceso al canal, esta supertrama es estudiada por el coordinador de red para transmitir “tramas baliza” cada ciertos intervalos (de 15.38 ms a 52 s). Esta estructura garantiza el ancho de banda dedicado y bajo consumo. Este modo es más recomendable cuando el coordinador de red trabaja con una batería. Los dispositivos que conforman la red escuchan a dicho coordinador durante el “balizamiento” (mensaje de broadcast entre 0.015 y 252 s). Un dispositivo que quiera intervenir, lo primero que tendrá que hacer es registrarse con el coordinador y es entonces cuando observa si hay mensajes para él. En el caso de que no haya mensajes, este dispositivo vuelve a “dormir”, y se despierta de acuerdo con un horario que ha establecido previamente el coordinador. En cuanto el coordinador termina el “balizamiento”, vuelve a “dormirse”.

Existen tres modelos de transferencia de datos. El primero es la transferencia de datos desde un dispositivo a un coordinador. El segundo es la transferencia de datos desde un coordinador a un dispositivo, el dispositivo de red es el que recibe los datos. El tercer modelo es la transferencia de datos entre 2 dispositivos iguales (peer to peer). En la topología estrella solo dos de esas transacciones son usadas, porque los datos solo pueden ser intercambiados entre el coordinador y un dispositivo. En la topología igual a igual los datos pueden ser intercambiados entre dos dispositivos de la red, en consecuencia, las tres transacciones pueden ser usadas en esta topología.

El mecanismo de cada tipo de transmisión depende de si la red soporta la transmisión de balizas. Una red con habilitación de balizas es usada para soportar dispositivos con bajo retardo, tales como periféricos de PC, si la red no necesita soportar a tales dispositivos, sin embargo, la baliza es requerida para la asociación de la red.

Transferencia de información entre dispositivos.

1. Transferencia de datos a un coordinador.

   Cuando un dispositivo desea transferir datos a un coordinador en una red que tiene habilitada la transmisión de balizas, este primero espera la baliza de red. Cuando la baliza es encontrada, el dispositivo se sincroniza con la estructura de la supertrama. En el momento adecuado, el dispositivo transmite la trama de datos usando CSMA-CA ranurado al coordinador. El coordinador notifica la recepción exitosa de los datos, transmitiendo una trama de confirmación. De esta manera se completa la transmisión (Figura 2.15).

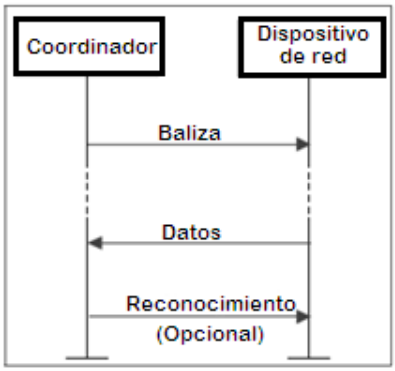


Figura 2.15 Transferencia de datos a un coordinador.

Cuando un dispositivo quiere transferir datos en una red sin habilitación de baliza, simplemente transmite su trama de datos usando CSMA-CA no ranurado al coordinador. El coordinador notifica la recepción exitosa de los datos transmitiendo una trama de confirmación, de esta manera se completa la transmisión (Figura 2.16).

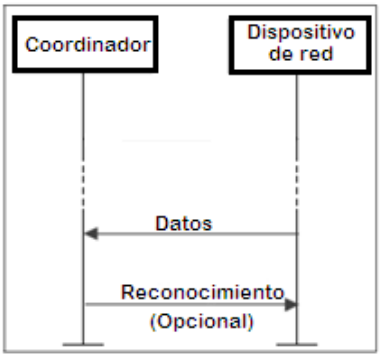


Figura 2.16 Transferencia de datos en una red sin habilitación.

2. Transferencia de datos desde un coordinador.

Cuando el coordinador desea transferir datos a un dispositivo en una red con habilitación de balizas, éste indica en la baliza de red que el mensaje de datos está pendiente. El dispositivo periódicamente espera la baliza de red y si un mensaje está pendiente transmite un comando MAC pidiendo datos, usando CSMA-CA ranurado. El coordinador confirma la recepción exitosa del pedido de datos transmitiendo una trama opcional de confirmación. La trama pendiente de datos es enviada luego usando CSMA-CA ranurado. El dispositivo confirma la recepción exitosa de los datos, transmitiendo una trama de confirmación. La transacción se completa. Una vez que la confirmación es recibida, el mensaje es removido de la lista de mensajes pendientes en la baliza (Figura 2.17).

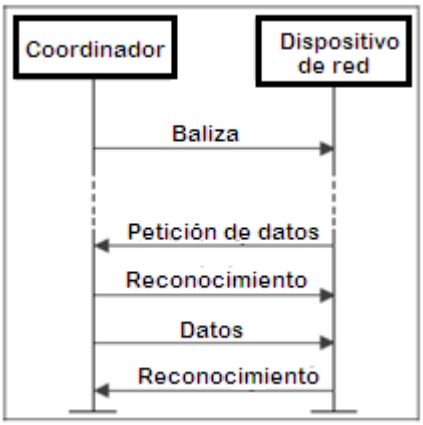


Figura 2.17 Transferencia de datos desde un coordinador.

Cuando un coordinador desea transferir datos a un dispositivo de una red sin balizas, éste guarda los datos para el dispositivo apropiado para hacer contacto y pedir información. Un dispositivo puede hacer contacto transmitiendo un comando MAC pidiendo datos, usando CSMA-CA no ranurado. El coordinador confirma la recepción exitosa del requerimiento de datos transmitiendo una trama de confirmación. Si hay datos pendientes, el coordinador transmite la trama de datos usando CSMA-CA no ranurado, al dispositivo. Si no hay datos pendientes, el coordinador transmite una trama de datos de longitud cero para indicar que no hay datos pendientes. El dispositivo confirma la recepción exitosa de los datos transmitiendo una trama de confirmación. La transacción se completa (Figura 2.18).

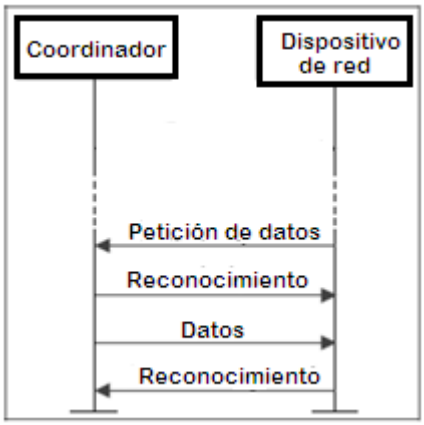


Figura 2.18 Recepción de los datos.

3. Transferencia de datos igual a igual

   En una PAN igual a igual cada dispositivo puede comunicarse con todos los otros dispositivos en su campo de influencia. Para hacer esto efectivo, el dispositivo que desea comunicarse debe estar sincronizado constantemente con los otros dispositivos. En este caso el dispositivo puede simplemente transmitir sus datos usando CSMA-CA no ranurado. En otros casos se deben tomar otras medidas para lograr la sincronización.

2.6 Modelo de red.

En ZigBee existen tres tipos de topologías: estrella, árbol y en malla (mesh network) como se muestra en la figura 2.19. Siempre hay un nodo de red que asume el papel de coordinador central encargado de centralizar la adquisición y las rutas de comunicación entre dispositivos. Además, si se aplica el concepto de malla, pueden existir coordinadores o routers alimentados permanentemente en espera de recibir/repetir las tramas de los dispositivos o sensores. Ambos dispositivos son del tipo FFD, debido a que exigen empotrar la mayoría de primitivas definidas por la pila ZigBee.

Los dispositivos que harán la función de sensores, termostatos o controles remotos serán de funcionalidad reducida y alimentados por baterías o pilas.

Sin lugar a dudas una de las mayores aportaciones de ZigBee y el que mayor interés está despertando a las empresas desarrolladoras de productos, es el concepto de red nodal o red en malla por el que cualquier dispositivo ZigBee puede conectarse con otro dispositivo usando a varios de sus compañeros como repetidores. A éste se le conoce como enrutamiento multi-salto, primero hace llegar la información al nodo ZigBee vecino, el cual puede además ser coordinador de la red, para así llegar al nodo destino, pasando por todos los que sean necesarios. De esta manera cualquier nodo ZigBee

puede hacer llegar los datos a cualquier parte de la red inalámbrica siempre y cuando todos los dispositivos tengan un vecino dentro de su rango de cobertura.

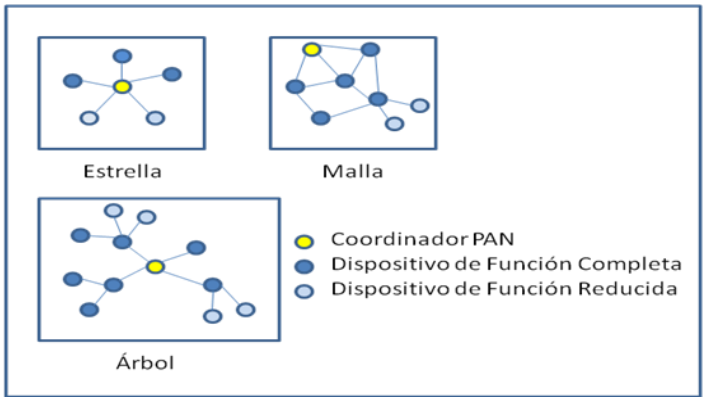


Figura 2.19 Topologías de red ZigBee.

2.7 Comparación con otras tecnologías

ZigBee de acuerdo con sus características puede ser comparada con otro tipo de red inalámbrica de poco alcance como lo es bluetooth y ver las enormes ventajas que ofrece (Figura 2.20).

- Una red ZigBee puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos, frente a los 8 máximos de una subred bluetooth.
- Menor consumo eléctrico que bluetooth. En términos exactos, ZigBee tiene un consumo de 30mA transmitiendo y de 3mA en reposo, frente a los 40mA transmitiendo y 0.2mA en reposo que tiene bluetooth. Este menor consumo se debe a que el sistema ZigBee se queda la mayor parte del tiempo dormido, mientras que en una comunicación bluetooth esto no se puede dar y siempre se está transmitiendo y/o recibiendo.
- Tiene una velocidad de hasta 250 kbps, mientras que en bluetooth es de hasta 1 Mbps.
- Debido a las velocidades de cada uno, uno es más apropiado para ciertas cosas. Por ejemplo, mientras que bluetooth se usa para aplicaciones como los teléfonos móviles y la informática casera, la velocidad de ZigBee se hace insuficiente para estas tareas, desviándola a usos tales como la domótica, los productos dependientes de la batería, los sensores médicos, y en artículos de juguetería, en los cuales la transferencia de datos es menor.
- Existe una versión que integra el sistema de radiofrecuencias característico de bluetooth junto a una interfaz de transmisión de datos vía infrarrojos desarrollado por IBM mediante un protocolo ADSI y MDSI.

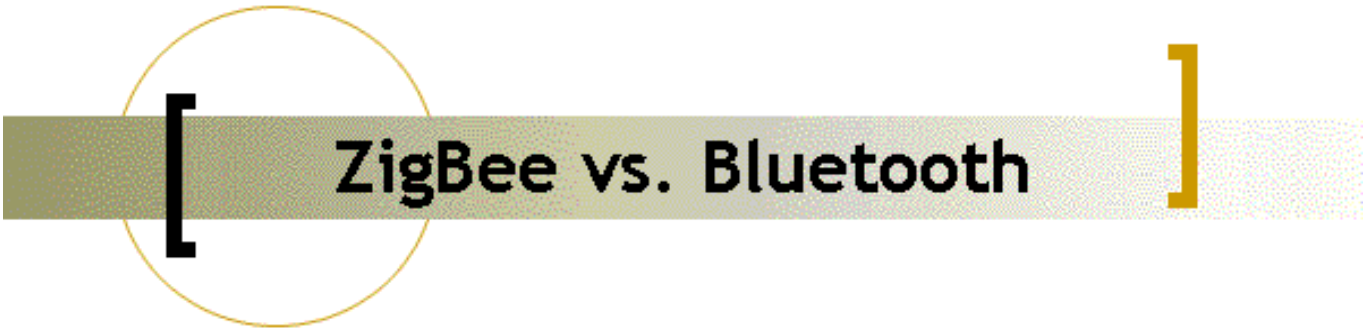


Figura 2.20 ZigBee vs Bluetooth.

CAPÍTULO III. APLICACIONES DE REDES ZIGBEE

En los años 90, las redes revolucionaron la forma en la que las personas y las organizaciones intercambian información y coordinan sus actividades. En esta década el ser humano será testigo de otra revolución, una nueva tecnología permitirá la observación y el control del mundo físico. Los últimos avances tecnológicos han hecho realidad el desarrollo de unos mecanismos distribuidos, diminutos, baratos y de bajo consumo que además son capaces tanto de procesar información localmente como de comunicarse de forma inalámbrica. La disponibilidad de microsensores y comunicaciones inalámbricas permitirá desarrollar redes de sensores para un amplio rango de aplicaciones.

Esto conllevará un necesario desarrollo de modelos físicos, los cuales requieren un análisis y una monitorización de datos efectivos y funcionales. Un segundo reto a superar es la variabilidad de este nuevo entorno. Mientras un buen sistema distribuido se desarrolla con la fiabilidad como elemento básico estas nuevas aplicaciones presentan un nivel de aleatoriedad más allá de lo común.

Pero la idea dominante radica en las restricciones impuestas por los sistemas en estado inactivo. Estos sistemas deben ser de bajo consumo y larga duración; tanto cuando operan como cuando permanecen a la espera. Además, como en internet, se tienen sistemas escalables, sin embargo, las técnicas tradicionales no son aplicables directamente, así que se deben desarrollar técnicas alternativas.

ZigBee Alliance ofrece un grupo de estándares que permiten tener redes con características antes mencionadas.

Miles de implementaciones elaboradas para usar los estándares ZigBee prueban la existencia de una gran variedad de soluciones con productos inteligentes y de fácil uso en cualquier lugar que sean requeridos, ya sea en el hogar, en el trabajo o en algún lugar donde se ofrezca algún servicio como puede ser un hospital. Estos estándares de innovación fueron diseñados con el propósito de permitir a los fabricantes ayudar a sus consumidores obtener un control completo de sus aplicaciones y poder realizar sus actividades diarias de una forma más sencilla por lo que el beneficio es redondo.

ZigBee permite soluciones fáciles, de bajo costo y agregando nuevas características inteligentes que aumentan la eficiencia, seguridad y rentabilidad de los dispositivos que usan este estándar. Lo cual ayuda a todo tipo de usuarios a tener entornos con un ahorro económico y de energía ofreciéndoles herramientas que son necesarias para un control total del lugar en donde se implemente (Figura 3.1).

Figura 3.1 Soluciones ZigBee.

3.1 Energía Inteligente

ZigBee energía inteligente es el estándar mundial líder para productos interoperables que monitorean, controlan, informan y automatizan la entrega y uso de energía y agua. Lo cual ayuda a crear casas ecológicas ofreciendo a los usuarios la información y automatización necesaria para ayudar a reducir su consumo de energía y ahorro económico.

Este estándar cubre las distintas necesidades de empresas del cuidado global de los ecosistemas, fabricantes de productos y grupos gubernamentales intentando resolver las necesidades del agua y el futuro de la energía.

Todos esos productos son certificados para ofrecer beneficios en la manufactura permitiendo a empresas y consumidores comprar de forma segura los recursos que requiera. Cada producto necesita implementar un área de red ZigBee de energía inteligente robusta disponible. Por lo que ZigBee permite tener productos que proporcionan de una forma fácil una instalación amigable y segura (Figura 3.2).

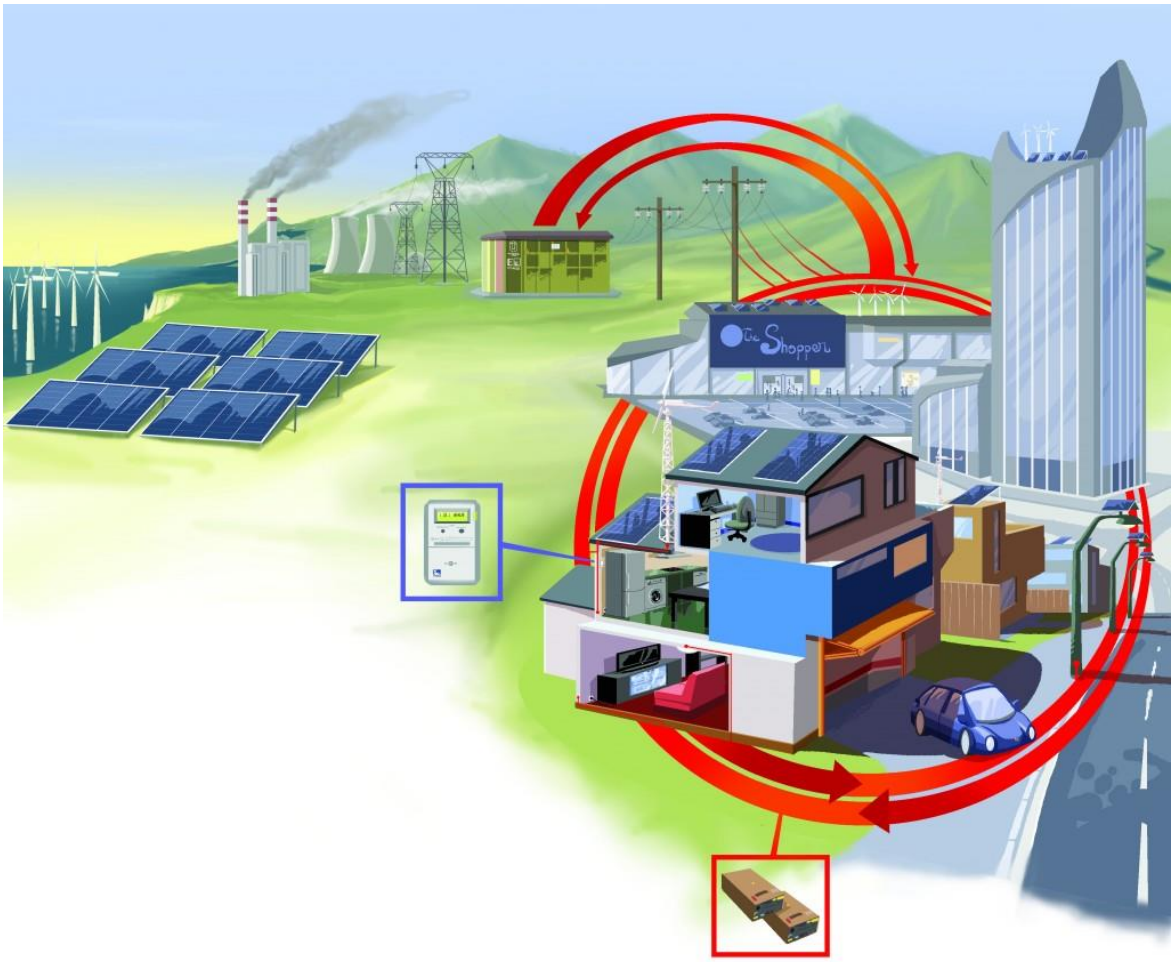


Figura 3.2 Energía inteligente.

Las principales características de energía inteligente son:

1. Medidores avanzados.

   - Comodidades múltiples incluyendo electricidad, gas, agua y temperatura ambiental.
   - Múltiples tipos de mediciones en las que se presenta información que contiene carga de perfiles, factores de energía, suma total de recursos usados y demanda de los mismos.
   - Información de consumo y producción en tiempo real.

2. Respuesta en demanda y control de carga.

   - Programación de eventos múltiples.
   - Control manual accesible para el manejo del usuario.
   - Habilidad de tener dispositivos ya sea individualmente o simultáneamente conectados a la red incluyendo calentadores de agua, luz, vehículos eléctricos y sistemas de generación de energía.

3. Asignación de precios.

   - Múltiples comodidades de pago incluyendo electricidad, gas, agua.
   - Múltiples divisas de soporte internacional.
   - Soporte para un radio de precios establecidos es decir el sistema es capaz de reconocer que precios se tienen en esa área.

4. Mensajes de texto.

   - Programación y cancelación de mensajes de solicitud de servicio.
   - Habilidad de requerir confirmación de mensajes.
   - Múltiples niveles de urgencias.

5. Seguridad.

   - Soporte individual, grupo o redes compartidas.
   - Registro de redes seguras usando llaves de seguridad preinstaladas o una clave pública estándar de métodos criptográficos.
   - Cifrado de información.

6. Beneficios.

   - Soporte adecuado para empresas que ofrezcan los servicios así como para los usuarios.
   - Redes fáciles de administrar.
   - Reduce significativamente el consumo de energía.
   - Reduce el impacto negativo al ambiente.

3.2 Control remoto

ZigBee control remoto proporciona un estándar global avanzado, ecológico y de fácil uso para controles remotos de radio frecuencia que erradica las restricciones de alcance entregando dos vías de comunicación, un rango más amplio de uso y una vida de batería extendido. Este estándar fue desarrollado para una variedad de dispositivos electrónicos de consumo incluyendo televisiones HD, equipo de cine en casa y equipos de audio principalmente.

El reemplazo de controles remotos de tecnología infrarroja por controles remotos ZigBee permite a los consumidores liberarse de apuntar directamente a los dispositivos. Esto ofrece a las personas una mayor flexibilidad, permitiendo el control de los dispositivos desde cuartos cercanos y poniendo esos dispositivos prácticamente donde se quiera incluyendo detrás de madera, de muros de concreto o vidrio. Es también una solución ecológica debido a su uso eficiente de energía y deja en desuso a la tecnología infrarroja (Figura 3.3).

Figura 3.3 Control remoto ZigBee.

Características del estándar de control remoto:

1. Comunicaciones de alta velocidad bidireccional.

   - Los fabricantes tienen un mejor control en la velocidad de transferencia de información aportando nuevas características al usuario final.
   - Habilidad de encontrar el control remoto perdido.
   - Nuevas capacidades interactivas.
   - Navegar en contenido en LCD.

2. Quitar barreras del campo de visión.

   - Los fabricantes tienen más opciones al no depender de un cierto rango de señal del dispositivo receptor.
   - Los dispositivos se vuelven más fáciles de controlar.

- Simplifica su uso al permitir a los usuarios no tener que apuntar directamente al dispositivo para controlarlo.
- Reduce devolución de productos por baja calidad y llamadas de soporte técnico.
- Extiende las distancias desde donde se pueden controlar los dispositivos y a través de muchas barreras.

3. Comandos estandarizados.

   - Los fabricantes ya no tienen que desarrollar o hacer licencias para bases de datos de comandos IR universal extensos.
   - Los usuarios no necesitan múltiples controles remotos al tener los mismos comandos para todos.

4. Actualizaciones y programación desde el aire.

   - Los fabricantes pueden actualizar el firmware para agregar nuevas características a sus productos.
   - Los usuarios pueden disfrutar de mejoras en sus productos después de haber sido instalados.
   - Los usuarios pueden hacer compras confidenciales sabiendo que los productos futuros tendrán soporte adecuado.

5. Mecanismos de eliminación de interferencias.

   - Los fabricantes eliminan la posibilidad de que se les regrese el producto debido a interferencias con otros dispositivos alrededor.
   - Los usuarios pueden poner su equipo casi en cualquier lugar sin preocupaciones de bloqueos de cualquier tipo.

6. Se incrementa la vida útil de la batería.

   - Mucho menos consumo de energía que IR.
   - Reduce el número de baterías que pueden ser usadas por los dispositivos lo que colabora con el ambiente.

7. Dispositivos soportados.

   - Televisiones.
   - Proyectores.
   - Reproductores.
   - Grabadores.
   - Reproductores de video.
   - Reproductores de audio.
   - Cine en casa.
   - Centros multimedia.
   - Consola de videojuegos.
   - Radios satelitales.
   - Monitores.
   - Controles remotos.

8. Beneficios.

   - Remplaza 30 años de tecnología IR.
   - Resuelve los problemas de tecnología.
   - Fácil de implementar.
   - Fácil de usar.
   - Comunicaciones rápidas y confiables.
   - Capacidad bidireccional.

3.3 Automatización del hogar.

ZigBee automatización del hogar ofrece un estándar global para dispositivos de interoperabilidad en la implementación de casas inteligentes capaces de controlar electrodomésticos, luz, ambiente, gestión de energía y seguridad, además de la capacidad de conectarse con otras redes ZigBee.

Las casas inteligentes permiten a los usuarios ahorrar dinero, cuidar el ambiente, sentirse más seguro y disfrutar de una gran variedad de comodidades que hacen del cuidado de una casa más fácil y de menor costo de mantenimiento.

ZigBee automatización del hogar da soporte a distintos proveedores de servicio y fabricantes de productos para la elaboración de nuevos dispositivos necesarios para crear casas inteligentes. Estos productos son ideales para nuevas construcciones, modernización de supermercados que son fáciles de mantener e instalar (Figura 3.4).

Numerosas compañías de innovación han contribuido con su pericia con este estándar, como lo son Philips, Control4 y Texas Instruments.

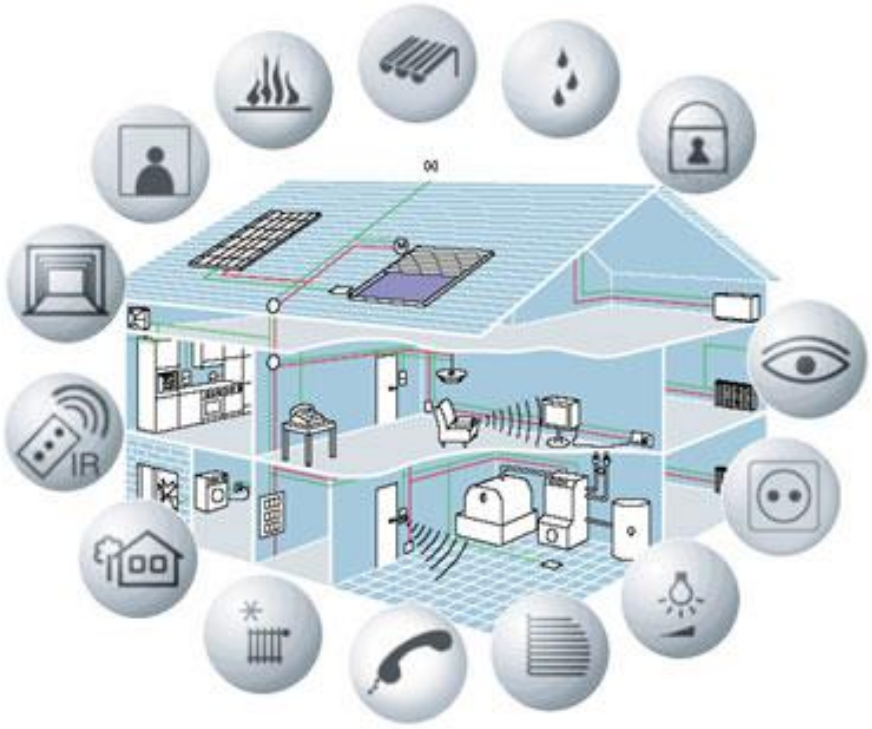


Figura 3.4 Casas Inteligentes.

Características del estándar casas inteligentes.

1. Fácil instalación.

   - Simplicidad de instalación, el mismo usuario puede llevar a cabo esta instalación.
   - Ideal para remodelaciones o nuevas construcciones.
   - Redes auto organizadas y de fácil instalación y mantenimiento.
   - Erradicación de interferencias lo que permite su uso libre.
   - Conectividad a internet.
   - Dispositivos de controles en cualquier sitio del mundo.
   - Uso de teléfonos móviles para el control de casas inteligentes.

2. Control de energía.

    - Monitor de uso de energía.
    - Apagado y encendido de dispositivos vía remota.
    - Administración de luz.

3. Seguridad.

    - Fácil instalación de nuevos dispositivos para crear un sistema de seguridad integrado en una casa inteligente.
    - Abrir y cerrar protectores para ventanas.
    - Integración de seguridad para casas inteligentes.

4. Dispositivos Soportados.

    - Dispositivos genéricos como apagadores.
    - Dispositivos que se usan para la luz.
    - Sistemas de alarmas contra intrusos.
    - Medidores de temperatura, calentadores, termostatos, etcétera.

5. Beneficios.

    - Fácil instalación.
    - Seguridad.
    - Interoperabilidad.

3.4 Cuidado de la salud.

ZigBee cuidado de la salud ofrece un estándar global para productos de interoperabilidad ofreciendo seguridad y confianza en el monitoreo y administración de un problema no crítico, baja agudeza de los servicios del cuidado de la salud como su meta de enfermedades crónicas, obteniendo independencia salud general, bienestar y buen estado físico.

Estos dispositivos inteligentes y de fácil uso promueven independencia en la gran mayoría de las enfermedades, bienestar y un buen estado físico. Una variedad de estos productos aun ofrecen una conexión innovadora con los cuidados de la salud profesionales como doctores y enfermeras, permitiéndoles monitorear la salud mientras la persona está en casa.

ZigBee cuidado de la salud da soporte a las necesidades de instituciones de salud fabricantes de productos y diseñadores de políticas para proveer una forma de estándar que permita el envío de información de un monitoreo fácil, controlado y automático en el cuidado de la salud, bienestar y buen estado físico de una casa para uso de un profesional (Figura 3.5).

Algunas de las empresas dedicadas a dar soporte a este estándar son: Motorola, Phillips, Freescale Semiconductor, Awarepoint y RF Technologies.

Figura 3.5 Cuidado de la salud.

Características del estándar cuidado de la salud.

1. Mejora continua y autosuficiente.

   - Permite monitoreo remoto a pacientes de forma confiable.
   - Mantienen libertad de movilidad.
   - Ofrece seguridad y sensores de monitoreo en casa y de uso de profesionales.
   - Provee capacidades de localización en tiempo real.

2. Manejo de enfermedades crónicas.

   - Ofrece realimentación rápida para un mejor manejo.
   - Permite colaboración entre dispositivos para gestionar múltiples enfermedades crónicas.
   - Posibilidad de conectar un gran número de dispositivos que son requeridos en tareas profesionales.

3. Salud y Bienestar.

   - Ofrece sensores para el cuerpo de análisis de salud de deportistas.
   - Optimiza los datos para todos los tipos de equipo para el bienestar.

4. Seguridad personalizable.

   - Seguridad de acuerdo con regulaciones regionales.
   - Acceso a soporte para usuarios, proveedores de servicio, proveedores de cuidado o redes compartidas.
   - Características de soporte a seguridad y privacidad de la información.
   - Generación eficiente de llaves, distribución y gestión para el hogar y profesionales.

5. Beneficios.

   - Elimina costos elevados eliminando la necesidad de permanecer en un hospital en una situación crítica.
   - Promueve autocuidado de la salud y bienestar.
   - Fácil instalación.
   - Seguro.
   - Interoperable.

3.5 Automatización en edificios.

Este estándar ofrece un estándar global de productos de interoperabilidad permitiendo seguridad y confianza en el monitoreo y control de sistemas de construcciones comerciales. Es el único estándar inalámbrico BACnet (Building Automation and Control Networks-Automatización de Edificios y Control de Redes) aprobado para edificios comerciales. Propietarios, operadores y arrendatarios pueden obtener grandes beneficios como ahorro de energía, bajos costos de ciclo de vida y una red inalámbrica robusta fácil de instalar. Usando este estándar se reduce o se elimina cableado y los conductos.

Al usar estos productos innovadores, es ahora posible ganar control sobre distintos tipos de construcciones, cuartos anteriormente inaccesibles o áreas sensibles, y aún más extender sistemas de automatización de edificios BACnet. También será posible eliminar redes cableadas requeridas para monitorear y administrar un sitio. La red permite a los sistemas de rápida reconfiguración acomodar una variedad de situaciones mientras se reduce la instalación y los costos de remodelación.

Los más beneficiados por este estándar son los dueños de edificios, operadores, fabricantes de productos, arquitectos y arrendadores. Estos grupos saben que el estándar ofrece la mejor forma de monitoreo sin la necesidad de cableado, control y sistemas de construcción automático comercial para crear un mundo más innovador, productivo y seguro (Figura 3.6).

Algunas de las empresas que usan este estándar son: Honeywell, Ingersoll-Rand/Trane, Johnson Controls, Schneider Electric and Siemens.

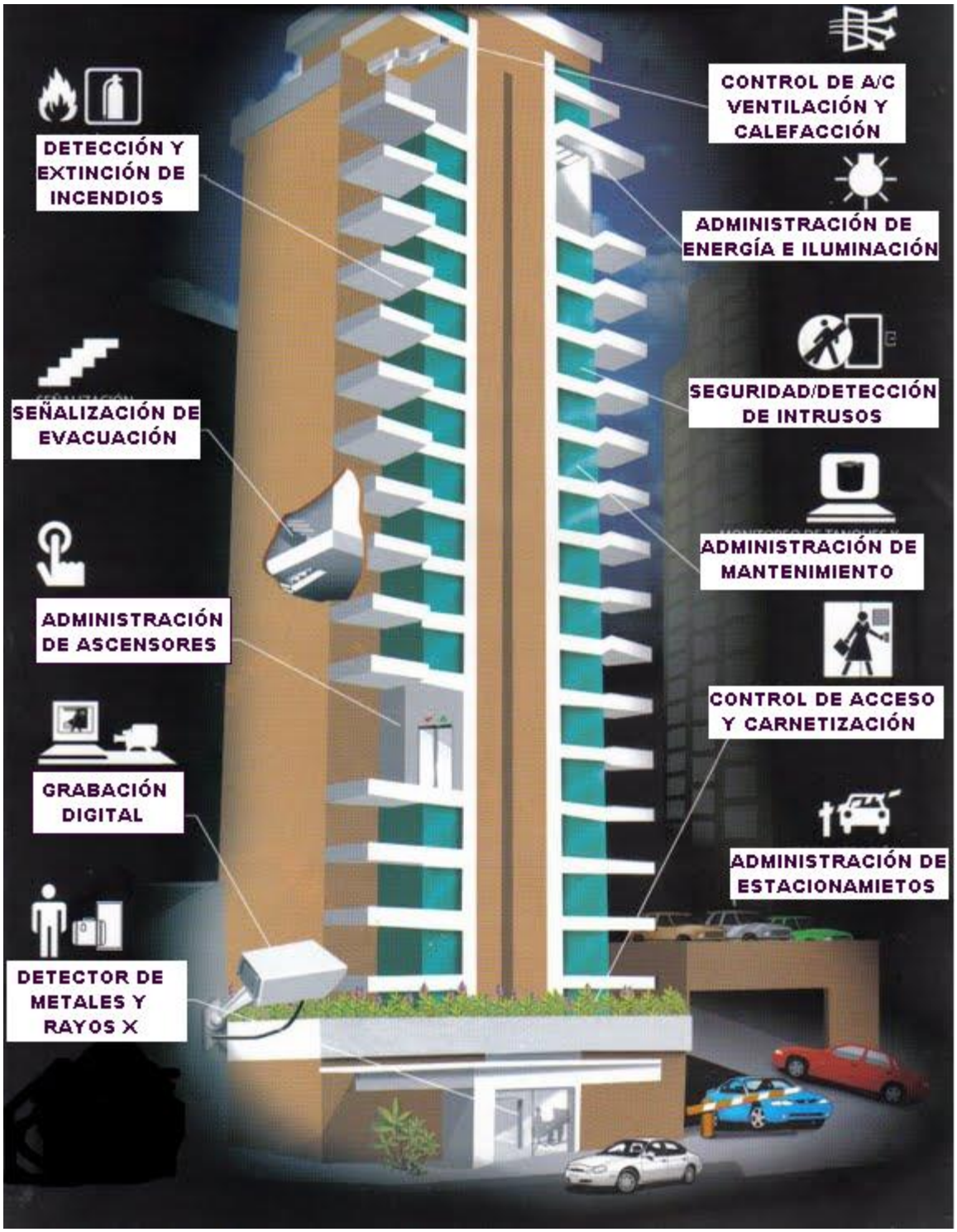


Figura 3.6 Edificio inteligente.

Existen en la actualidad 18 millones de kilómetros de cable existente instalado en construcciones comerciales solo en los Estados Unidos. Las soluciones de construcciones sin cables es la meta principal que se desea alcanzar para un edificio sustentable: reduciendo, reusando y reciclando. Menos cableado y más soluciones sin cables significa menos tiraderos de desperdicios que pueden ser quemados y emitir gases tóxicos al ambiente. Por lo que se tienen los siguientes escenarios:

a) Sistemas de actualización. Las soluciones sin cables son idealmente apropiados para espacios ya existentes debido a que eliminan la necesidad de quitar pisos, paredes o techos para el control de acceso. Las personas o procesos no necesitan ser trasladados a otro sitio mientras se llevan a cabo actualizaciones, permitiendo acceso continuo a laboratorios, información sensible, instalaciones de salud y áreas de procesos críticos.

b) Reconfiguración del espacio. Espacios abiertos, áreas de usos múltiples y espacios temporales pueden ahora ser automatizadas. Controles y sensores inalámbricos pueden ser fácilmente removidos para cubrir las necesidades de los usuarios o eventos. Conferencias y pasillos de exhibición, almacenes y auditorios son algunos de los ejemplos de espacios que son frecuentemente reestructurados para diferentes propósitos.

c) Restricciones estructurales. Construcciones o áreas hechas con concreto, mármol y otros materiales pueden ahora ser controlados inalámbricamente. Espacios con atrios, techos altos, edificios con características históricas y otros elementos arquitectónicos únicos pueden ser controlados actualmente inalámbricamente y sin cableados de alto costo o la preocupación de dañar dichas estructuras.

d) Lugares sensibles. Construcciones tales como hospitales, museos, laboratorios y centros de datos comúnmente requieren de un muy preciso y estable aire acondicionado que es manipulado por un control inalámbrico. Sin una instalación invasiva el control inalámbrico hace posible que funcionen de una manera sorprendente.

Características del estándar edificio inteligente.

1. Tecnología ZigBee.

   - Operación global en la banda de frecuencia de 2.4GHz de acuerdo con la IEEE 802.15.4.
   - Especificación ZigBee.
   - Larga vida de batería.
   - Rango de señal de 70m en interiores y 400m en exteriores.
   - Flexibilidad de redes para cubrir campus enteros.
   - Especificación abierta y gratuita basada en estándares internacionales.
   - Una escalabilidad alta de soluciones para miles de dispositivos.

2. Soluciones para todo tipo de construcciones.

   - Provee conectividad inalámbrica entre controles de luz, sensores y otros dispositivos dentro de edificios comerciales.
   - Conectividad inalámbrica a través de múltiples niveles de red.
   - Trabajo conjunto entre ZigBee PRO y el protocolo BACnet para crear estándares de comunicación de automatización de edificios.

3. Perfil de interoperabilidad.

   - Dispositivos debidamente certificados para asegurar una perfecta interoperabilidad y uso exacto de los estándares.
   - Una gran variedad de productos y dispositivos con la habilidad de trabajar juntos.

4. Perfil de interoperabilidad certificada.

   - Dispositivos debidamente certificados para asegurar una perfecta interoperabilidad y uso exacto de estándares.
   - Una gran variedad de productos y dispositivos con la habilidad de trabajar juntos.

5. Seguridad avanzada.

   - Uso de cifrado AES 128, claves y dispositivos de autenticación.
   - Cifrado de acceso seguro enfocado a la administración de información critica.

6. Construido para utilidades de gran escala comercial.

   - Soporta miles de dispositivos en una sola red.
   - De fácil conexión a internet u otras redes usando puertas de enlace.
   - Nuevos servicios pueden ser introducidos en forma controlada a escala como requerimientos de crecimiento.

7. Fácil reemplazo de controles obsoletos.

   - Eliminación de problemas al usar redes antiguas existentes que se van degradando o simplemente incompatibles.

8. Beneficios.

   - Integra dispositivos de control y monitoreo para luz, seguridad, detección de movimiento, ocupación y comodidad.
   - Permite sistemas existentes de gestión expandible para incluir sensores inalámbricos.
   - Interoperabilidad entre una variedad de dispositivos de automatización de edificios.
   - Reduce los costos del ciclo de vida. Espacios interiores que son reconfigurados frecuentemente tales como oficinas comerciales pueden tener ahorros significativos sobre el ciclo de vida de construcciones debido a que se eliminan costos de cableado.
   - Se evitan modificaciones a edificios.
   - Reduce costos de integración dentro de sistemas existentes a través del uso de puertas de enlace ZigBee.
   - Estándares abiertos soportan mercados competitivos de productos múltiples con bajo costo.
   - Al no existir cables que pueden ser jalados se producen menos interrupciones para sus usuarios.
   - Los costos se ven reducidos al eliminar cables y canales innecesarios.
   - Los sensores pueden ser fácilmente removidos dentro de la zona de control para un mejor sensado de temperatura, CO2, niveles de luz y humedad.
   - Los sensores pueden ser fácilmente agregados para proporcionar un porcentaje de lecturas desde múltiples puntos dentro de las zonas de mejor control por los ocupantes.
   - No existe un solo punto de falla.

- Usa tecnología de malla lo que permite establecer caminos redundantes de comunicación.
- Construcciones tales como hospitales, museos, laboratorios, centros de datos requieren de un mayor cuidado a la hora de instalar una red.
- Estos espacios pueden ser usados con dispositivos inalámbricos sin destruir o invadir algo.
- Reduce el uso de plásticos para fabricación de cables.
- Reduce el uso de materiales caros.
- Provee ahorro dramático de materiales.

3.6 Servicios de Telecomunicaciones.

ZigBee servicios de telecomunicaciones ofrece un estándar global para productos de interoperabilidad que permite una extensa variedad de servicios, incluyendo entrega de información, juegos en línea, pagos móviles seguros, control de acceso de la oficina móvil, compartir información peer-to-peer.

Este único estándar ofrece una asequible y forma fácil de introducir una nueva forma innovadora de servicios disponibles para casi todos usando teléfonos móviles y otros dispositivos portátiles. Ofrece también una variedad de servicios para operadores de red de teléfonos móviles, minoristas, empresarios y gobiernos. Ahora estos grupos tienen nuevas formas de alcanzar nuevos clientes. Los consumidores pueden usar su teléfono móvil para pagar productos y servicios, crear sus propias redes de juego y comunicaciones, recibir descuentos o cupones de empresas, y obtener direcciones o información de espacios públicos a través de GPS.

Algunas de las empresas desarrolladoras de este estándar son: Phillips, Telecom Italia, Telefónica, OKI, Huawei, Motorola and Texas Instruments.

Características del estándar de servicios de telecomunicaciones.

1. Escalabilidad.

   - Soporta miles de dispositivos en una sola red.
   - Fácil de conectar a internet u otras redes usando puertas de enlace.
   - Nuevos servicios pueden ser agregados en cualquier momento sin problemas.

2. Comandos estándar.

   - Estándares abiertos para interoperabilidad e internet en las redes.
   - Soporta intercambio de datos y navegación en la web usando una solución ligera y escalable.

- Maximiza el uso de dispositivos existentes desde aplicaciones públicas ZigBee.

3. Eliminación de interferencias.

   - Ofrece mecanismos de eliminación de interferencias y agilidad en los canales.
   - Coexistencia demostrada con bluetooth y Wi-Fi.

4. Extensa variedad de servicios adicionales de gran valor.

   - Avisos de proximidad.
   - Servicios básicos de localización.
   - Voz.
   - Compartir información.
   - Entrega de información.
   - Pagos seguros a través de teléfonos móviles.
   - Oficina móvil.
   - Realidad aumentada.

5. Dispositivos soportados.

   - Tarjetas SIM ZigBee.
   - Terminales móviles.
   - Herramientas de configuración.
   - Aumentadores de rango.
   - Access Point.
   - Información de nodos.
   - Información de terminales.
   - Puntos de venta.
   - Tarjetas flash.
   - Micrófonos.
   - Muchas otras posibilidades de tecnología móvil.

6. Beneficios.

   - Ofrece una gran cantidad de servicios.
   - Es de fácil uso.
   - Es de fácil implementación.

Como se puede ver en este capítulo, ZigBee ofrece diversas alternativas en diferentes ámbitos en donde las personas requieren de una tecnología barata y eficiente para llevar a cabo sus actividades cotidianas de una forma más adecuada ayudando además a bajar considerablemente el consumo de energía trayendo consigo grandes beneficios al ambiente, proporcionando una solución por así llamarla “verde”.

CAPÍTULO 4. SEGURIDAD EN REDES ZIGBEE

4.1 Análisis de amenazas y vulnerabilidades.

El desarrollo de redes de sensores requiere tecnologías de tres áreas de investigación diferentes:

a) Detección.
b) Comunicación.
c) Computación.

Los nodos sensores se encuentran normalmente esparcidos en algo llamado campo sensor. Cada uno de estos nodos sensores esparcidos por la red tiene capacidad tanto para recolectar datos, como para enrutarlos hacia el nodo recolector, cabe mencionar que este nodo puede comunicarse con el nodo administrador vía internet, vía satélite o de forma directa.

El diseño de una red de sensores como la descrita en la figura 4.1 tiene una gran influencia en los siguientes factores:

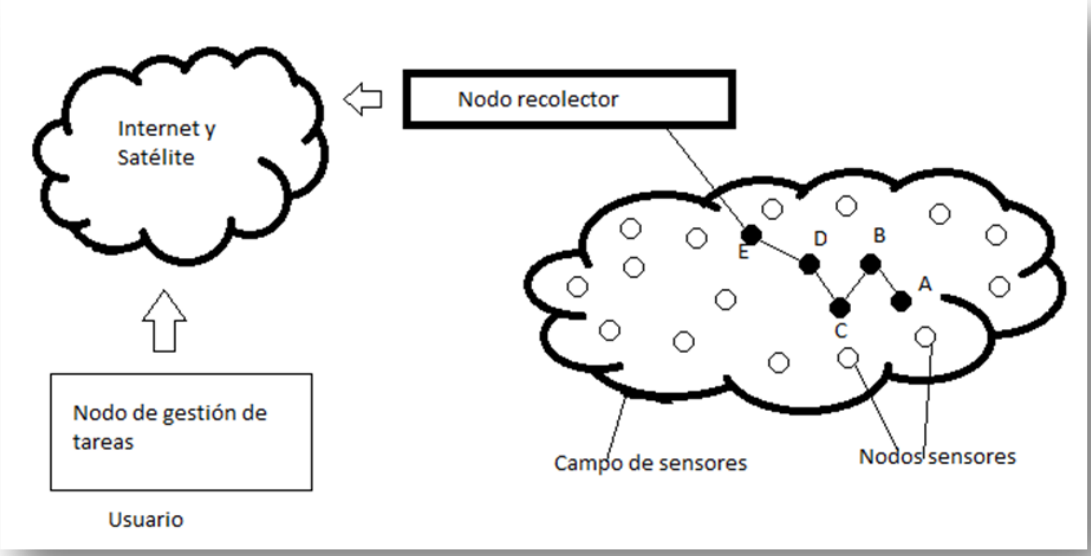


Figura 4.1 Estructura de una red de sensores.

Se pueden describir los siguientes principales problemas:

1. Tolerancia a fallas: Algunos nodos sensores pueden fallar o bloquearse debido a la falta de energía, o recibir daños físicos o interferencias debido al ambiente. El fallo de nodos sensores no debería comprometer el funcionamiento global de la red de sensores. Éste es el principio de la tolerancia a fallas o fiabilidad.

2. Escalabilidad: Los nuevo diseños deben ser capaces de trabajar con un número de nodos del orden de centenares, millares, e incluso, dependiendo de la aplicación, millones. También deben tomar en cuenta la alta densidad, que puede llegar hasta algunos centenares de nodos sensores en una región, que puede ser menor de 10m de diámetro.

3. Costos de Producción: Dado que las redes ZigBee consisten en un gran número de nodos sensores, el costo de un nodo individual es clave para que una red inalámbrica sea rentable en comparación con una red cableada. Si el costo de la red es más caro que el despliegue de sensores tradicionales, la red de sensores no está justificada desde el punto de vista económico.

4. Limitaciones de hardware: Un nodo sensor está constituido por cuatro componentes básicos, una unidad sensora, una unidad de proceso, una unidad transceptora y una unidad de energía, aunque pueden tener también componentes adicionales dependiendo de su aplicación como un sistema de localización, un generador de energía o un movilizador.

   Las señales analógicas producidas por los sensores son convertidas a señales digitales por un conversor ADC (Analog Digital Converter), para ser pasadas después a la unidad de proceso.

   La unidad de proceso, generalmente asociada a una pequeña unidad de almacenamiento, maneja los procedimientos necesarios para que el nodo sensor colabore con los demás en la realización de las tareas de percepción asignadas. Una unidad transceptora conecta el nodo a la red.

   Uno de los componentes más importantes de un nodo sensor es la fuente de alimentación. La fuente de alimentación puede ser abastecida por unidades captadoras de energía como es el caso de las células solares.

5. Topología: El despliegue de un gran número de nodos densamente distribuidos precisa de un mantenimiento y gestión de la topología muy bien cuidados. Se pueden dividir las tareas de mantenimiento y cambio de la topología en tres fases:

   a) Pre-despliegue y despliegue: Los nodos sensores pueden ser arrojados en masa o colocados uno por uno en el campo sensor.

b) Post-despliegue: Después del despliegue, los cambios de topología son debidos a cambios en la posición de los nodos sensores, accesibilidad, energía disponible, funcionamiento defectuoso y detalles de las tareas encomendadas.

c) Despliegue de nodos adicionales: Nodos sensores adicionales pueden ser desplegados en cualquier momento para reemplazar nodos defectuosos o debido a cambios en la dinámica de las tareas.

6. Entorno: Los nodos sensores son desplegados densamente muy cerca o directamente en el interior del fenómeno a ser observado. Por consiguiente, normalmente trabajan desatendidos en áreas geográficas remotas. Pueden estar trabajando en el interior de maquinaria grande, en el fondo del océano, en un área contaminada biológicamente o químicamente, en un campo de batalla más allá de las líneas enemigas, así como en edificios y hogares.

7. Medio de transmisión: En una red de sensores multisalto, los nodos de comunicaciones están conectados mediante un medio inalámbrico. Estas conexiones pueden estar formadas por medios vía radio, infrarrojo u óptico, aunque la gran mayoría del hardware actual para redes de sensores está basado en RF (Radio frecuencia).

   Otro posible modo de comunicación entre nodos en redes de sensores es mediante infrarrojos. La comunicación por infrarrojos no necesita licencia y es robusta frente a interferencias producidas por dispositivos eléctricos. Los transceptores basados en infrarrojos son baratos y fáciles de construir.

8. Consumo energético: los nodos sensores inalámbricos están equipados con una fuente energética limitada (0.5 A, 1.2V). En los escenarios de algunas aplicaciones la recarga de los recursos energéticos puede ser imposible. El tiempo de vida de los nodos sensores, en consecuencia, muestra una gran dependencia del tiempo de vida de la batería.

   El funcionamiento defectuoso de algunos nodos puede causar cambios de topología significativos y puede requerir re-enrutamiento de los paquetes y reorganización de la red. De aquí que, la conservación y administración energética tomen una importancia adicional.

   Observando las amenazas básicas que afectan a un sistema que pretende garantizar la seguridad de la información, en este apartado se particulariza al contexto de las redes inalámbricas de sensores.

La principal característica que va a orientar los ataques a estas redes consiste en la naturaleza del medio de comunicación. Las comunicaciones inalámbricas utilizan el espectro electromagnético, por lo que un atacante con la cobertura adecuada podría interceptar la información sin ser detectado.

Aunado a eso, muchas de las aplicaciones de este tipo de redes se desarrollan en entornos no controlados e incluso hostiles, por lo que la seguridad física de los sensores tampoco puede controlarse.

De estos factores se deriva la mayor parte de los riesgos, los cuales afectarán a la información y a la infraestructura. Las medidas de seguridad han de disponer de los mecanismos necesarios para preservar los siguientes aspectos:

a) La confidencialidad, debido a la facilidad de acceder al canal de comunicación.
b) La autenticidad de la información, ya que se transmite por el aire a todos los dispositivos dentro del área de influencia del emisor.
c) La integridad de la información transmitida, para evitar modificaciones accidentales o malintencionadas.
d) La vigencia de la información, para evitar la retransmisión de la información obsoleta.
e) La disponibilidad del canal y de los nodos, evitando ataques de denegación de servicio.
f) El acceso lógico a la red, el cual debe ser exclusivo a los nodos designados.
g) La captura de algún nodo, siendo necesario que el acceso físico al mismo no permita acceder a la información que contiene.
h) Evitar la suplantación de los nodos por dispositivos malintencionados, los cuales pueden afectar la integridad mediante la inyección de información falsa o a la disponibilidad de la red, impidiendo el paso de mensajes legítimos o provocando un consumo descontrolado de los recursos de los nodos.

A continuación se muestran las vulnerabilidades que existen en redes ZigBee.

a) Capa Física. La principal vulnerabilidad en este ámbito se debe a la imposibilidad de asegurar el entorno físico del sensor. Muchas de las aplicaciones de las redes de sensores requieren un despliegue masivo de los mismos sobre entornos desatendidos, por lo que no es posible aplicar medidas preventivas. Si un atacante tiene acceso físico a un nodo, nada le impide destruirlo o capturarlo.

Otra debilidad inherente a la capa física afecta directamente al medio de transmisión, las interferencias de radio, que pueden ser tanto intencionadas como accidentales. En entornos industriales, la posibilidad de interferencia debido a maquinaria y otros dispositivos es muy elevada, lo que refuerza la idea de implementar un mecanismo que garantice un medio libre de ruidos.

Adicionalmente, la emisión intencionada de interferencias, denominada jamming (interferencia o bloqueo), pueden deshabilitar por completo un red sin necesidad de tener una ubicación próxima o disponer de información sobre los protocolos de comunicación que intervienen. Estos tipos de ataques en los que se ocupa el canal de manera continua suelen ser muy ruidosos y fácilmente detectables.

Por otro lado, el jamming reactivo, el cual escucha el canal para provocar colisiones cuando algún sensor emite datos, puede pasar inadvertido, por lo que no se podrán tomar medidas para mitigar el impacto. Existen estudios que plantean una serie de soluciones para evitar este hecho de manera eficiente identificando los nodos legítimos que provocan la acción de los jammers y modificando su rol dentro de la red.

Además del efecto inmediato a la disponibilidad del canal de comunicación, estos ataques pueden devenir en que se agoten las baterías de los nodos, debido al intento de retransmisión de las tramas.

El estándar IEEE 802.15.4 establece el uso de DSSS (Direct Sequence Spread Spectrum – Espectro Ensanchado por Secuencia Directa) en la modulación, la cual presenta resistencia frente al jamming, tanto intencionado como accidental, entre otras ventajas. En un nivel superior, hace uso de CSMA/CA y GTS para evitar colisiones además de una etapa de evaluación del canal antes de transmitir CCA (Clear Channel Assesment – Canales Limpios de Evaluación).

Principales ataques en la capa MAC.

Los ataques a nivel MAC requieren mayor conocimiento de la topología y funcionamiento de la red objetivo. Se consideran más sofisticados, aunque en muchos casos requieren un perfil de ataque de insider (intruso).

Basado en el efecto comentado sobre el agotamiento de las baterías, surge el sleep deprivation torture insider (ataque de interrupción del sueño).

Esencialmente se provocan colisiones intencionadas y continuadas para que se retransmita la información, sin permitir que el nodo pase al estado de espera. Para lograr esto puede utilizarse jamming o información legítima, como la inyección de tramas NAK (Negative Acknoledgement-Reconocimiento negativo), aunque el receptor haya recibido correctamente los datos.

Utilizando una técnica similar a ésta se encuentran los ataques de repetición, en los que se utilizan tramas legítimas utilizadas anteriormente, como un beacon (baliza), y se vuelven a transmitir. Esto provoca que la integridad de la información se vea comprometida. Lógicamente, el estándar IEEE 802.15.4 mantiene un esquema de numeración secuencial para evitar este tipo de situaciones.

Un ataque que se puede presentar es el ataque Sybil (llamado así por la protagonista de un libro sobre una mujer con desorden de personalidades múltiples) en donde un nodo malicioso presenta numerosas identidades a la red invalidando la información de los nodos legítimos y modificando la información de ruteo (Figura 4.2).

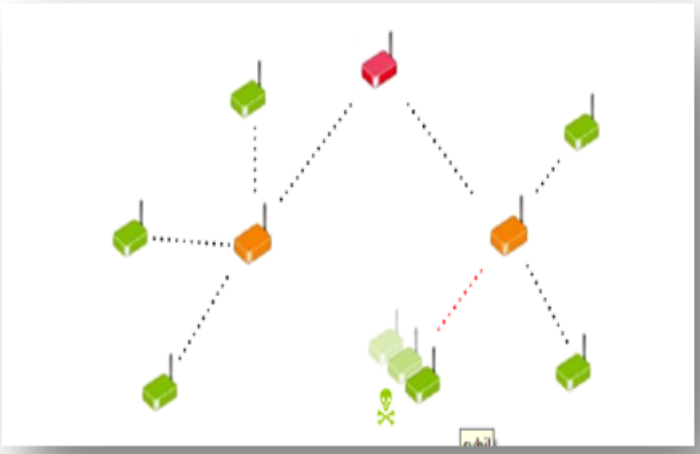


Figura 4.2 Ataque Sybil.

Principales ataques en la capa de red

En esta capa los ataques son llevados a cabo por insiders que funcionan como enrutadores (FFD sin ser coordinador), ya que afectan a los algoritmos de ruteo de la red. Esencialmente falsifican esta información para provocar la indisponibilidad de la red, entorpeciendo el diagnóstico.

Un ataque que caracteriza este comportamiento es el sinkhole (sumidero). Un nodo comprometido presenta rutas de muy buena calidad entre diferentes partes de la red. Esto provoca que toda la información que circule por él se pierda. Se convierte en un sumidero de información y son muy difíciles de detectar, sobre todo si se hace una selección de la información que es retenida. Lo más recomendable es asegurar que no existan nodos autenticados en la red (Figura 4.3).

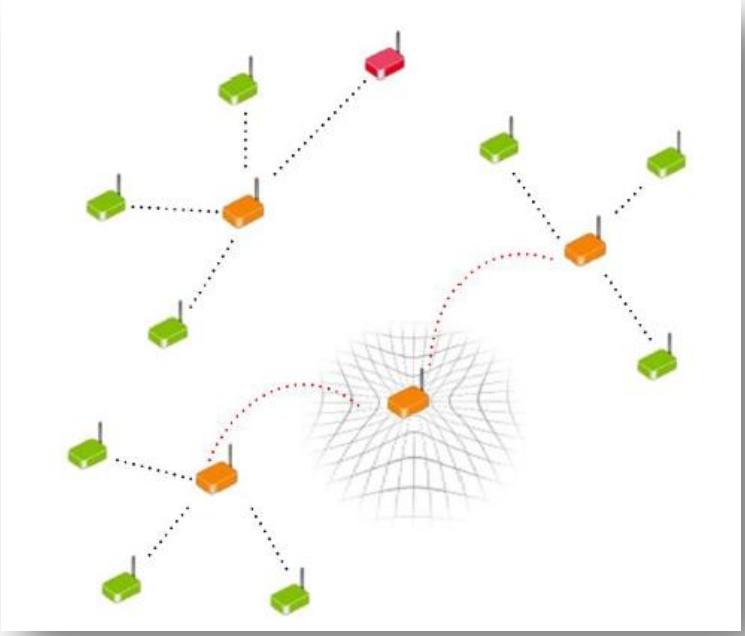


Figura 4.3 Ataque sinkhole.

Existe una variación más sofisticada de este ataque, en la que se utilizan enlaces fuera de banda de baja latencia para falsear la distancia entre los nodos, ya que se tuneliza la información. Esto genera sinkholes, difíciles de detectar como se ha comentado, e inmunes a la solución propuesta en el caso anterior.

Los nodos malintencionados no requieren formar parte de la red, ni tener una identidad en la comunicación. Simplemente actuando como relays (relevos) pueden modificar la información de ruteo, aún empleando criptografía y autenticación. Frente a este tipo de amenazas se han desarrollado algoritmos que tienen en cuenta la localización geográfica de los motes para realizar el ruteo (Figura 4.4).

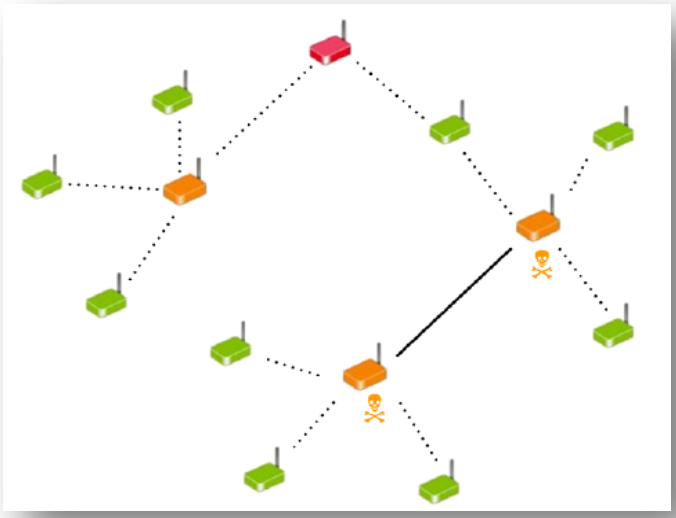


Figura 4.4 Variación del ataque sinkhole.

Utilizando una antena de alta ganancia se podría llevar a cabo otro tipo de ataque para confundir a la red. Presentándose como vecino de un número de sensores, cuando éstos no tienen la capacidad de emisión suficiente para comunicarse con la antena se denomina Hollo flood y provoca el consumo de las baterías, ya que los nodos tratan de responder al anuncio, emitiendo señales al vacío (Figura 4.5).

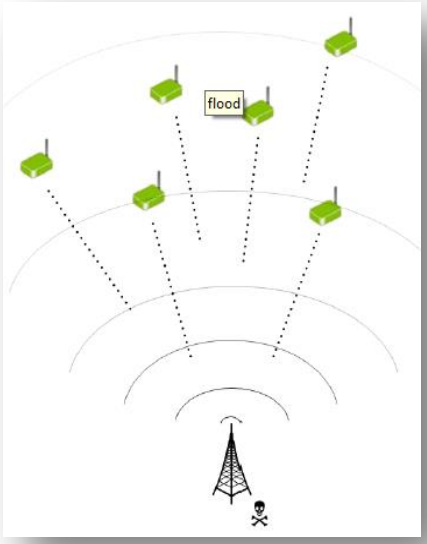


Figura 4.5 Hollo flood.

b) Vulnerabilidades de capa de aplicación.

En esta capa, las vulnerabilidades asociadas a las aplicaciones dependen de la implementación de las mismas, así como en aplicaciones de otras plataformas, es posible explotar los problemas ocasionados por desbordamiento de buffers, memory leaks (pérdida de memoria) o inyección de parámetros. Estos ataques escapan del ámbito de este estudio por la diversidad de los mismos y porque son fuertemente dependientes de la propia aplicación.

Un problema común será el consumo de recursos asociados al número de conexiones que se establezcan en las aplicaciones, por lo que se deberán provisionar mecanismos para gestionar el número de conexiones permitidas.

4.2 Seguridad para redes ZigBee.

Como se ha visto, el número y naturaleza de las amenazas y ataques es muy elevada y puede parecer inabarcable abordar todos estos problemas. Hay que destacar que la mayoría de estos ataques presuponen que se tiene acceso lógico a la red de sensores. Sin este acceso, la explotación práctica de los ataques es muy complicada, si no imposible, por lo que los esfuerzos han de enfocarse en evitar que un nodo cualquiera pueda asociarse a una red establecida.

Para ello, el estándar IEEE 802.15.4 establece una serie de medidas que permitirán autenticar a los dispositivos que formen parte de la red, inhabilitando la asociación de aquellos que no estén autorizados. En este apartado se describen esas funcionalidades, que son el objeto de estudio de este proyecto.

El estándar establece el algoritmo de cifrado que debe utilizarse en las operaciones criptográficas, sin embargo, no específica cómo han de gestionarse las claves o las políticas de autenticación que deben aplicarse. Estas tareas deben ser tratadas por las capas superiores, gestionadas por ZigBee.

La seguridad se obtiene del cifrado simétrico, el cual cubrirá los requisitos de confidencialidad e integridad. El algoritmo de cifrado usado es AES (Advanced Encryption Standard – Cifrado Estándar Avanzado) con una longitud de claves de 128 bits (16 Bytes). Este algoritmo no sólo se utiliza para cifrar la información, sino también para validarla. Mediante un código de integridad del mensaje (MIC), también denominado código de autenticación del mensaje (MAC) añadido al final del mensaje, se consigue dotar de integridad a las comunicaciones. Este código asegura la integridad de la cabecera MAC y del payload, a la vez que asegura que el emisor es quien dice ser. Se construye cifrando ciertas partes de la cabecera Mac con la clave que establezca la política de gestión de claves, y que será conocida por los nodos que se estén comunicando. Si se recibe una trama de algún nodo no confiable, el código MIC (Código de integración de mensajes) generado no corresponde con el que fue enviado en la trama, al haberse generado con una clave diferente. El MIC puede tener varios tamaños, 32, 64 y 128 bits, aunque siempre se construye utilizando el algoritmo AES de 128 bits. Este tamaño únicamente indica cuántos bits se añadirán al final de cada trama.

La confidencialidad de las comunicaciones se conseguirá cifrando el contenido del payload mediante el algoritmo AES y una clave de 128 bits.

Para gestionar estas operaciones de seguridad, es necesaria una serie de campos de las tramas IEEE 802.15.4 mostrados en la Figura 4.6.

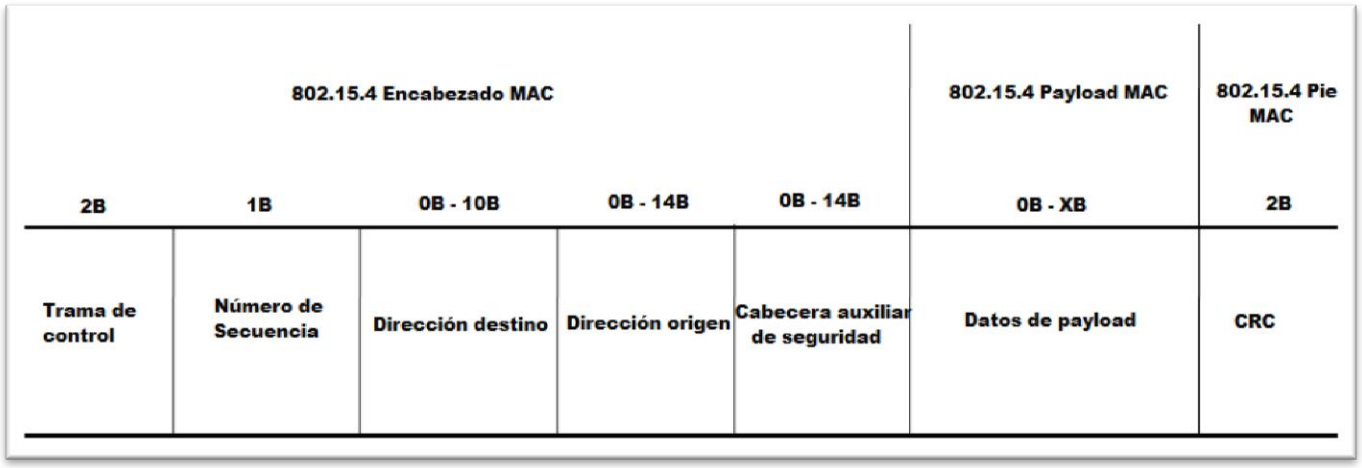
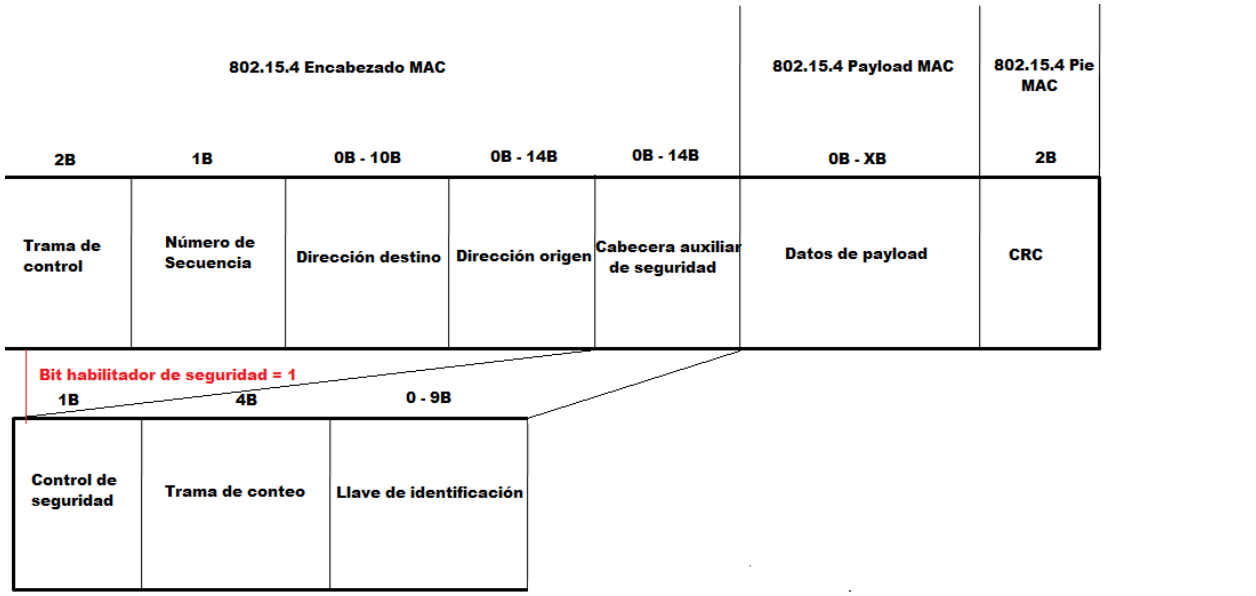


Figura 4.6 Trama IEEE 802.15.4.

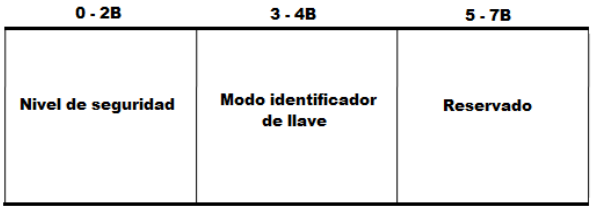
Los principales campos de la trama son:

a) Control de trama. Se encuentra ubicado en la cabecera MAC.
b) Cabecera auxiliar de seguridad. Se encuentra localizado en la cabecera MAC.
c) Data Payload. Ubicado en el campo de datos MAC.
d) Control de Seguridad. Indica el nivel de seguridad seleccionado para esta trama.
e) Contador de trama. Es un contador proporcionado por el emisor de la trama para proteger ante ataques de repetición. Por esta razón, cada mensaje tiene un número de secuencia único representado por este campo, no necesariamente correlativo.
f) Identificador de llave. Especifica la información necesaria para seleccionar la clave en el nodo receptor. Los nodos han de contener las mismas claves, organizadas de la misma manera.

Esta trama también cuenta con campos que permiten aportar seguridad dividido en control de seguridad y llave de identificación (Figura 4.7).



Control de Seguridad



Llave de identificación

Figura 4.7 Organización de claves para los nodos.

El subcampo control de seguridad es el lugar donde se ubica la política de seguridad, que seleccionará el modo de funcionamiento de AES, y el modo de identificación de la clave, que puede ser implícito o explícito. El resto del espacio está reservado para posibles ampliaciones.

Los valores posibles del modo identificador de llave son:

a) 0, el valor de la clave es conocido de manera implícita por el emisor y el receptor, por lo que no se específica en este mensaje.
b) 1, la identificación de la clave se realiza de manera explícita con el byte del índice llave y el parámetro estático macDefaultKeyStore.
c) 2, la identificación de la clave se realiza de manera explícita con el byte de Key index y los 4 bytes de Key Source.
d) 3, la identificación de la clave se realiza de manera explícita con el byte de Key index y los 6 bytes de Key Source.

Según esta configuración, el número máximo de claves que pueden utilizarse es de 2^n claves, lo que implicaría un consumo máximo de memoria para las claves de 2^{72} x 16B, lo que no es factible en ningún sistema. Lo importante de este aspecto no es el número en sí, sino que el número es suficientemente grande para que sea escalable a diferentes políticas de gestión de claves.

La implementación que se hace de la seguridad indica que ésta se efectúa a razón de cada trama. Esto quiere decir que un receptor, para cada trama recibida, tendrá que seleccionar la clave correspondiente, actualizar los valores de contador y realizar la operación criptográfica correspondiente. Teóricamente, un mismo nodo emisor podrá enviar dos tramas diferentes a un mismo receptor con niveles de seguridad distintos, lo que aporta una gran flexibilidad. Por ejemplo, se podrán evitar tramas baliza garantizando la identidad del coordinador, pero sin cifrar el contenido, y utilizar un cifrado completo en caso de enviar tramas de datos.

Otra opción que se utiliza para aportar seguridad a las redes ZigBee son los niveles de seguridad que ofrece IEEE 802.15.4 los cuales se especifican en el subcampo Security level (Nivel de seguridad) de la cabecera auxiliar de seguridad. Estos niveles definen el modo de funcionamiento del algoritmo AES, proporcionando autentificación, confidencialidad o ambas.

Los 3 bits de este campo permiten seleccionar entre 7 niveles de seguridad, desde lo más bajo, que no realiza ninguna operación criptográfica, hasta el nivel que ofrece más garantías. Estos niveles se muestran en la Tabla 4.1.

Tabla 4.1 Operaciones criptográficas.

Valor	Cifrado	Operación
0	Sin seguridad	Datos en claro. Autenticación sin validar
1	AES-CBC-MAC-32	Datos en claro. Autenticación validada
2	AES-CBC-MAC-64	Datos en claro. Autenticación validada
3	AES-CBC-MAC-128	Datos en claro. Autenticación validada
4	AES-CTR	Datos en claro. Autenticación sin validar
5	AES-CCM-32	Datos en claro. Autenticación validada
6	AES-CCM-64	Datos en claro. Autenticación validada
7	AES-CCM-128	Datos en claro. Autenticación validada

Esencialmente, lo que indica la tabla 4.1 es que existen 3 modos diferenciados de realizar las operaciones criptográficas, y que aportarán funcionalidades diferentes. En los siguientes incisos se detalla el funcionamiento y particularidades de cada modo de funcionamiento.

a) Modo CBC-MAC. El primero de estos modos se utilizará para autenticar los mensajes, como indica el acrónimo MAC. Cada bloque toma como entradas el resultado de su mensaje anterior y el bloque de mensaje correspondiente para generar un bloque del mismo tamaño con la información cifrada, con excepción del primer bloque, que se inicializa a 0 (vea Figura 4.8).

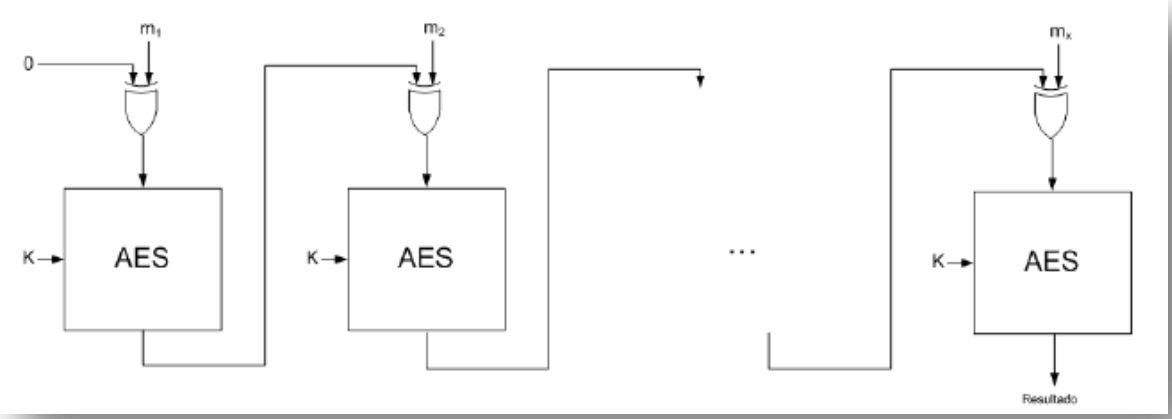


Figura 4.8 Modo CBC-MAC.

De esta manera, al final se obtendrán 128 bits generados a partir del mensaje y la clave, formando un resumen o hash criptográfico del mensaje. Este resultado se anexa al mensaje que se pretende enviar. Cuando el receptor quiere comprobar la validez del mensaje, sólo tiene que realizar el mismo cálculo y compararlo con el resumen anexado. Si coincide, significa que quien ha enviado el mensaje conoce la clave de cifrado y que el mensaje no ha sido modificado en tránsito. De esta manera se obtiene autenticación e integridad.

b) Modo CTR. Llamado así porque hace uso de un contador como vector de inicialización, se utiliza para cifrar el contenido de los mensajes, aportando confidencialidad. A cada bloque del mensaje se le aplica una función XOR con la salida del cifrador, el cual ha generado un valor de 128 bits a partir de la clave y un vector de inicialización.
Este vector de inicialización, de 128 bits, está formado por un nonce (number used once – número usado una vez) y un contador de bloque, que se irá incrementando en función del bloque que tenga que cifrar. El nonce debe construirse con información conocida por el emisor y el receptor, y suele estar contenido en la cabecera de la trama a enviar. El motivo de esta configuración es para evitar que mensajes idénticos resulten en mensajes cifrados idénticos, ya que esos mensajes serían susceptibles al criptoanálisis y la rotura del cifrado. Los bloques se cifran de manera independiente, por lo que podría aprovecharse el paralelismo para cifrar todos los bloques simultáneamente (Vea Figura 4.9).

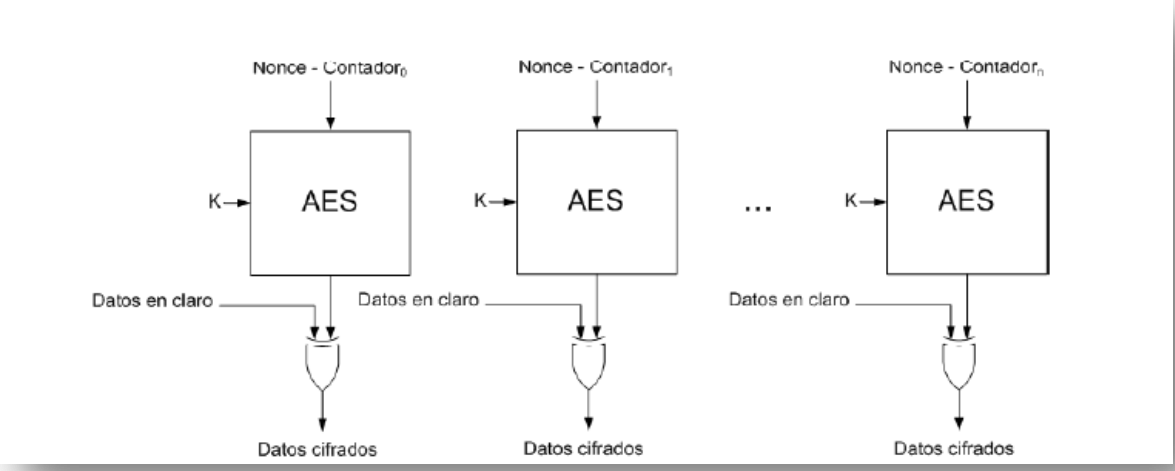


Figura 4.9 Modo CTR.

c) Modo CCM. Este modo combina los dos modos en uno solo, aportando confidencialidad, autenticación e integridad. El costo de esto es que ha de realizar dos pasadas sobre el mensaje; la primera de ellas para generar el MIC, y una segunda para cifrar el payload y el MIC. La única diferencia es que en el cálculo del MIC, el vector de inicialización corresponde con el que se utilizará en el cifrado (Vea Figura 4.10).

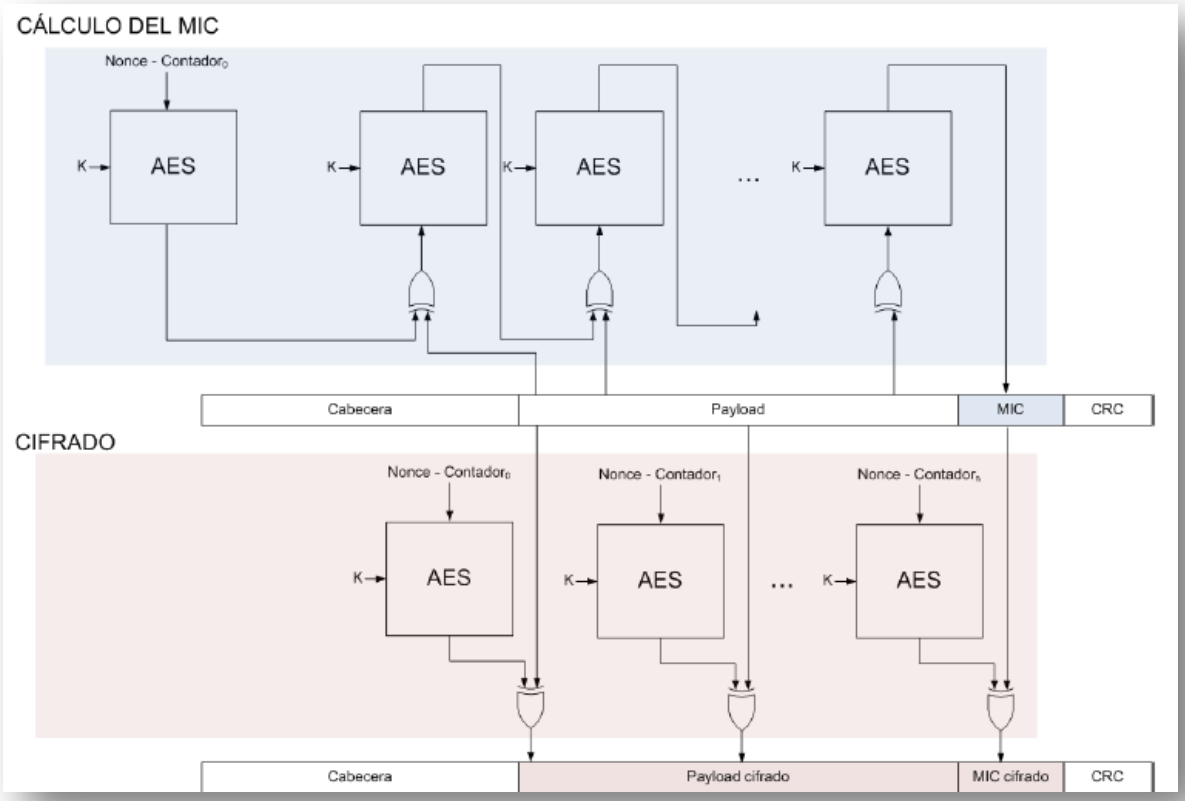


Figura 4.10 Modo CCM.

4.3 Políticas de seguridad para redes ZigBee.

Una vez teniendo en cuenta las posibilidades de seguridad que ofrece ZigBee, es necesario elaborar las políticas de seguridad adecuadas para garantizar un buen uso de esta tecnología. Las redes de sensores inalámbricos son un ámbito relativamente nuevo de las telecomunicaciones y por lo tanto no han alcanzado una madurez como la que se tiene en Wi-Fi o en Bluetooth. Una consecuencia de ello es que las directivas de seguridad aún no están completamente definidas y se espera con impaciencia su desarrollo.

A continuación se listan políticas de seguridad que se ha considerado son aplicables para la tecnología ZigBee.

1. Políticas para la red de sensores inalámbricos.

   a) Debido a que en los casos de diseño se considera una sola red de área personal el identificador de la PAN debe cambiarse cada cuatro meses y los cambios no deben seguir ningún patrón fácil de descifrar.
   b) El identificador del nodo en la red de sensores inalámbricos debe cambiarse cada cuatro meses.

   c) Respaldar el código implementado en la red luego de los cambios de identificador de PAN y de nodo.

   d) Está prohibida la divulgación de información relacionada con la red de sensores inalámbricos con personal que no sea el interno a la empresa.

2. Políticas para el sistema de control.

   a) Respaldar los procedimientos programados en el sistema de control cada cuatro meses.

   b) No divulgar información acerca del modo de operación del sistema de control a personal externo.

3. Políticas para la base de datos.

   a) Cambiar el usuario y la clave del administrador de la base de datos cada seis meses.

   b) Realizar respaldos de la base de datos del sistema cada dos meses.

   c) Mantener oculta información de la base de datos a personal que no esté directamente relacionado con la misma.

4. Políticas para la publicación web.

   a) Verificar cada dos meses que las políticas de acceso sólo permitan acceder a los servicios necesarios como lo es un firewall.

   b) Respaldar las configuraciones de los equipos que brinden seguridad al sistema cada dos meses.

c) Mantener de forma confidencial información de la seguridad TCP/IP del sistema.

5. Políticas para el sistema en general.

a) Resguardar las instalaciones de todo el sistema de personal no autorizado.

b) Respaldar todos los datos en otro lugar cada seis meses.

c) Realizar capacitación de políticas de seguridad al personal cada seis meses.

CAPÍTULO 5.

BUENAS PRÁCTICAS PARA EL DISEÑO DE UNA RED ZIGBEE

5.1 Requerimientos para una red ZigBee.

Antes de comenzar cualquier proyecto es necesario hacer un análisis adecuado de cuáles son las necesidades que se desean satisfacer y de esta forma presentar una propuesta adecuada para resolver cualquier tipo de problema o dificultad.

En este caso se desea hacer una red inalámbrica utilizando s el protocolo ZigBee por lo que es muy importante tomar en cuenta diversos factores, en primer lugar que es lo que se va requerir para poder realizar una red que cumpla con las características mencionadas en los capítulos anteriores, en que espacio físico se instalarán los dispositivos necesarios, hardware, software y algo muy importante como se protegerá la comunicación de información.

Como se mencionó en capítulos anteriores ZigBee Alliance define tres tipos diferentes de dispositivos ZigBee según el papel que cumplen en la red.

Un coordinador ZigBee. El tipo de dispositivo más completo. Existe uno por red, independientemente de la topología utilizada. Es el encargado de iniciar la formación de la red y selecciona la frecuencia del canal a ser usado. Es el responsable de la asociación y desasociación de dispositivos.

Router ZigBee. Interconecta dispositivos separados en la topología de la red. Puede actuar como coordinador. Se asocia con el coordinador de la red o con otro router ZigBee. Es capaz e enrutar mensajes entre dispositivos y soportar asociaciones. El router no puede estar en estado de sleep.

Dispositivo final. Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o router), pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías. Tiene requerimientos mínimos de memoria y es por tanto significativamente más barato. Los dispositivos finales están siempre localizados en los extremos de la red.

Sabiendo lo anterior una nueva red ZigBee es establecida por un coordinador. Al inicializarse, el coordinador busca otros coordinadores en sus canales permitidos, basado en la energía del canal y el número de redes encontradas en sus canales, establece su propia red y selecciona un identificador PAN único de 16 bits. Una vez que la nueva red ha sido establecida, los ruteadores y terminales son habilitados a

unirse a red. En caso de conflictos por PAN ID repetidos en diferentes coordinadores, se efectúa un procedimiento de resolución que cambiará en uno de los coordinadores su identificador.

Los distintos dispositivos guardan información acerca de otros nodos de la red, en un área no volátil de memoria llamada tabla de vecindades. Al inicializarse, si un dispositivo determina a través de la tabla que fue parte de una red, puede ejecutar un procedimiento de notificación para localizarla. Los dispositivos que reciban la notificación, verificarán sus tablas para cerciorarse de que el nuevo dispositivo pertenecía a su red. Si la notificación falla o el dispositivo no se encuentra en las tablas de vecindad del resto, tratará de unirse a una de las redes como un nuevo dispositivo.

Una vez en la red, un dispositivo puede desasociarse ya sea por pedido del coordinador o router o por sí mismo.

5.2 Análisis del espacio para su instalación.

Una de las posibilidades o una de las mejores características que tienen las redes ZigBee es que son de fácil instalación, puede crearse una red en diferentes tipos de espacios, de estructuras y no es necesario cambiar demasiado el entorno donde se haga la implementación.

Se puede poner por ejemplo la agricultura, en donde quizás se quieran saber diversos datos importantes como temperatura, humedad y otros datos que permitan obtener un monitoreo efectivo de lo que se haya sembrado.

Para hacer el análisis del espacio para este ejemplo se puede observar la figura 5.1.

Figura 5.1 Diferentes ejemplos de agricultura.

En esta figura se muestran dos ejemplos de agricultura una de ellas es a campo abierto y el otro es por medio de un invernadero por lo que el análisis para poder instalar una red de sensores se tienen que hacer consideraciones diferentes para que sea funcional.

En la figura de la izquierda se observa un campo abierto en el que se está desprotegido del medio ambiente, por lo que puede haber factores que afecten los dispositivos de la red, como lo pueden ser el aire, agua, la fauna que pudiera haber o simplemente el acceso de personas ajenas.

En cambio en la figura de la derecha se trata de un invernadero, lo que ofrece un ambiente controlado, el viento rebota en las paredes y no llega con tanta fuerza, el riego es artificial o controlado, y el acceso a otras personas no es tan sencillo a menos que entren por la fuerza o alguien les permita la entrada cuidando sus movimientos.

Todas estas características son de gran importancia ya que dependiendo del análisis que se haga será el impacto y buen funcionamiento de la red implementada, se hará un uso adecuado del espacio aprovechándolo al máximo, no se dañará el entorno, y arrojará la información que se desea obtener de manera correcta (Figura 5.2).

Figura 5.2 Diferentes entornos que podrían usar ZigBee.

5.3 Estructura de la red.

a) Topología en estrella.

Para este tipo de topología existe un dispositivo coordinador el cual se encarga de distribuir y controlar la información de un dispositivo final a otro por lo que si un dispositivo final necesita comunicarse con algún otro, primero necesita enviar información al coordinador central y este último se encarga de enviarla al destino correcto. Si el dispositivo central se llega a descomponer el intercambio de información se pierde.

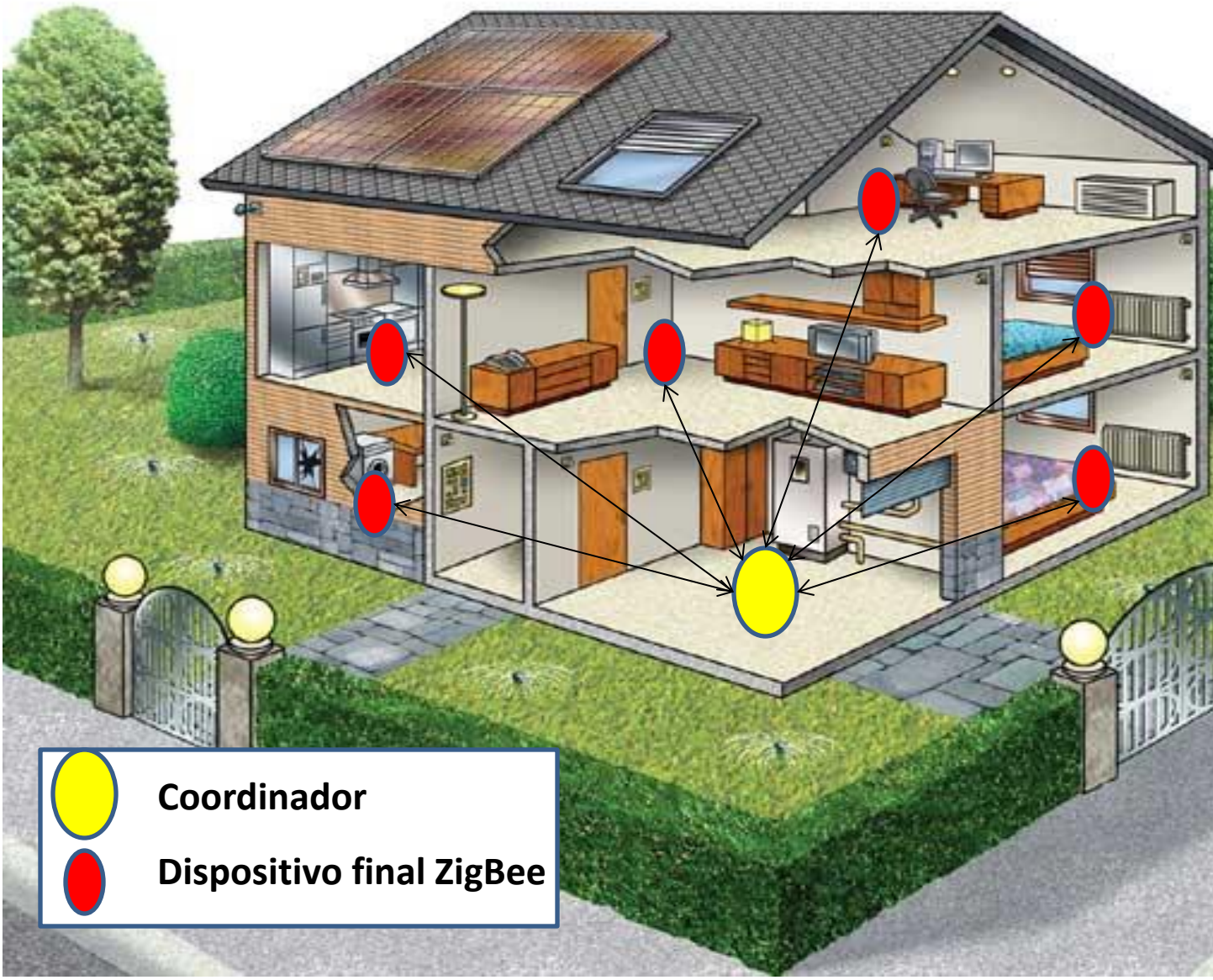


Figura 5.3 Red en estrella en casa inteligente.

En la figura 5.3 se muestra un ejemplo del uso de la red en estrella, un coordinador ZigBee permite una administración centralizada la cual permite tomar el control total de la red, ya sea control de energía, dispositivos de la cocina, dispositivos contra incendios o de cámaras de vigilancia, dispositivos de entretenimiento, aire acondicionado entre otras muchas posibilidades.

Topología en árbol.

Este tipo de topología permite que los dispositivos finales puedan estar unidos entre sí por medio de routers o coordinadores originando una red más amplia, más compleja y con un mayor número de dispositivos. Todos los mensajes se enrutan a lo largo del árbol por medio de los coordinadores y no se necesita un rango determinado de radio del coordinador.

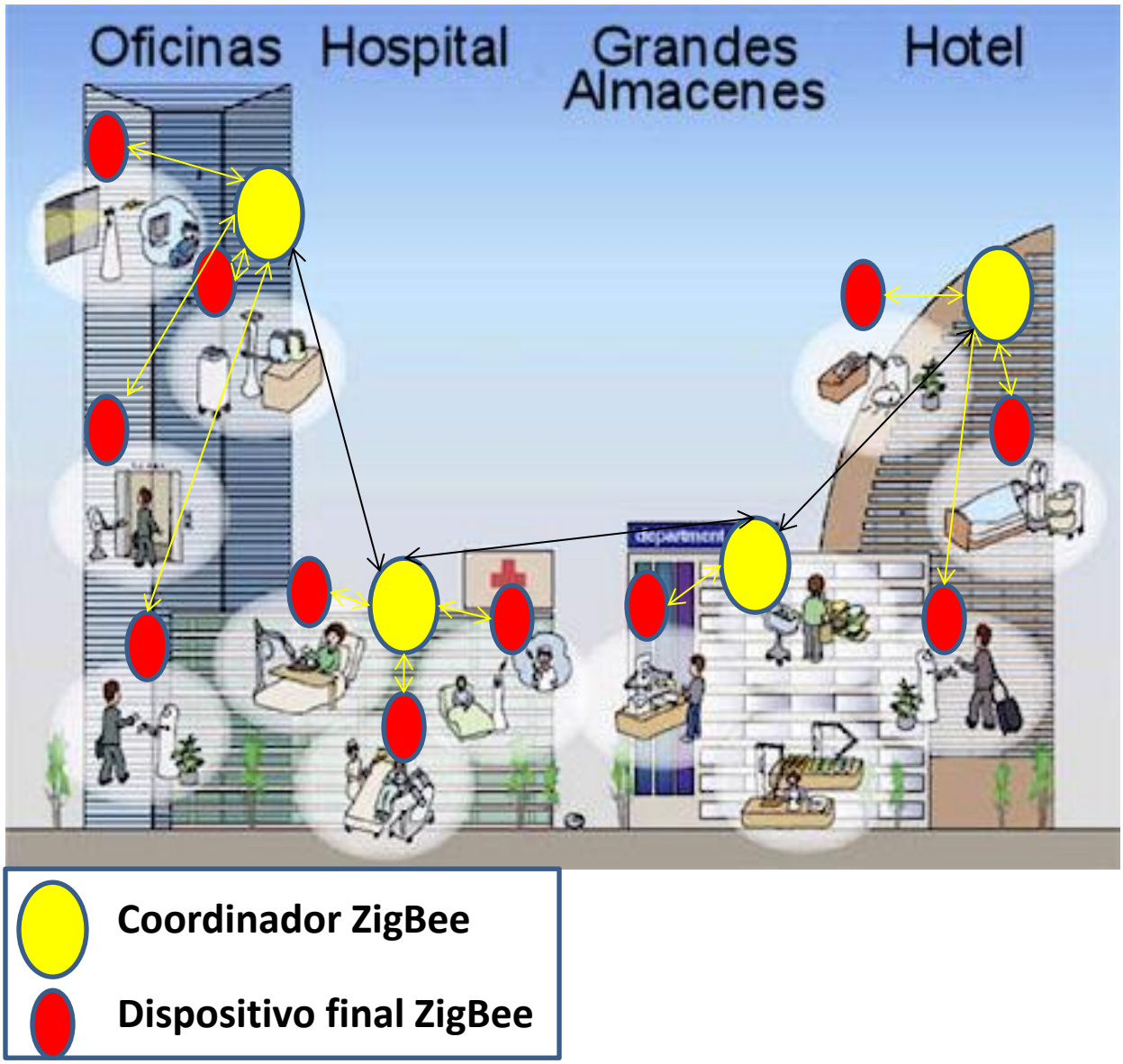


Figura 5.4 Red en árbol en edificios inteligentes.

En la Figura 5.4 se puede apreciar el uso de la topología en árbol en donde se puede llegar a utilizar un gran número de dispositivos y que por medio de los coordinadores la efectividad de este tipo de redes se ve alterada de forma positiva permitiendo un uso adecuado de los dispositivos tecnológicos de hoy día para diferentes tipos de construcciones y usos de dichos edificios.

b) Topología en malla.

Este tipo de topología es la más compleja de todas pero es la más confiable y usada en redes ZigBee debido a su característica principal que es la posibilidad de que un dispositivo final se puede comunicar con otro sin la necesidad de un coordinador o un router. Una red en malla es muy similar a una en árbol con la diferencia antes mencionada.

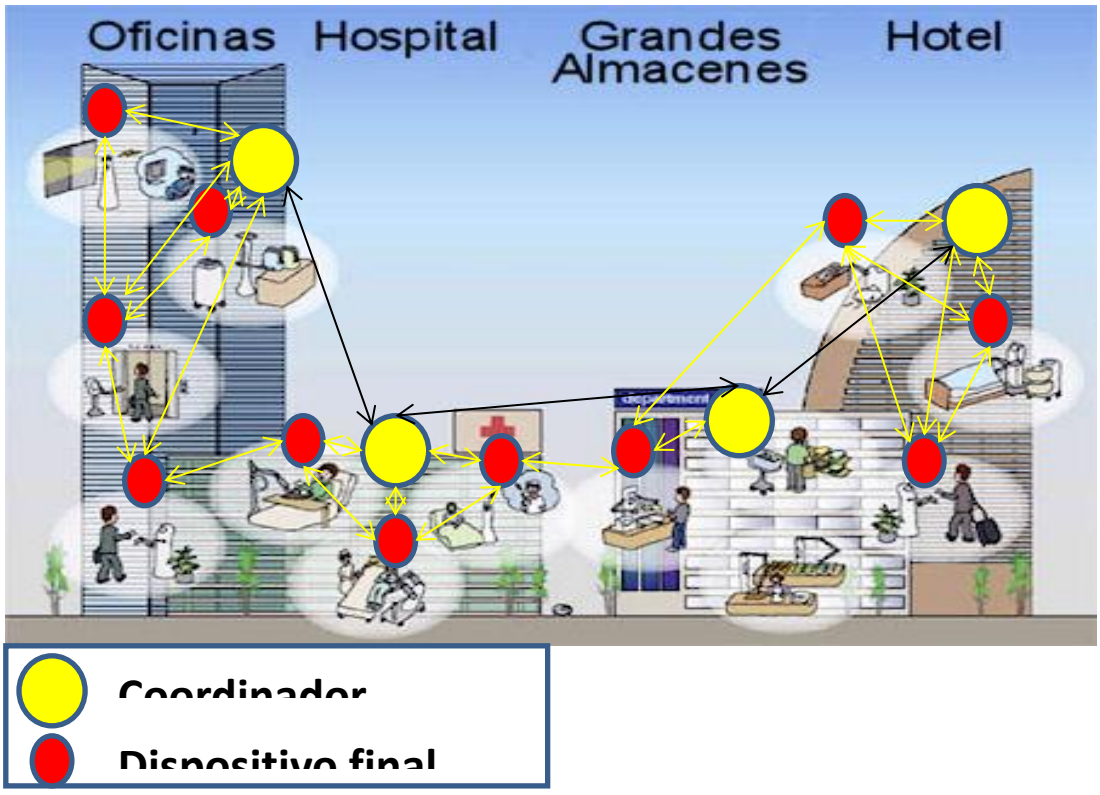


Figura 5.5 Red en malla en edificios inteligentes.

En la figura 5.5 se muestra la red en malla la cual como se puede observar es muy similar con la topología árbol solo que con la diferencia de que los dispositivos finales se pueden intercomunicar entre sí.

5.4 Hardware y Software necesario

En la implementación de una red ZigBee es muy importante realizar un análisis completo de que componentes son necesarios para que sea funcional de bajo costo y brinde los resultados esperados. Tanto los componentes físicos así como el software permiten una buena administración y una implementación relativamente sencilla.

Hardware.

El hardware debe incluir dispositivos para la transmisión y recepción de datos formando una red inalámbrica bajo el estándar ZigBee, permitir la interacción de las terminales con los transmisores de corriente de dos hilos que adquieren señales analógicas desde sensores industriales, permitir la comunicación entre los equipos de cómputo y los coordinadores ZigBee, proporcionar la interfaz necesaria para la programación del software requerido por los nodos y suministrar la energía requerida para el funcionamiento de los distintos módulos.

Desde que en el 2005 apareciera la primera especificación beta del protocolo ZigBee. No han dejado de surgir distintos tipo de dispositivos capaces de utilizar dicha tecnología.

En principio, para este tipo de dispositivos se consideró, que debido a su bajo costo de fabricación, el precio no sería muy superior a los 3.7 dólares por dispositivo. Así como, que se fabricaron cuarenta mil dispositivos durante su primer año de vida. Finalmente un dispositivo ZigBee tiene un costo de alrededor de 49.34 dólares, como mínimo.

ZigBee se trata de una tecnología en la que muchas empresas han puesto sus expectativas de futuro y por lo tanto, han aparecido multitud de dispositivos. Fabricando componentes de bajo nivel, que llevan embebido procesadores y sistemas capaces de trabajar con este protocolo, como dispositivos comerciales, listos para utilizar el protocolo directamente desde cualquier equipo de cómputo o teléfono móvil.

Dispositivos de bajo nivel.

Una de las empresas desarrolladoras de dispositivos ZigBee es una alianza entre dos, rfSolutions y Flexipanel. Está alianza ha permitido la creación de diversos dispositivos ZigBee, tanto de bajo nivel como de alto nivel.

Uno de esos dispositivos es el llamado EasyBee. Se trata de un transceptor RF que cumple con la IEEE 802.15.4. Preparado para trabajar dentro de una red ZigBee como un dispositivo final como el mostrado en la Figura 5.6.

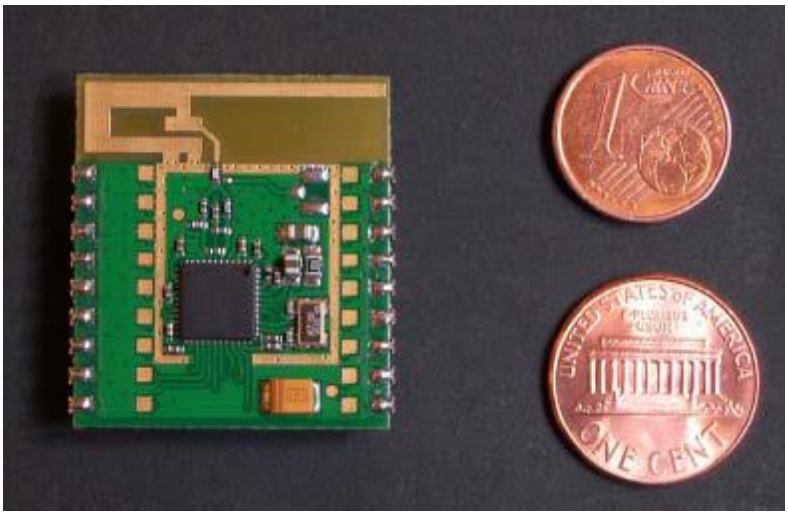


Figura 5.6 Dispositivo final.

Se trata de un dispositivo de reducidas dimensiones, tan sólo 26mmx20mm, con un consumo de energía de 2.1V a 3.6V y con capacidad para estar operativo en condiciones climáticas adversas, pues puede trabajar con temperaturas entre -40C y 85C. Además puede comunicarse con otros dispositivos ZigBee que se encuentren hasta 200 m de distancia, con una tasa de transferencia de datos de hasta 25kbps.

Las aplicaciones para la que se ha orientado este dispositivo son:

a) Reemplazar el cableado de cualquier red.
b) Viviendas automatizadas.
c) Redes y control industrial.
d) Sensores para redes inalámbricas.

Otro dispositivo creado por esta empresa es el denominado Pixie. Este dispositivo no es uno sólo, sino que se trata de una serie, hasta ahora compuesta por dos dispositivos. Orientados para ejercer el rol de Coordinador y Router, dentro de una red ZigBee. Dentro de la serie Pixie, han recibido el nombre de Pixie y Pixie Lite respectivamente (Figura 5.7).

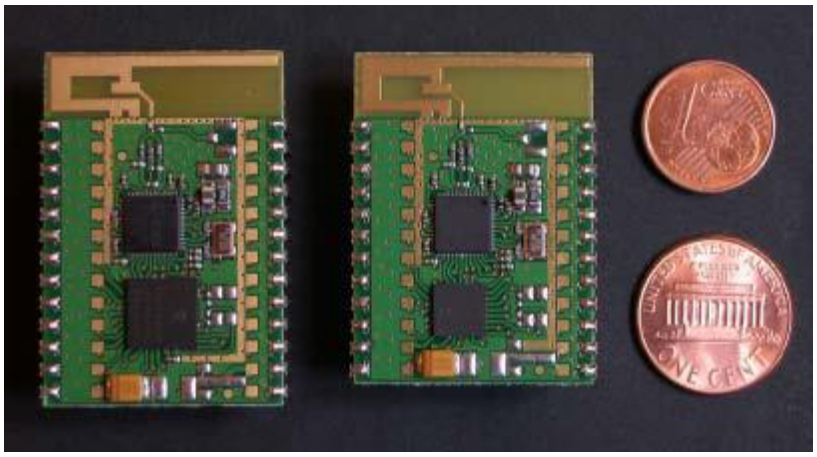


Figura 5.7 Dispositivo Pixie y Pixie Lite.

Ambos dispositivos tienen las características técnicas que el dispositivo final EasyBee, pero con mayor capacidad del procesamiento, lo que les permite ejercer como dispositivos más potentes que estos, dentro de una red ZigBee.

Estos dispositivos disponen de la posibilidad de ser conectados a una antena externa, lo que les otorgaría un alcance mucho mayor. Otro dispositivo elaborado por estas empresas es un cable de conexión USB, el cual es un cable con el que se puede conectar un ordenador a los dispositivos ZigBee desarrollados por estas empresas. Una vez conectado, el cable se convierte en una conexión serie a través de USB, desde donde podremos configurar y manejar los dispositivos ZigBee e incluso entrar a la red, en la que se encuentre el dispositivo al que nos encontremos conectados. El dispositivo se llama Pixie Configuration Tool (Figura 5.8).

Figura 5.8 Dispositivo de conexión USB.

El producto más completo orientado a desarrolladores se denomina Pixie Evaluation Kit. Con este producto cualquier desarrollador interesado en esta tecnología (protocolo) podrá probar físicamente sus diseños de dispositivos XigBee.Así como trabajar directamente sobre los dispositivos ofertados por estas empresas, con los que es totalmente compatible. Esto permitirá el control total de los dispositivos, así como su programación directa y análisis de su funcionamiento (Figura 5.9).

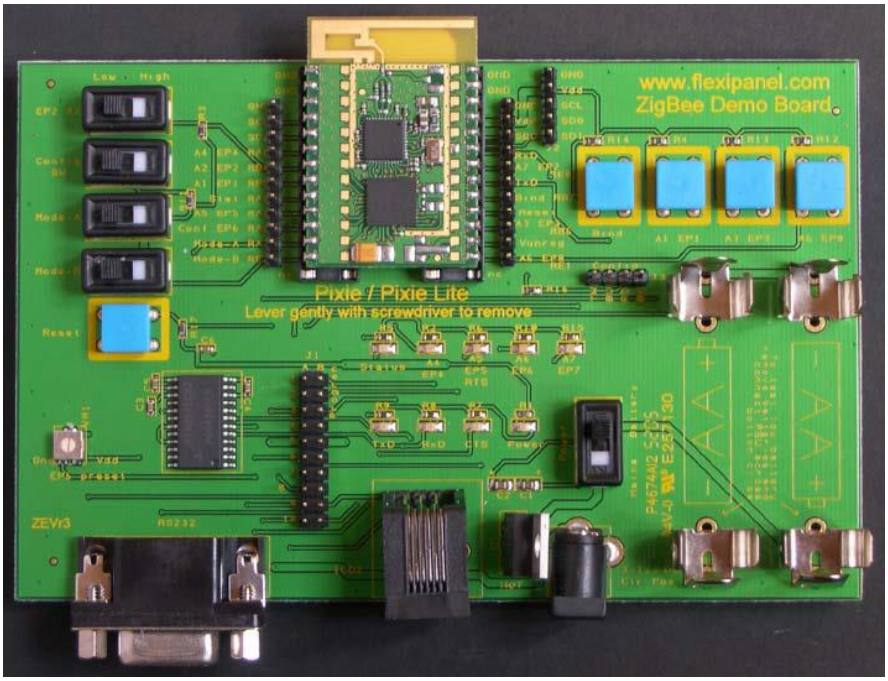


Figura 5.9 Pixie Evaluation Kit.

Otra empresa desarrolladora de dispositivos ZigBee es Telegesis. Esta empresa dispone de dispositivos que implementan el protocolo ZigBee, pero que pueden ejercer dispositivos finales para una red ZigBee, así como de Routers y Coordinadores. Así como un kit de desarrollo bajado en sus dispositivos.

Uno de esos dispositivos es ETRX1 el cual es de bajo costo y preparado para ser ingresado a una red ZigBee. Sus dimensiones son 27.75x20.45mm, un consumo ligeramente superior 2.7V a 3.6V y mismas características físicas para trabajar a temperaturas de entre -40C y 85C. Pero aun siendo más grandes y consumir más, hay que tener en cuenta que se trata de un dispositivo que puede ejercer, tanto de dispositivo final, como de Coordinador.

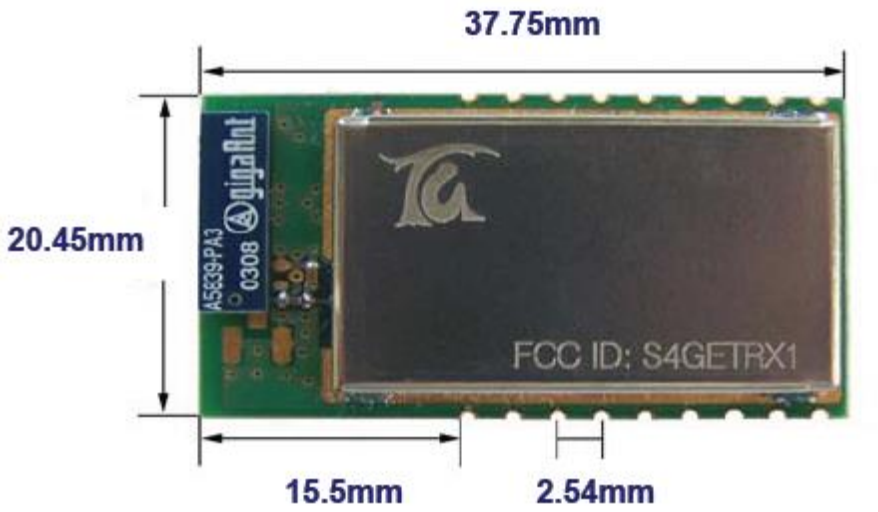


Figura 5.10 Dispositivo ETRX1.

Este dispositivo está orientado a:

a) Lectura automática de métricas.
b) Alarmas inalámbricas y seguridad.
c) Viviendas automatizadas.
d) Sensores de presencia inalámbricos.
e) Control industrial.
f) Periféricos de PC.

El dispositivo ETRX2 es algo menos económico, dispone de 128k de memoria flash y otros 5kbytes de SRAM. Lo que le permite poder actuar como cualquier tipo de dispositivo dentro de una red ZigBee. Añadiendo además la posibilidad de tres tipos de antenas simultáneas conectadas al dispositivo, lo que haría que la conexión se pudiese dar a distancias muy superiores que las indicadas en el estándar del protocolo (Figura 5.11).

Sus aplicaciones son:

a) Lectura automática de métricas.
b) Alarmas inalámbricas y seguridad.
c) Viviendas automatizadas.
d) Sensores de presencia inalámbricos.
e) Control industrial.
f) Periféricos de PC.
g) Controles industriales M2M.
h) Diversos sistemas ZigBee.

Figura 5.11 Dispositivo ETRX2.

Para poder programar ambos dispositivos se dispone de una interfaz en línea de comandos, intuitiva y sencilla. Lo que hace que no sea necesaria mucha experiencia en módulos RF para su programación.

Dispositivos de alto nivel.

Son los dispositivos ZigBee desarrollados, que son totalmente independientes y que no están compuestos sólo por los componentes electrónicos que soportan el estándar, sino que además ya disponen de interfaz que nos permite trabajar con ellos directamente sobre redes ZigBee.

Telegesis desarrollo un dispositivo ZigBee que es totalmente operativo, dentro de un Pendrive o dispositivo USB. Basado en la tecnología de su dispositivo de bajo nivel ETRX1 y posteriormente ETRX2, recibe el nombre de ETRX1USB y ETRX2USB respectivamente. Y se trata de un dispositivo que trabaja en la banda de frecuencia de los 2.4GHz, con alcance de hasta 100m de distancia para encontrar otros dispositivos ZigBee, antena omnidireccional y capacidad de utilizar hasta 16 canales para las búsquedas de dispositivos (Figura 5.12).

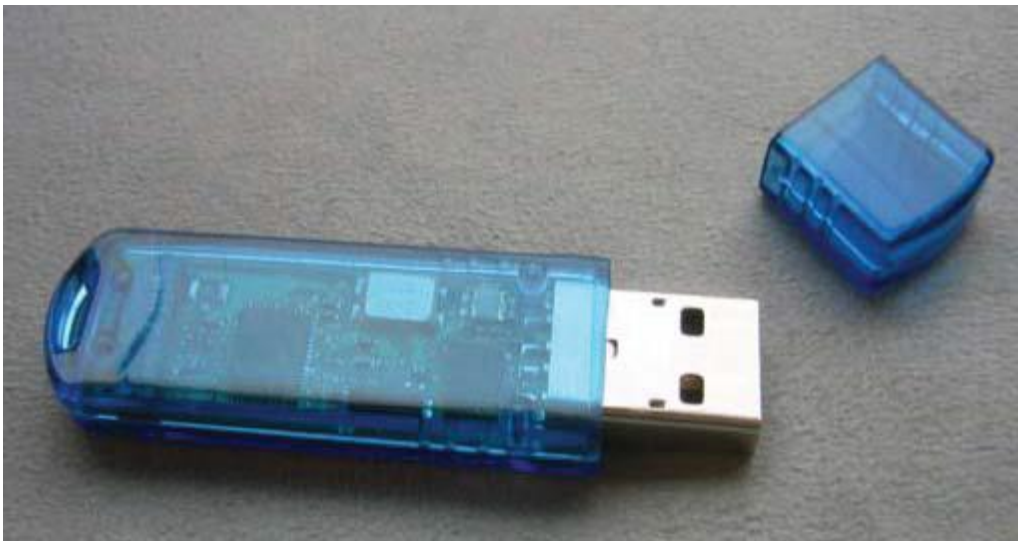


Figura 5.12 Dispositivo ETRX USB.

Otro dispositivo importante es el ETRX1CF, evolucionado con el sistema ETRX2 a ETRX2CF y de tarjeta Compact Flash. Lo que le permite ser utilizado desde un ordenador, utilizando el mismo sistema que las tarjetas PCMCIA.

Software.

Sistema Operativo. Una vez ensamblados los dispositivos que integran ZigBee, el fabricante añade el sistema operativo embebido que utilizarán para operar y que permitirán la comunicación de desarrolladores con estos, para su programación o adaptación al entorno de operación. Existen dos posibilidades uno basado en Hyperterminal y otro conocido como TinyOS.

El sistema operativo de Hyperterminal es un entrono sencillo que permite la comunicación con los dispositivos a través de comandos AT. Utiliza el mismo sistema de comunicación que los antiguos módems, mediante un puerto serie RS232. Los comandos AT que utiliza son los estándares para realizar las operaciones más básicas, además se han implementado una serie de comandos AT especiales preparados para este tipo de dispositivos que nos permiten crear en red, expulsar dispositivos, buscar una red, enviar información de un dispositivo a otro o a todos los dispositivos, etc. También y dependiendo del fabricante, se han incluido comandos AT propietarios, como es el caso de los dispositivos desarrollados por telegesis, que además proporciona un entorno de acceso propio, que contiene las opciones más comunes en botones que permiten que la comunicación y las operaciones se realicen en pocos clics de ratón.

La segunda opción es la llamada TinyOS, es un sistema operativo basado en UNIX y de código libre bajo licencia open source, orientado a componentes para redes de sensores inalámbricas. Desarrollado por un consorcio o asociación encabezado por la Universidad de california, en cooperación con Intel Research. Suele ser utilizado en los dispositivos ZigBee OEM. De la misma forma que sucedía en el caso de Hyperterminal, para comunicarnos con los dispositivos ZigBee será necesario hacerlo a través de un puerto serie. En cuanto al desarrollo de aplicaciones, puede trabajarse con distintos lenguajes de programación, aunque las aplicaciones suelen ser implementados principalmente en una variante de C conocido como nesC, orientado y optimizado para las limitaciones de memoria y comunicación de este tipo de redes; otros dos lenguajes también muy extendidos en este tipo de dispositivos son Java y el código interpretado Bash. Desde TinyOS se proporciona interfaces, módulos y configuraciones específicas e interfaces estándar para entradas y salidas de hardware. Actualmente la versión estable del sistema es la TinyOS 2.0 y dispone de entorno de programación para Linux, sistemas operativos Windows.

5.5 Condiciones de seguridad.

La seguridad en una red de dispositivos ZigBee se basa en claves de enlace y de red. En una comunicación por unicast entre pares de entidades APL la seguridad se basa en claves de 128 bits entre los dispositivos. Por otro lado, la comunicación existente cuando es por broadcast, también las claves para la seguridad se establecen de 128 bits entre todos los dispositivos de la red.

Un dispositivo adquiere la clave de enlace mediante el transporte de clave, establecimiento de clave o dad en la preinstalación desde el fabricante. Por otro lado, para el establecimiento de la clave de red hay dos maneras: el transporte de clave y la preinstalación. El establecimiento de clave se obtiene previamente de una clave maestra. Está clave maestra puede ser obtenida por el transporte de dicha clave o en fábrica.

La clave de red tiene que ser usada por las capas MAC, NWK y APL de ZigBee. Las claves maestras y las de enlace solo pueden ser usadas en la subcapa APS, de hecho las claves maestras y de enlace deben estar disponibles solo en la capa APL.

Los servicios de establecimiento de clave en la subcapa APS proporcionan el mecanismo por el cual un dispositivo ZigBee puede obtener una clave secreta compartida con otro dispositivo ZigBee. En establecimiento de clave existen dos elementos: el que inicia la comunicación y el que responde, que normalmente es el que le dará la validación. La información de validación, es decir, la clave maestra da paso a que el elemento iniciador pueda establecer una clave de enlace.

En el establecimiento del protocolo de clave simétrica Symmetric-Key key establishment (SKKE), el dispositivo iniciador establece una clave de enlace con el receptor usando la clave maestra. Esta clave maestra, puede venir dada de fábrica o que simplemente desde el centro de validación, que puede ser un tercer elemento o bien puede venir dada como datos introducidos por usuario.

Transporte de clave.

El servicio de transporte de clave proporciona tanto la posibilidad de transportar la clave de manera segura y no segura de un dispositivo a otros. La instrucción o comando de transportar clave segura significa transportar las claves maestras, de enlace, de red desde el centro de validación a los dispositivos. Este comando no protege con criptografía que tiene que ser cargada.

Actualización de Dispositivos.

El servicio de actualización de dispositivos proporciona una forma segura para que un dispositivo, como un router, informe a otro dispositivo, como el centro de validación, que existe un tercer dispositivo que ha cambiado su estado y que por tanto hay que actualizarlo, como pudiera ser la inclusión o eliminación de un dispositivo en la red. De esta manera el centro de validación mantiene una lista precisa de los dispositivos activos en la red.

Eliminación de dispositivos.

El servicio de eliminación de dispositivos proporciona una forma segura por la cual un dispositivo como el centro de validación puede informar a otros, como son los routers de que uno de sus hijos tiene que ser eliminado de la red. De esta manera se puede eliminar un dispositivo de la red que no ha cumplido los requisitos de seguridad dados por el centro de validación que hay en la red.

El servicio de petición de clave proporciona una manera segura para los dispositivos pedir la clave de red o bien la clave maestra a otro dispositivo como es el centro de validación.

Rol del centro de validación.

Por temas de seguridad, ZigBee define el rol de Centro de Validación. Este elemento es un dispositivo validado por los dispositivos de la red para distribuir las claves para que gestione la configuración de aplicación de los dispositivos. Todos los miembros de la red deben reconocer solo a un centro de validación y debe existir solo y solo un centro de validación por cada red segura.

Las funciones dadas por el Centro de Validación pueden ser subdivididas en tres roles: el gestor de validación, el gestor de la red y el gestor de la configuración. Un dispositivo se encarga de validar el gestor de validación para identificar los dispositivos que toman el rol en dicha red y el gestor de configuración. El gestor de red se encarga de gestionar la clave de red, tanto para tenerla como para distribuirla. El gestor de configuración se encarga del enlace de dos aplicaciones y facilitar la seguridad entre estos dos dispositivos que gestiona, como por ejemplo distribuyendo las claves maestras o de enlace. Para simplificar el manejo de estos tres roles, se incluyen dentro de un único dispositivo el centro de validación.

CONCLUSIONES

A través de este trabajo se pudo conocer la tecnología ZigBee, su importancia en su utilización y los grandes beneficios que se pueden obtener de ella. En principio se vieron las definiciones básicas de las redes de computadoras, sus componentes y tecnologías que las hacen posibles así como los principales protocolos usados y los modelos de referencia que permiten planear su correcto funcionamiento. Se explicaron desde las redes que requieren de cableado como lo es Ethernet y fibra óptica hasta las redes inalámbricas que permiten movilidad y bajos costos de implementación a comparación con la cableada. En el rubro de las redes inalámbricas entran las redes ZigBee que combinan los bajos costos de la electrónica actual. También fue de gran importancia mencionar los conceptos básicos de la seguridad informática que son fundamentales para implementar las políticas y los mecanismos de seguridad que permiten que la información se mantenga como se creó, confiable y esté disponible en todo momento.

Después de conocer los principios básicos de las redes de computadoras se abordó el tema de las redes ZigBee, empezando por un panorama general explicando los orígenes del estándar IEEE 802.x y 802.15, se explicó la Arquitectura ZigBee haciendo énfasis en cada una de sus capas y cuál es su función de una forma detallada, se describieron los principales dispositivos que utilizan dicha tecnología y los modelos de red con los cuales puede implementarse, se mostró una comparación con respecto a bluetooth y se argumentaron los beneficios que se obtienen de ZigBee.

En cuanto a sus aplicaciones se abordaron los principales beneficios que tiene el estándar para la humanidad como lo es energía inteligente que es la administración de recursos utilizados en el hogar como electricidad y consumo de gas; automatización del hogar que permite tener un control inteligente de todos los recursos de una casa, automatización en edificios que permite por ejemplo la administración de energía e iluminación, control de ventilación y calefacción, detección de intrusos, administración de mantenimiento, control de acceso, administración de estacionamientos entre otras muchas posibilidades; servicios de telecomunicaciones como lo es compartir información peer-to-peer o juegos en línea; cuidado de la salud que permitiría por ejemplo monitoreo y administración de un problema de salud no crítico, sensores para el cuerpo de análisis de deportistas.

Todo lo anterior no sería confiable sino hubiera mecanismos de protección para el uso de este tipo de redes, por lo que también se abordó ampliamente el tema de seguridad, analizando amenazas y vulnerabilidades, se describieron los principales ataques que existen para estos tipos de redes y de esta forma determinar una mejor protección. Una vez analizados los problemas de seguridad existentes se describieron los métodos de protección y cifrado que existen para este estándar así como las políticas que se deben seguir para resguardar la información que circula a través de ellas.

Por último se describieron las buenas prácticas a seguir para llevar a cabo la implementación de una red ZigBee cuidando cualquier tipo de factor que pudiera afectar su correcto funcionamiento o que afectara la seguridad de la misma. Se vieron principalmente los requerimientos para implementar una red ZigBee, así como el análisis del espacio para su instalación, estructura de la red dependiendo del espacio en donde se implementará, hardware y software necesarios para su construcción y administración, y que condiciones de seguridad se deben cumplir para que sea funcional al 100%.

De esta forma se puede concluir que ZigBee es una tecnología que permite un ahorro significativo de energía y que gracias a su flexibilidad y el poco espacio que ocupa una red de este tipo existe la intercomunicación de una gran cantidad de dispositivos electrónicos y abarcar y extender un gran número de aplicaciones. Esta tesis puede ser utilizada como la base para llevar a cabo la implementación de una red y aprovechar todas sus características.

Por lo tanto se puede concluir que:

- Se dio a conocer ZigBee una tecnología que proporciona una alternativa a otras redes ya en uso como bluetooth. Fueron descritos sus principales componentes así como la función que desempeñan.
- Se explicó que ventajas otorga ZigBee frente a otras tecnologías.
- Se describió la arquitectura ZigBee dando a conocer sus principales características y manejo de la información así como el estándar en que se basa.
- Se dieron a conocer las principales aplicaciones de una red ZigBee definiendo su uso, características, ventajas, desventajas y en que dispositivos se puede implementar.
- Se explicó la forma en que se implementa seguridad en ZigBee a través de su estándar así como la descripción de los ataques más comunes. Se establecieron políticas para la protección de una red implementada.
- Se dieron a conocer buenas prácticas para el diseño de una red ZigBee desde su planeación hasta las consideraciones de seguridad que se deben tener en cuenta.

APÉNDICE A.

MEDIOS DE TRANSMISIÓN

Medios de transmisión.

1. Terrestres o guiados.

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción de las señales desde un extremo a otro.

Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

La velocidad de transmisión depende directamente de la distancia entre las terminales y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilidades diversas.

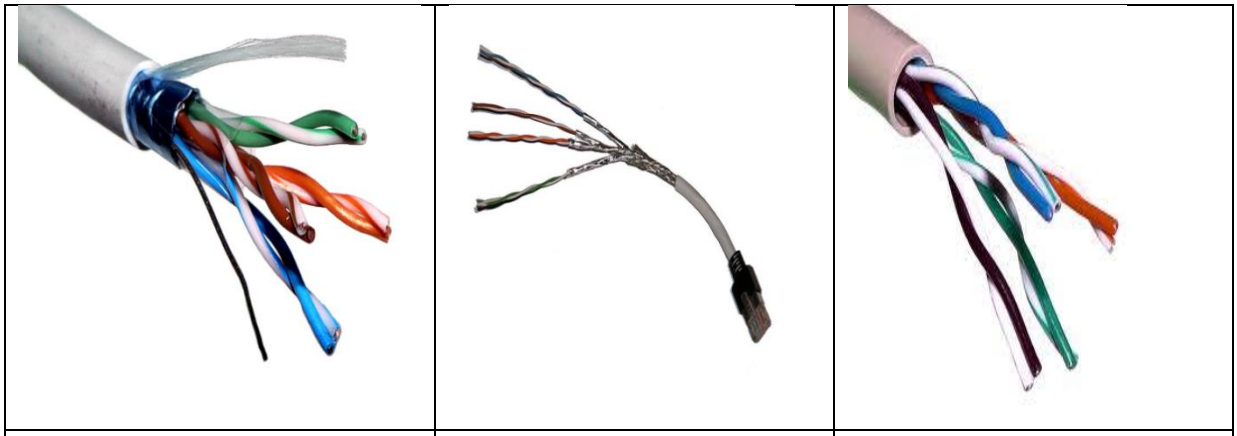
Dentro de los medios de transmisión guiados, los más utilizados en el campo de las comunicaciones y la interconexión de computadoras son:

a) **Cable de par trenzado.** El par trenzado surge como una alternativa del cable coaxial en 1985. Un cable de par trenzado es un cable de pares de hilos, normalmente de cobre, trenzados entre sí, lo que permite mantenerlo estable ante las propiedades eléctricas a lo largo de toda la longitud de cable y reduce las interferencias creadas por cada hilo adyacente en los cables compuestos por varios pares, es un cable muy utilizado en la actualidad y se divide en tres grupos (Figura A.1):

   - **UTP (Unshielded Twisted Pair-par trenzado sin apantallar).** Son cables que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal. Además que no cuentan con protección adicional como el par trenzado apantallado, lo que lo hace más vulnerable.

   - **STP (Shielded Twisted Pair-Cable de par trenzado apantallado).** Se trata de cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor de un conjunto de cables y por lo tanto, a su inmunidad al ruido. Se utiliza en redes de ordenadores como Ethernet o Token Ring. Es más caro que la versión no apantallada o UTP pero tienen menos errores al transmitir la información.

- **FTP (Foiled Twisted Pair-Par trenzado con pantalla global).** Son cables de pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias y su impedancia es de 12 ohms.



Cable FTP	Cable STP	Cable UTP

Figura A.1 Tipos de Par Trenzado.

En la tabla A.1 se ilustran las diferentes categorías y las respectivas características de un par trenzado:

Tabla A.1 Principales Categorías de cable de par trenzado.

Categoría	Ancho de Banda (MHz)	Aplicaciones
1	0.4	Líneas telefónicas y modem de banda ancha
2	0.4	Cable para conexión de antiguas terminales
3	16	10 BASE-T y 100 BASE-T4 Ethernet
4	20	16 Mbit/s Token Ring
5	100	100BASE-TX y 1000BASE-T Ethernet
5e	100	100BASE-TX y 1000BASE-T Ethernet
6	250	10000BASE-T Ethernet
6e	500	10GBASE-T Ethernet (En desarrollo)

b) Fibra Óptica. Son filamentos de vidrio de alta pureza extremadamente compactos. El grosor de una fibra es similar a la de un cabello humano. Son fabricadas a alta temperatura con base de silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones, entre sus principales características se puede mencionar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de

transmisión y un alto grado de confiabilidad debido a que son inmunes a las interferencias electromagnéticas de radio-frecuencia, además de no conducir señales eléctricas, por lo tanto, son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión. Los tipos existentes son:

- **Fibra Multimodo**. En este tipo de fibra viajan varios rayos ópticos reflejándose a diferentes ángulos. Los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede transmitir está limitada (Figura A.2).

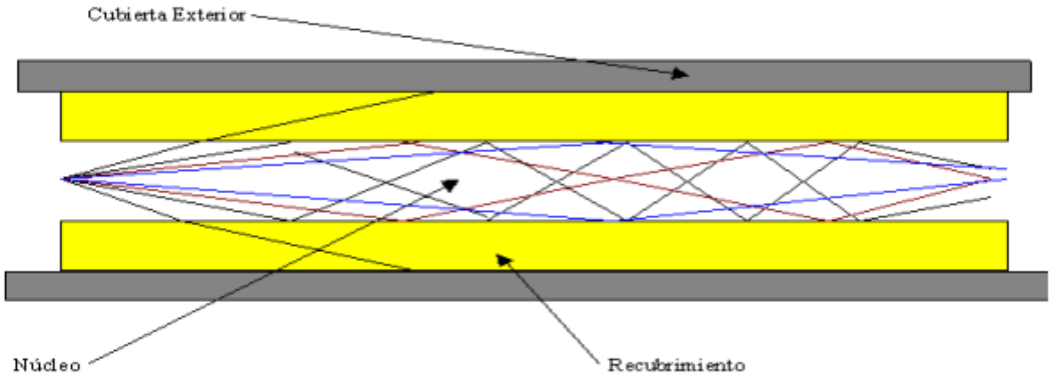


Figura A.2 Fibra óptica multimode.

- **Fibra multimodo con índice graduado.** En este tipo de fibra óptica el núcleo está hecho de varias capas concéntricas de material óptico con diferentes índices de refracción, por lo que el número de rayos ópticos diferentes que viajan es menor y por lo tanto, sufren menos el severo problema de las fibras multimodo (Figura A.3).

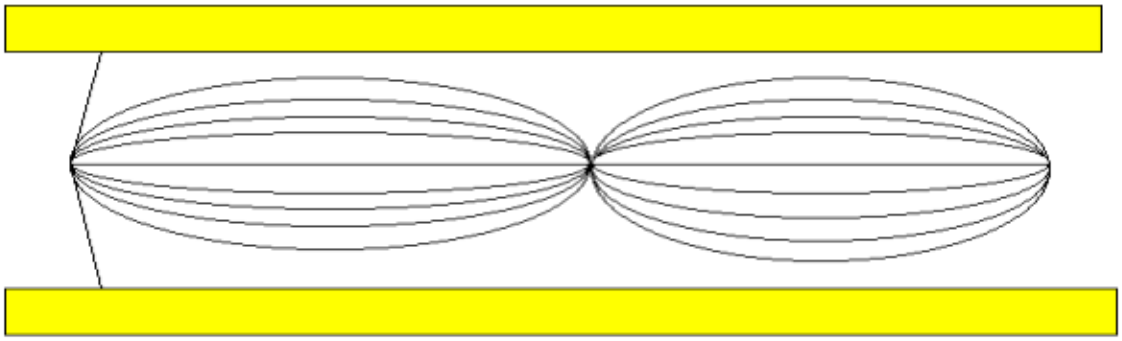


Figura A.3 Fibra óptica multimodo con índice graduado.

- **Fibra monomodo.** Esta fibra óptica es la de menor diámetro y solamente permite viajar al rayo óptico central. No sufre del efecto de las otras dos pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mayores. La fibra óptica ha venido a revolucionar la comunicación de datos ya que tiene las siguientes ventajas:
    - Gran ancho de banda (alrededor de 14Hz).
    - Muy pequeña y ligera.
    - Muy baja atenuación.
    - Inmunidad al ruido electromagnético.

Para transmitir señales por fibra óptica se utiliza modulación de amplitud sobre un rayo óptico, la ausencia de señal indica un cero y la presencia un uno. La transmisión de fibra óptica es unidireccional. Actualmente se utilizan velocidades de transmisión de 50, 100 y 200 Mbps, pero experimentalmente se han transmitido hasta Gbps sobre una distancia de 110 Km.

2. Aéreos o no guiados.

En la actualidad las personas necesitan comunicarse entre sí para poder obtener información importante e indispensable para llevar a cabo sus actividades diarias, ya sea para trabajar o para asuntos escolares y no importando la distancia a la que se encuentren. Con los avances en la tecnología es necesario estar en línea todo el tiempo, por lo que el envío de información a través de cables resulta incómodo sobre todo para las personas que necesitan estar en constante movimiento viajando a diferentes lugares, es aquí donde surgen las redes inalámbricas, las cuales ofrecen diversas posibilidades como la movilidad, costos menores de instalación y disminución en el uso de materiales como lo son grandes distancias de cableado de red.

Se dice que los medios de transmisión no guiados son los que envían las señales mediante la ausencia de cable, las señales se propagan libremente a través del medio como lo es el aire y el vacío. La comunicación digital inalámbrica comenzó en las islas de Hawaii, en donde partes considerablemente grandes del Océano Pacífico separaban a los usuarios y el sistema telefónico era inadecuado. Aquí se mencionan algunos tipos de transmisiones inalámbricas.

a) Radiotransmisión.

La radio transmisión o comunicación vía radio es aquella que emplea un medio inalámbrico de transmisión como puede ser la atmósfera o el espacio libre, este tipo de comunicación tiene como característica principal utilizar una onda electromagnética para trasladar la información de un lugar a otro que permite propagarse en un medio no material en una dirección y un sentido deseado, con una forma modulada por la información a transmitir, y ajustada a los requerimientos clásicos de cualquier comunicación: alcance, calidad y fiabilidad.

Existen cuatro formas distintas de propagación de las ondas radioeléctricas:

- Propagación directa. Son las ondas que viajan desde una antena transmisora a otra antena que funciona como receptora. Este tipo de ondas pueden sufrir en su camino reflexiones y/o refracciones debidas a las variaciones de las características físicas de la atmósfera. Como ejemplos se tienen la radiofusión comercial en FM, televisión en UHF y VHF que son transmisiones superiores a 30 MHz.

- Propagación por reflexión. Se entiende por reflexión el cambio de la dirección de propagación de un fenómeno ondulatorio, como las ondas radioeléctricas, cuando inciden sobre una superficie reflectante. Al haber diversos obstáculos las ondas son reflejadas, lo que ocasiona una propagación no muy deseable debido a que además de la señal directa varias señales reflejadas procedentes de uno o varios puntos llegan a la antena receptora originando señales iguales y desfasadas en el tiempo, puesto que las trayectorias de las reflejadas son más largas, producen imágenes fantasma o dobles imágenes. Para evitar este problema se deben utilizar antenas receptoras de gran directividad, correctamente situadas con relación al emisor.

- Propagación por refracción. Es el cambio en la dirección de la propagación de un movimiento ondulatorio, como las señales radioeléctricas, debido al paso de la onda desde un medio a otro de distinto índice de refracción.

- Propagación por difracción. Es el fenómeno característico de las propiedades ondulatorias de la materia, por la cual un obstáculo que se opone a la propagación libre de las ondas se presenta como una fuente secundaria que emite ondas derivadas en todas las direcciones. Gracias a este fenómeno las ondas rodean el obstáculo y consiguen salvarlo.

b) Antenas.

Como se mencionó, la antena es la encargada de transferir la energía EM, soportada por la señal portadora, desde un medio cableado al medio inalámbrico y viceversa. Existen varios tipos de antenas dentro de las cuales se tienen los siguientes:

- Antena de hilo. Es la antena por excelencia. Se trata de una varilla telescópica, más o menos flexible, cuya longitud depende de la frecuencia de trabajo. Es de uso común en comunicaciones móviles y se aplican en receptores de emisiones AM y FM (Figura A.4).

Figura A.4 Antena de hilo.

- Antena rómbica. Es una antena de cuatro hilos, formando un rombo a cierta altura del suelo, acabada en carga resistiva. Normalmente tiene grandes dimensiones. Se usa principalmente en comunicaciones a gran distancia en frecuencias inferiores a 30Mhz por onda ionosférica (Figura A.5).

Figura A.5 Antena rómbica.

- Antena logarítmica. Se trata de una antena multielemento que permite trabajar con una amplia gama de frecuencias, transmisiones en banda ancha. Se emplea en frecuencias inferiores a 30 MHz, en radionavegación y comunicaciones a larga distancia (Figura A.6).

Figura A.6 Antena logarítmica.

- Antena Yagi. Es la antena más conocida, es usada en los techos de casas y edificios para la recepción de televisión desde ciertos puntos de una geografía particular (Figura A.7).

Figura A.7 Antena Yagi.

- Arreglo de dipolos. Consiste en un agrupamiento de dipolos, con el fin de lograr unas ciertas características de radiación en cuanto a ganancia y direccionalidad. Tiene una gran cantidad de aplicaciones, ya que en función del diseño de los dipolos y del dimensionado del arreglo en cuanto a geometría y forma de excitación de los mismos se logran muy distintos alcances, potencias y diagramas de radiación. Es una superficie de revolución, que tiene la propiedad de concentrar la radiación en un punto denominado foco, donde se sitúa el elemento activo (dipolo, bocina, etcétera). Son las antenas empleadas en las comunicaciones vía satélite espacial artificial (Figura A.8).

Figura A.8 Antena dipolo FM.

c) Microondas.

Las microondas son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las súper altas frecuencias, SHF, utilizándose para redes inalámbricas la banda de los 18 a 19 GHz Estas redes tienen una propagación muy localizada en un ancho de banda que permite alcanzar los 15 Mbps.

En la transmisión de microondas se enfoca un haz estrecho en donde las ondas viajan en línea recta más arriba de los 100Mhz, lo que origina una concentración de energía con una antena parabólica que produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora deben estar alineadas entre sí.

Ya que las microondas viajan en línea recta, si las torres están muy separadas, partes de la tierra estorbarán, por lo que es necesario tener repetidores que estén colocados periódicamente. Mientras más altas sean las torres, más separadas pueden estar. La distancia entre los repetidores se eleva en forma muy aproximada con la raíz cuadrada de la altura de las torres, por ejemplo, con torres de 100m de altura, los repetidores pueden estar separados a 80 km de distancia.

Se pueden mencionar las siguientes desventajas:

- Las microondas no atraviesan bien los edificios.
- Un haz aun estando bien enfocado puede llegar a tener cierta divergencia en el campo.
- Algunas ondas pueden refractarse en las capas atmosféricas más bajas y tardar un poco más en llegar que las ondas directas.
- Se puede presentar un fenómeno llamado desvanecimiento por múltiples trayectorias ocasionado por ondas diferidas que pueden llegar fuera de fase con la onda directa y cancelar así la señal.
- Las bandas de hasta 10 GHz ahora son de uso rutinario, pero con las de aproximadamente 4Ghz surge un problema: son absorbidas por el agua.

La comunicación por microondas se utiliza para la comunicación telefónica de larga distancia, los teléfonos celulares, la distribución de la televisión. Esta tecnología tiene varias ventajas significativas respecto a la fibra, la principal es que no necesita derecho de paso; basta con comprar un terreno pequeño cada 50 km y construir en él una torre de microondas para saltarse el sistema telefónico y comunicarse en forma directa.

Las microondas también son relativamente baratas. Levantar dos torres sencillas y poner antenas en cada una puede costar menos que enterrar 50km de fibra a través de un área urbana congestionada o sobre una montaña y también puede ser más

económico que rentar la fibra de alguna compañía de teléfonos, en especial si ésta aún no ha recuperado por completo la inversión hecha por el cobre que quitó cuando instaló la fibra (Figura A.9).

Figura A.9 Antena transmisora de microondas.

d) Ondas infrarrojas.

Las ondas infrarrojas y milimétricas no guiadas se usan mucho para la comunicación de corto alcance. Todos los controles remotos de los televisores, grabadoras de video y estéreos utilizan comunicación infrarroja. Estos controles son relativamente direccionales, económicos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. En general, conforme se pasa de la radio de onda larga hacia luz visible, las ondas se comportan cada vez más como la luz y cada vez menos como la radio (Figura A.10).

Figura A.10 Control remoto por medio de luz infrarroja.

e) Transmisión por ondas de luz.

La óptica de espacio libre es una tecnología de comunicación óptica que utiliza la propagación de luz en la atmósfera para transmitir información entre dos puntos. Al igual que las redes de fibra óptica, esta tecnología utiliza un diodo emisor de luz (LED - light emitting diode) o un láser como fuente de transmisión, aunque no necesita que el haz de luz sea guiado a través de cables ópticos. Para su recepción, estos haces de luz operan en la parte de terahertz del espectro. Para recibir la señal, los haces de luz se centran en una lente de recepción conectada a un receptor de alta sensibilidad a través de un cable de fibra óptica.

Las comunicaciones ópticas han sido usadas por cientos de años. Desde los antiguos griegos que pulían sus escudos para enviar señales durante la batalla a los modernos semáforos y el telégrafo inalámbrico solar, también llamado heliógrafo que transmiten señales en código para comunicarse.

En 1880 Alexander Graham Bell y su asistente, Sarah Orr crearon el fotófono, considerado por los laboratorios Bell, su invento más importante. El dispositivo permitía la transmisión de sonido sobre un haz de luz. El 3 de Junio de 1880, Bell realizó la primera transmisión de telefonía inalámbrica entre dos edificios cercanos.

La invención del láser en la década de 1960 revolucionó las comunicaciones ópticas en el espacio libre. Las organizaciones militares estaban particularmente interesadas y se impulsó su desarrollo. Sin embargo, la tecnología perdió impulso en el mercado cuando la instalación de redes de fibra óptica para su uso civil estaba en su apogeo.

La óptica de espacio libre se utiliza también para permitir las comunicaciones de las naves espaciales. Los enlaces ópticos pueden ser implementados utilizando láseres de luz infrarroja, aunque también para enviar datos a bajas velocidades y para distancias cortas se utilizan LEDs. El rango máximo de enlaces terrestres es del orden de 2.3km pero la estabilidad y la calidad del enlace es altamente dependiente de los factores atmosféricos como lluvia, niebla, polvo y calor. En el espacio exterior el alcance de las comunicaciones ópticas de espacio libre en la actualidad es del orden de varios miles de kilómetros pero tiene el potencial de alcanzar distancias interplanetarias de millones de kilómetros, utilizando telescopios ópticos como expansores de haz. La comunicación infrarroja utilizada por algunos dispositivos como los teléfonos celulares es también una forma muy simple de comunicación óptica de espacio libre.

APÉNDICE B. TECNOLOGÍAS INALÁMBRICAS

1. Espectro radioeléctrico.

Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar por el espacio libre. El físico británico James Clerk Maxwell predijo estas ondas en 1865 y el físico alemán Heinrich Hertz las observó en 1887. La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, *f*, y se mide en Hz. La distancia entre dos puntos máximos consecutivos se llama longitud de onda y se designa de forma universal con la letra griega lambda λ (Figura B.1).

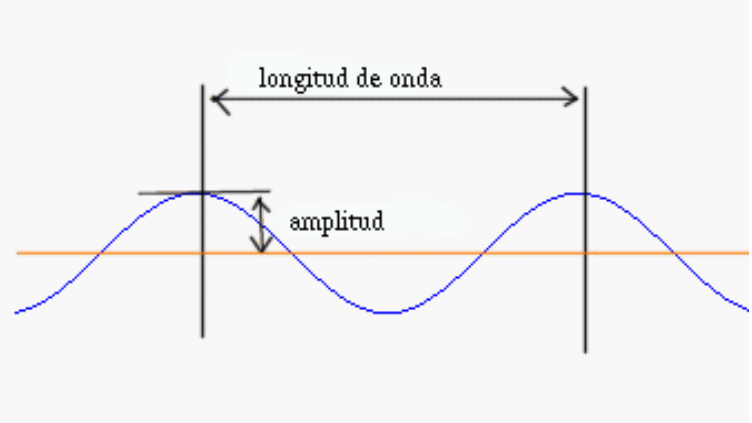


Figura B.1 Características de una onda electromagnética

Tomando en cuenta lo anterior, se denomina espectro radioeléctrico o electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Referido a un objeto se denomina espectro electromagnético o simplemente espectro a la radiación electromagnética que emite o absorbe una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Este espectro se extiende desde la radiación de menor longitud de onda, como los rayos gamma y los rayos x, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio (Figura B.2).

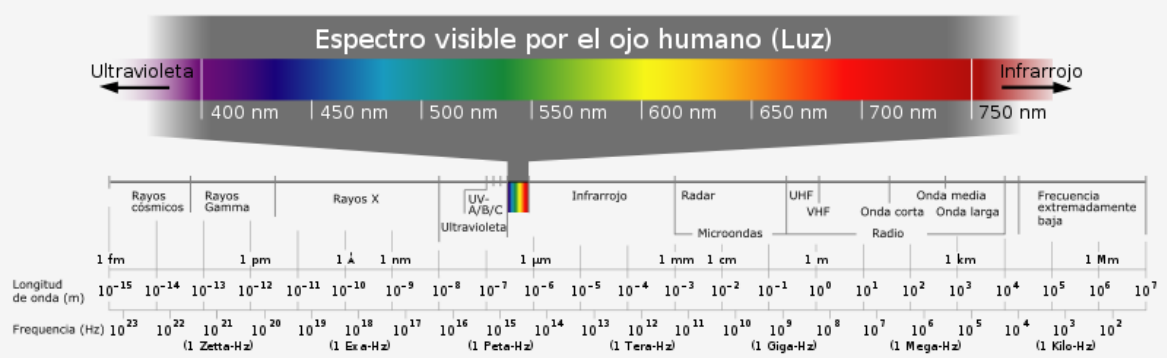


Figura B.2 Espectro electromagnético.

Para su estudio, el espectro electromagnético se divide en segmentos o bandas, aunque esta división es inexacta. Existen ondas que tienen una frecuencia, pero varios usos, por lo que algunas frecuencias pueden quedar en ocasiones incluidas en dos rangos (Tabla B.1).

Tabla B.1 Segmentos del espectro electromagnético.

Banda	Longitud de onda (m)	Frecuencia (Hz)	Energía (J)
Rayos gamma	< 10 pm	> 30,0 EHz	$> 20 \cdot 10^{-15}$ J
Rayos X	< 10 nm	> 30,0 PHz	$> 20 \cdot 10^{-18}$ J
Ultravioleta extremo	< 200 nm	> 1,5 PHz	$> 993 \cdot 10^{-21}$ J
Ultravioleta cercano	< 380 nm	> 789 THz	$> 523 \cdot 10^{-21}$ J
Luz Visible	< 780 nm	> 384 THz	$> 255 \cdot 10^{-21}$ J
Infrarrojo cercano	< 2,5 µm	> 120 THz	$> 79 \cdot 10^{-21}$ J
Infrarrojo medio	< 50 µm	> 6,00 THz	$> 4 \cdot 10^{-21}$ J
Infrarrojo lejano/submilimétrico	< 1 mm	> 300 GHz	$> 200 \cdot 10^{-24}$ J
Microondas	< 30 cm	> 1 GHz	$> 2 \cdot 10^{-24}$ J
Ultra Alta Frecuencia - Radio	< 1 m	> 300 MHz	$> 19.8 \cdot 10^{-26}$ J
Muy Alta Frecuencia - Radio	< 10 m	> 30 MHz	$> 19.8 \cdot 10^{-28}$ J
Onda Corta - Radio	< 180 m	> 1,7 MHz	$> 11.22 \cdot 10^{-28}$ J
Onda Media - Radio	< 650 m	> 650 kHz	$> 42.9 \cdot 10^{-29}$ J
Onda Larga - Radio	< 10 km	> 30 kHz	$> 19.8 \cdot 10^{-30}$ J
Muy Baja Frecuencia - Radio	> 10 km	< 30 kHz	$< 19.8 \cdot 10^{-30}$ J

En radiofrecuencia se tienen los siguientes rangos (Tabla B.2):

Tabla B.2 Radiofrecuencia.

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000–10.000 km
Super baja frecuencia	SLF	2	30-300 Hz	10.000–1000 km
Ultra baja frecuencia	ULF	3	300–3000 Hz	1000–100 km
Muy baja frecuencia	VLF	4	3–30 kHz	100–10 km
Baja frecuencia	LF	5	30–300 kHz	10–1 km
Media frecuencia	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia	HF	7	3–30 MHz	100–10 m
Muy alta frecuencia	VHF	8	30–300 MHz	10–1 m
Ultra alta frecuencia	UHF	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia	SHF	10	3-30 GHz	100-10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10–1 mm
			Por encima de los 300 GHz	< 1 mm

Estas radiaciones son las que permiten al ser humano poder enviar información a través del ambiente y crear la comunicación persona a persona sin la necesidad de tener que viajar de un lugar a otro o tener que utilizar grandes cantidades de cables, facilitando así el traslado de la información.

Para ello cada país es el encargado de regular el uso del espectro radioeléctrico, permitiendo de esta forma evitar conflictos entre las diferentes compañías que ahí laboren o utilicen dicho espectro y lo hacen mediante las bandas de frecuencia, las cuales se muestran a continuación:

a) Banda mixta de 2.5GHz.

   Las bandas entre 2.5 y 2.69 GHz han sido reservadas por E.E.U.U. México, Brasil y algunos países de Asia (principalmente Singapur), donde han sido poco utilizadas para su utilidad original, relacionada con la transmisión de televisión.

   En Asia, Australia, Corea del Sur y Nueva Zelanda, se utiliza la banda de 2.3 GHz, que se espera que se cubra con los sistemas de 2.5GHz. Esta banda de 2.3 GHz (WCS) está formada por dos slots de 15MHz con una separación en medio de 25MHz, debido a que está reservado para servicios de radio digital (DARS).

b) Banda de 2.4 GHz a 2.4835GHz.

Esta banda designada por el Reglamento de Radiocomunicaciones para aplicaciones ICM (aplicaciones Industriales Científicas y Médicas), podrá ser utilizada también para los siguientes usos:

- Acceso inalámbrico a redes de comunicaciones electrónicas, así como para redes de área local para la interconexión sin hilos entre ordenadores y terminales y dispositivos periféricos para aplicaciones en interior de recintos.
- Dispositivos genéricos de baja potencia en recintos cerrados y exteriores de corto alcance, incluyendo aplicaciones de video.

c) Banda con licencia de 3.5 GHz.

Es la primera banda utilizada para operadores de banda ancha con licencia, que generalmente se localiza entre los 3.4 y 3.6 GHz, aunque hay nuevas posibilidades en el rango de 3.3 y 3.4 GHz (usado en China y la India) y el rango 3.6-3.8GHz (usado por Francia, Reino Unido, Europa y Estados Unidos).

d) Banda libre de 5 GHz.

El rango de frecuencias de interés incluye las bandas entre 5.25GHz y 5.57GHz. La banda entre 5.15 y 5.25 GHz es la más utilizada para aplicaciones interiores de baja potencia. En el caso de la banda de frecuencia usada es la norma 802.11a. Además, se caracteriza por disponer de poca potencia en las frecuencias bajas. Para el caso de las bandas inferiores a 5.47GHz, la potencia máxima es de 250mW.

e) Bandas con licencia.

Para emplear una solución con licencia es preciso que el administrador adquiera un espectro, el cual es un proceso muy variable en función del país en el que se quiera operar. Se permite un uso exclusivo de una banda, lo que ofrece una gran calidad al no tener restricciones de potencia tan exigentes como las de banda de uso libre. Existen bajas interferencias ofreciendo altos niveles de calidad en la transmisión que no son posibles en las bandas sin licencia.

f) Bandas de uso libre.

El elevado costo de adquisición de espectro lleva a muchos administradores de redes inalámbricas a considerar el uso de bandas sin frecuencia para áreas rurales o mercados emergentes. Este tipo de soluciones tiene una serie de ventajas respecto a las soluciones de bandas libres, como es el menor costo,

mayor escalabilidad o la mayor interoperabilidad. Desafortunadamente también tienen desventajas que se tienen que considerar y se mencionan a continuación.

- Interferencias**.** Debido a que el espectro que no requiere licencia puede ser utilizado por varios sistemas diferentes de radiofrecuencia, hay altas probabilidades de que ocurran interferencias.
- Mayor competencia. Los administradores que utilizan el espectro que no requiere licencia tienen que asumir que otro administrador fácilmente podría ingresar en el mercado empleando el mismo espectro.
- Potencia limitada. Los entes reguladores de gobierno limitan la cantidad de potencia que puede transmitirse.
- Disponibilidad. Mientras el espectro de 2.4GHz está disponible universalmente, en la actualidad del espectro de 5GHz no se encuentra disponible en varios países.

2. Wi-Fi.

Wi-Fi u 802.11b, es un estándar robusto, maduro y bien establecido que continúa creciendo y evolucionando. En el año de 2004 se certificaron dos versiones de especificaciones: 802.11a y 802.11g, mostrando éste último un crecimiento dramático (Figura B.3).

Una de las ventajas de la tecnología 802.11g es que es totalmente compatible con los productos desarrollados en la versión anterior 802.11b, de los cuales existen muchos instalados y muy pronto esa compatibilidad incluirá a los sistemas 802.11a. Se pueden mencionar las siguientes características:

- Wi-Fi () es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11.
- Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.
- Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.

Figura B.3 Estándar Wi-Fi.

Hay, al menos, dos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11.

Los estándares IEEE 802.11b e IEEE 802.11g son los más utilizados internacionalmente debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Existe también el estándar IEEE 802.11n que trabaja a 2.4 GHz a una velocidad de 108 Mbps. Aunque estas velocidades de 108 Mbps son capaces de alcanzarse ya con el estándar 802.11g gracias a técnicas de aceleramiento que consiguen duplicar la transferencia teórica. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N, sin embargo, no son del todo seguros ya que el estándar no está completamente revisado y aprobado.

En Estados Unidos y Japón se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. En otras zonas, como la Unión Europea, 802.11a no está aprobado todavía para operar en la banda de 5 GHz, y los reguladores europeos están todavía considerando el uso del estándar europeo HIPERLAN.

La tecnología inalámbrica Bluetooth también funciona a una frecuencia de 2.4 GHz, por lo que puede presentar interferencias con Wi-Fi, sin embargo, en la versión 1.2 y mayores del estándar Bluetooth, se ha actualizado su especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías.

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en

consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de seguridad de datos específicos para los protocolos Wi-Fi como el WEP y el WPA que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos o IPSEC (túneles IP) y el conjunto de protocolos IEEE 802.1X, proporcionados por otros dispositivos de la red de datos y de reconocida eficacia a lo largo de años de experiencia. Actualmente existe el protocolo de seguridad llamado WPA2, que es una mejora relativa a WPA, es el mejor protocolo de seguridad para Wi-Fi en este momento.

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo 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.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todos los mismos protocolos. El estándar original de este protocolo data de 1997, es el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2.4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11 legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2.4 GHz. También se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la versión b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el estándar b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g (actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializaban seguían el estándar 802.11g con compatibilidad hacia el 802.11b.

Los estándares 802.11b y 802.11g utilizan bandas de 2.4 GHz que no necesitan de permisos para su uso. El estándar 802.11a utiliza la banda de 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2.4 GHz.

Protocolos de Wi-Fi.

a) 802.11.

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bits por segundo (Mbits/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2.4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Éstas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

b) 802.11b.

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbits/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbits/s sobre TCP y 7.1 Mbits/s sobre UDP.

c) 802.11a.

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el estándar 802.11 con velocidades de transmisión de 2Mbps. En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b. En 2001 hicieron su aparición en el mercado los productos del estándar 802.11a. La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbits/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbits/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbits/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares. Dado que la banda de 2.4 GHz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

d) 802.11g.

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Éste utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbits/s o cerca de 24.7 Mbits/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g, la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se

debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

e) 802.11n.

En Enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 para desarrollar una nueva revisión del estándar. La velocidad real de transmisión podría llegar a los 600 Mbps y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología entrada múltiple-salida múltiple (MIMO-Multiple Input-Multiple Output) que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado, y se viene implantando desde 2008. Anteriormente ya había dispositivos adelantados al protocolo y que ofrecían de forma no oficial este estándar. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2.4 GHz y 5GHz. Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento. El estándar 802.11n fue ratificado por la organización IEEE el 11 de Septiembre de 2009 con una velocidad de 600Mbps en capa física.

f) 802.11e.

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de calidad de servicio (QoS-Quality of Service) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de calidad de servicio. Para cumplir con su objetivo, IEEE 802.11e introduce un nuevo elemento llamada Función de Coordinación Hibrida (HCF-Hybrid Coordination Function) con dos tipos de acceso: canal de acceso distribuido mejorado (EDCA- Enhanced Distributed Channel Access) y acceso al canal controlado (HCCA- Controlled Channel Access).

g) Protocolo propietario 802.11 Super G.

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 GHz y 5 GHz, alcanza una velocidad de transferencia de 108 Mbps. De la empresa D-Link.

3. Bluetooth.

Bluetooth está detrás de Wi-Fi en un proceso evolutivo, pero ahora cada vez mejor. Las especificaciones están completas. La nueva versión 1.2, incorpora la función de salto de frecuencia adaptiva, la cual minimiza la interferencia mutua con sistemas de frecuencia estática (802.11) y hace posible la coexistencia de diferentes sistemas inalámbricos en el mismo entorno. Esta función permite a los dispositivos bluetooth operar más efectivamente en donde existen redes inalámbricas, como en los grandes supermercados y en muchos almacenes. La versión 1.2 también ha corregido los problemas asociados con la transmisión de voz y soporta mejor los audífonos inalámbricos, como los de los teléfonos celulares y los sistemas basados en voz utilizados en los almacenes.

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. Los principales objetivos que se pretende conseguir con esta norma son:

• Facilitar las comunicaciones entre equipos móviles y fijos.

• Eliminar cables y conectores entre éstos.

• Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

La tecnología Bluetooth comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM, Intel y otros. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente lo hagan también empresas de sectores tan variados como: automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etcétera, con lo que en poco tiempo se presentará un panorama de total conectividad de diversos aparatos tanto en casa como en el trabajo (Figura B.4).

Figura B.4 Estándar Bluetooth.

GLOSARIO

- Access Point. El punto de acceso corresponde a un transmisor-receptor de redes inalámbricas o estación base que puede conectar una red LAN cableada a uno o varios dispositivos inalámbricos. Los puntos de acceso también se pueden conectar en puente entre sí.

- Acuse de Recibo (Acknowledgment o ACK). ACK es un mensaje corto para informar al transmisor que han llegado datos al destino deseado. El mensaje puede indicar que los datos llegaron sin novedad o que los datos tuvieron problemas hasta llegar a su destino.

- AODV-Ad Hoc On-Demand Vector Routing. Protocolo creado por Charles E. Perkins el cual intercambia mensajes cuando necesita establecer una comunicación, es decir, envía mensajes a los vecinos para calcular cada ruta. Cada nodo tiene asociada una tabla de encaminamiento que utiliza para poder establecer enlaces con otros nodos.

- ADC-Convertidor analógico digital (Analog Digital Converter). Es un sistema que permite enlazar variables analógicas con procesos digitales. El objetivo básico de un ADC es transformar una señal eléctrica análoga en un número digital equivalente. El sistema inverso un DAC transforma un número digital en una señal eléctrica análoga.

- ADSI. Los Servicios de Interfaces de Directorio Activo es un grupo de interfaces abiertas que abstrae las capacidades de los servicios de directorio desde varios proveedores de red distintos para presentar una sola vista de acceso y administración de recursos de red. Administradores y desarrolladores pueden usar los servicios ADSI para enumerar y administrar recursos en un servicio de directorio no importando en qué entorno de red se encuentre el recurso.

- AES. Es un algoritmo de cifrado simétrico desarrollado por los estudiantes Vincent Rijmen y Joan Daemen. AES toma como elemento básico al byte (8 bits) y se toma a los bytes como elementos del campo finito, toda operación del algoritmo está basada en operaciones sobre este campo finito, rotaciones de bytes y operaciones de suma módulo 2. AES es un algoritmo de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser cifrados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se le puede ver como un bloque o matriz de 4x4 bytes al que se le llama estado.

- ALOHA. Era un Sistema de red de computadoras pionera desarrollada en la Universidad de Hawai. ALOHAnet empezó a funcionar en junio de 1971, este protocolo utilizaba un nuevo método de acceso al medio y experimental de ultra

alta frecuencia para su funcionamiento, ya que las asignaciones de frecuencia para las comunicaciones hacia y desde una computadora que no estaban disponibles para aplicaciones comerciales en la década de 1970.

- Autenticación. Es el proceso de detectar y comprobar la identidad de una entidad de seguridad examinando las credenciales de un usuario y validando esas credenciales contra alguna autoridad.

- BACnet Automatización de edificios y Control de Redes (Building Automation and Control Networks). Es un protocolo de comunicación de datos diseñado para comunicar entre sí a los diferentes dispositivos electrónicos presentes en los edificios inteligentes actuales (alarmas, sensores de paso, aire acondicionado, calefacción)

- Baliza (beacon). En redes ZigBee se conoce a las balizas como un mecanismo de control del consumo de potencia en la red. Permite a todos los dispositivos saber cuándo pueden transmitir. Las balizas que dan nombre a este tipo de entorno, se usan para poder sincronizar todos los dispositivos que conforman la red, identificándola red domótica, y describiendo la estructura de la supertrama. Los intervalos de las balizas son asignados por el coordinador de red y pueden variar desde los 15ms hasta los 4 minutos.

- Bluetooth. Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son: Facilitar las comunicaciones entre equipos móviles, Eliminar los cables y conectores entre éstos, Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales. Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

- Broadcast. Se basa en un único proceso de envío, independientemente del número de potenciales máquinas receptoras de una misma información en una o más unidades de datos desde un origen a todas las máquinas de una red de área local. Todo ello, sin necesidad de transmitir desde el origen una copia de la misma información, por separado, a cada una de dichas máquinas.

- CAP - Contention Access Periodo. Periodo de tiempo originado por un GTS que aparece antes de periodo libre de contención (CFP) de una supertrama activa.

- CCA (Clear Channel Assesment). Etapa de evaluación previa de un canal de transmisión para verificar que se encuentre disponible para el envío de la misma.
- CFP - Contetion Free Period. Periodo de tiempo originado Por un GTS que aparece al final de una supertrama activa.
- CO2. El Dióxido de carbón es un gas carbónico y anhídrido carbónico, cuyas moléculas están compuestas por dos átomos de oxígeno y uno de carbono.
- Comandos AT. Son instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y un modem.
- Criptografía. Es la ciencia de cifrar y descifrar información, utilizando técnicas que hagan posible el intercambio de mensajes de manera segura, que sólo pueden ser leídos por las entidades a quienes va dirigido
- CSMA/CA. Es un protocolo de redes que evita que dos estaciones que transmiten datos al mismo tiempo originen una colisión de información. Este método asegura que el mensaje enviado se recibe correctamente. Los pasos que realiza son los siguientes: 1. Escucha el canal de comunicación para ver si está libre, 2. Si está libre transmite la información, 3. Espera un reconocimiento por parte del receptor.
- Dispositivo final ZigBee ZED (ZigBee End Device). Es el dispositivo que posee la funcionalidad necesaria para comunicarse con su nodo padre (coordinador o router) pero no puede transmitir información destinada a otros dispositivos. Este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías.
- OEM. Acrónimo de Original Equipment manufacturer o fabricante de equipos originales. Son equipos fabricados por una empresa y vendidos a otra. Las siglas OEM comúnmente hacen referencia a la empresa que originalmente hace el producto.
- Domótica. La palabra domótica deriva de la unión de “domus” (casa) y de Informática, y hace referencia a la incorporación a la vivienda de un conjunto de tecnologías informáticas y de comunicaciones que permiten gestionar y automatizar desde un mismo sistema las diferentes instalaciones de uso cotidiano de una vivienda.
- DSAP (Destination Service Access Point - Servicio de Destino del Punto Acceso). Es un campo de 8 bits que le permite a la capa LLC mantener un registro de múltiples conexiones a través de un entorno LAN y el valor hexadecimal por default 0xAA, mientras el campo de control es puesto a 3

- DSSS - Direct Squence Spread Spectrum. El espectro ensanchado por secuencia directa es una técnica de codificación que utiliza un código de pseudoruido para modular digitalmente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radioreceptores les parecerá ruido menos al que va dirigida la señal.

- ED. Acrónimo de Energy Detection o Detección de energía.

- Embebido. Un sistema embebido (anglicismo "embedded") o empotrado es un sistema de computación diseñado para realizar una o algunas pocas funciones dedicadas frecuentemente en un sistema de computación en tiempo real. Al contrario de lo que ocurre con los ordenadores de propósito general (como por ejemplo una computadora personal o PC que están diseñados para cubrir un amplio rango de necesidades, los sistemas embebidos se diseñan para cubrir necesidades específicas.

- Entidades APL. Son los objetos de aplicación definidos por cada uno de los fabricantes y se encuentran en la capa superior de ZigBee.

- Estado de sleep. Es el estado en que se encuentra un dispositivo al no estar recibiendo o transmitiendo información.

- FCS - Frame Checksum. Secuencia de números en los encabezados que enlaza tramas de reconocimiento o acuse de recibo con transmisiones anteriores lo que permite verificar la integridad de las tramas MAC.

- FFD - Full Function Device. Dispositivo ZigBee, comúnmente un router, capaz de enviar y recibir información a dispositivos finales u otros routers.

- Firmware. Es el conjunto de instrucciones de un programa informático que se encuentra registrado en una memoria ROM, flash o similar. Estas instrucciones fijan la lógica primaria y ejercen el control de los circuitos de alguna clase de dispositivo.

- GTS - Guaranteed Time Slots. Son las partes de una trama activa que un coordinador PAN puede dedicar a las aplicaciones para lograr mínima latencia en caso de haber mucho tráfico en ciertos dispositivos que tengan cierta prioridad.

- HAN-Home Area Network. La red de área doméstica es un conjunto de dispositivos de todo tipo, informáticos (PC´s) o no (electrodomésticos) instalados

en un hogar y conectados entre sí. Todos ellos pueden incluso ser operados a distancia mediante internet.

- Hash criptográfico. Son funciones que permiten verificar la integridad de los mensajes. Una función hash transforma cadenas de bits de longitudes arbitrarias pero finitas, en otras cadenas de longitud fija de n-bits.

- HD-High Definition. Alta definición es un sistema de video con una resolución 1280x720 y 1920x1080 píxeles. La captura de imágenes en alta definición y la visualización, combinada con las nuevas técnicas de codificación y transmisión digital, pueden proporcionar imágenes con una resolución de hasta cuatro veces mejor que la televisión estándar.

- Hollo flood. Ataque informático en el que utilizando una antena de alta ganancia el atacante se presenta como vecino de un cierto número de sensores cuando no tienen la capacidad de emisión suficiente lo que provoca el consumo de las baterías.

- IBM. International Business Machines (IBM). Es una empresa multinacional estadounidense de tecnología y consultoría con sede en Armonk, Nueva York. IBM fabrica y comercializa hardware y software para computadoras, y ofrece servicios de infraestructura, alojamiento de internet, y consultoría en una amplia gama de áreas relacionadas con la informática, desde computadoras centrales hasta nanotecnología.

- IC (Integrated Circuits - Circuitos Integrados). Es una combinación de elementos de un circuito que están miniaturizados y que forman parte de un mismo chip soporte. El CI está elaborado con un material semiconductor, sobre el cual se fabrican los circuitos electrónicos a través de la fotolitografía. estos circuitos, que ocupan unos pocos milímetros, se encuentran protegidos por un encapsulado con conductores metálicos que permiten establecer la conexión entre dicha pastilla de material semiconductor y el circuito impreso.

- IEEE. Corresponde a las siglas de Institute of Electrical and Electronics Engineers, en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización de tecnología. Está formada por profesionales de nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática, matemáticos aplicados, ingenieros en biomédica, ingenieros en telecomunicaciones e ingenieros en mecatrónica.

- Insiders. Este ataque se lleva a cabo cuando una persona dentro de una organización adquiere un cierto nivel de confianza para obtener información y la usa para sus propósitos.
- IR comandos. Comandos utilizados para programar controles con tecnología infrarroja.
- ISM Industrial, Scientific and Medical-Industrial –Industrial, Científica y Médica Industrial). ISM es el acrónimo del nombre que se le da a las bandas de frecuencias para uso sin licencia reservadas internacionalmente para su uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. Estas bandas son las utilizadas por los teléfonos inalámbricos domésticos, microondas, Wi-Fi, Bluetooth.
- Jamming (interferencia o bloqueo). Es un tipo de ataque informático que desactiva o satura los recursos de la red informática. Por ejemplo, un atacante puede consumir toda la memoria o espacio en un disco, así como enviar demasiado tráfico a la red para que nadie pueda usarla.
- LQI - Link Quality Index. Acrónimo de Indicador de calidad de conexión.
- LR-WPAN - Low Rate Wireless Personal Area Network - Red de Área Personal Inalámbrica de Bajo Consumo. Son redes inalámbricas pequeñas de bajo rendimiento y costo que tienen como objetivo centrarse en aplicaciones que demandan rangos de comunicación pequeños de una persona o dispositivo. Este tipo de redes son usadas en equipos electrónicos que no requieren de altas tasas de transmisión de datos y bajo consumo de energía.
- mA. Unidad de medida usada para representar corriente eléctrica en dispositivos electrónicos.
- Mbps. Unidad de medida que se utiliza para representar la cantidad de información enviada en unidades de tiempo.
- MFR - MAC Footer. Parte final de la trama MAC en ZigBee.
- MHR - MAC Header. Encabezado de la trama MAC en ZigBee.
- Modo CBC-MAC. Es una técnica para la construcción de un mensaje de autenticación desde un libro de cifrado.
- Modo CCM. Protocolo que permite asegurar la confidencialidad de un mensaje enviado.
- Modo CTR. Modo de cifrado basado en un contador.

- MPDU - MAC Protocol Data Unit. Unidad de datos del protocolo MAC.
- MSDU - MAC Service Data Unit. Unidad de datos del servicio MAC.
- Multicast. Se basa en un único proceso de envío, independientemente del número de potenciales máquinas receptoras, de una misma información en una o más unidades de datos desde una máquina origen a todas las máquinas destinatarias que posean al menos un miembro de un determinado grupo de multidifusión y que, además, compartan una misma dirección de multidifusión; y, posiblemente, dispersas geográficamente en múltiples redes por internet.
- NAK (Negative Acknowledgement). Este mensaje se envía cuando no se obtiene una respuesta afirmativa de autenticación.
- Nonce. Término en inglés que se refiere a un número usado una sola vez.
- PAN. Las redes de área personal son una configuración básica usada en un entorno individual que está integrada por los dispositivos que están situados en el entorno local del usuario. Ya sea casa, trabajo, carro, parque, centro comercial. Esta configuración permite al usuario establecer una comunicación entre dispositivos a corto alcance y que sea de manera rápida y eficiente.
- Payload- carga útil. Es el conjunto de datos que representa la información del usuario.
- PC. Denominación a un equipo de cómputo fijo que es usado por un usuario.
- PCMCIA. Las tarjetas PCMCIA son interfaces de hardware un poco más grandes que una tarjeta de crédito estándar que habilita una función adicional en algún equipo portátil (Laptop y otros dispositivos portátiles).
- PDA Personal Digital Assistant. Es un dispositivo pequeño que combina las funciones de una computadora, teléfono/fax, internet y conexiones de red.
- Peer to peer. Son conexiones conocidas como punto a punto es decir dos equipos conectados directamente entre sí.
- Pendrive. Es un dispositivo de almacenamiento de información que se conecta a un equipo de cómputo y se utiliza para guardar todo tipo de datos como documentos, música, video, fotos.
- PHY. Capa de red más básica de la arquitectura ZigBee, es la encargada de proporcionar los medios para transmitir bit a bit sobre un enlace de datos físico conectado a nodos de red.

- PLME. Acrónimo en inglés de Entidad de Administración de Capa Física.
- PPDU Unidad de Datos de Protocolo de capa física PHY. Es la unidad de información que se utiliza en la capa física del modelo de arquitectura ZigBee.
- Relays. Relevadores en español que permiten tener control remoto de apagado y encendido en los dispositivos inalámbricos.
- RF (Radio Frecuencia). El término radiofrecuencia, también denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre 3kHz y 300GHz. Hz es la unidad de medida de la frecuencia de ondas y corresponde a un ciclo por segundo.
- RFC. Son un conjunto de documentos que sirven como referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.
- RFD - Reduced Function Device. Dispositivos ZigBee que se utilizan como dispositivos finales, reciben la información por medio de un router.
- RMS. Acrónimo en inglés de valor medio cuadrático.
- Router. Router o enrutador es un punto de acceso o dispositivo que envía datos desde una red de área local (LAN) o red de área amplia (WAN) a otra. El enrutador monitorea y controla el flujo de datos, y envía información a través de la ruta más eficiente en función del tráfico, el costo, la velocidad, las conexiones.
- SAP (Service Access Point - Punto de Acceso de Servicio). Interfaz que existen entre entidades de servicio que hay en los grupos de bloques llamados capas.
- SHR - Synchronization Header - Encabezado de Sincronización. Encabezado de la unidad de datos de protocolo de la capa física en ZigBee que permite gestionar el envío de información de forma ordenada.
- Sinkhole. Nombre de ataque de intrusión en redes inalámbricas de sensores.
- SSAP. Acrónimo de Servicio Fuente del Punto de Acceso.
- Subcapa APS. La subcapa de soporte de aplicación proporciona una interfaz entre la capa de red y la capa de aplicación en redes ZigBee a través de un conjunto de servicios que se utilizan junto a los ZDO y otros objetos que hayan sido definidos por los fabricantes.

- Subcapa de control de acceso al medio ZigBee MAC.
- PHR. Encabezado de la trama PPDU de la capa física que indica la longitud de un paquete.
- Unicast. Se basa en un proceso de envío de información en una o más unidades de datos desde una máquina origen a una única máquina destino o receptor final.
- Wi-Fi. Del inglés Wireless Fidelity o Fidelidad inalámbrica. Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como "Wi-Fi" pueden operar entre sí incluso si son de marca diferente.
- WPAN. Wireless Personal Area Network, Red Inalámbrica de Área Personal o Red de área personal es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal.
- ZC - ZigBee coordinator. El dispositivo coordinador es la raíz de una red ZigBee y sirve como puente hacia otras redes. Es capaz de almacenar información sobre la red y puede actuar como un banco de claves de seguridad. Solo puede existir un coordinador Zigbee en la red.
- ZDO (ZigBee Device Objects - Objetos de Dispositivo Zigbee). Los objetos de dispositivos ZigBee son la interfaz que se encuentra entre la capa de aplicación y la subcapa de soporte de aplicación. Permite así que se cumplan todos los requisitos de las aplicaciones que operan con la pila de protocolo ZigBee.
- ZigBee. ZigBee es una tecnología inalámbrica de corto alcance y bajo consumo, originaria de la antigua alianza HomeRF y que se definió como una solución inalámbrica de baja capacidad para aplicaciones en el hogar como la seguridad y la automatización. Algunas de sus aplicaciones son: Domótica, Automatización industrial, reconocimiento remoto, juguetes interactivos, medicina.
- ZR - ZigBee Router. Dispositivo que se encarga de interconectar dispositivos separados en la topología de red. Transmite mensajes desde un dispositivo final ZigBee hacia otros routers o dispositivos coordinadores.

REFERENCIAS

Bibliografía

López Barrientos, M., & Quezada Reyes, C. (2006). *Fundamentos de Seguridad Informática.* México D.F.: UNAM.

Magaña, E., Iskue, E., & Prieto, M. (2003). *Comunicaciones y Redes de Computadores, Problemas y Ejercicios Resueltos.* México D.F.: Pearson Educación.

Tanenbaum, A. (2003). *Redes de Computadoras.* México D.F.: Pearson Educación.

Fuentes de información

1. **Cable de par trenzado**
   (Última revisión: 12-Febrero-2011)

   (http://proxy.iescon (Cable de Par Trenzado, 2011)

2. **Cable de par trenzado**
   (Última revisión: 13-Marzo-2011)

   http://es.wikipedia.org/wiki/Cable_de_par_trenzado

3. **Comparación de ZigBee con otras tecnologías**
   (Última revisión: 16-Mayo-2011)

   http://www.tutorial-reports.com/wireless/zigbee/zigbee-comparisons.php

4. **Definición de estándar**
   (Última revisión: 28-Marzo-2011)

   http://www.eveliux.com/mx/estandares-de-telecomunicaciones.php

5. **Espectro radioeléctrico**
(Última revisión: 12-Abril-2014)

http://bibing.us.es/proyectos/abreproy/11677/fichero/Volumen+1%252F4.-Espectro+Radioel%E9ctrico.pdf

6. **Estándares de redes inalámbricas**
(Última revisión: 8-Abril-2011)

http://www.metrologicmexico.com/contenido1/informacion_tecnica/estandares_inalambricos.

7. **Estándares de telecomunicaciones**
(Última revisión: 14-Agosto-2011)

http://www.eveliux.com/mx/estandares-de-telecomunicaciones.php

8. **Estándares inalámbricos**
(Última revisión: 16-Abril-2014)

http://www.x-net.es/tecnologia/wireless.pdf

9. **Ethernet**
(Última revisión: 28-Marzo-2011)

http://www.uni-koblenz.de/~ros/Rechnerorganisation/ethernet.pdf

10. **Fibra óptica**
(Última revisión: 28-Marzo-2011)

http://www.monografias.com/trabajos-pdf/fibra-optica-maravilla-moderna/fibra-optica-maravilla-moderna.pdf

11. Hardware y Software usado en ZigBee
(Última revision: 19-Agosto-2012)

http://rua.ua.es/dspace/bitstream/10045/1109/1/InformeTecZB.pdf

12. Información sobre tarjeta de red
(Última revisión: 12-Febrero-2011)

http://www.wisegeek.com/what-is-a-network-interface-card.htm

13. Introducción capítulo 3
(Última revisión: 15-Julio-2011)

http://www.uv.es/montanan/ampliacion/trabajos/Redes%20de%20Sensores.pdf

14. Organismos de estandarización
(Última revisión: 31-Marzo-2011)
http://www.ramonmillan.com/enlaces/enlacesOrganismos.php

15. Protocolo 802.15.4
(Última revisión: 09-Mayo-2011)

http://www.dea.icai.upco.es/sadot/Comunicaciones/avanzadas/Alberto_Gasc%C3%B3n_Zigbee%20y%20el%20Est%C3%A1ndar%20IEEE%20802.15.4.pdf

16. Radiotransmisión
(Última revisión: 12-Agosto-2011)

http://s3.amazonaws.com/lcp/malvasanchez/myfiles/Propagacion-de-Ondas-Electromagneticas.pdf

17. Redes inalámbricas
(Última revisión: 06-Abril-2011)

http://www.redsinfronteras.org/pdf/redes_wireless.pdf

18. Stack Zigbee
(Última Revisión: 03-Mayo-2011)

http://www.eetasia.com/ARTICLES/2006JAN/PDF/EEOL_2006JAN02_RFD_NETD_TA_01.pdf?SOURCES=DOWNLOAD

19. Switches y Ruteadores
(Última revisión: 28-Marzo-2011)

http://www.redes-linux.com/manuales/Tecnologia_redes/switchesyruteadores.pdf

20. Tabla modelo OSI
(Última revisión: 07-Marzo-2011)

https://learningnetwork.cisco.com/.../OSI%20Model%20Concepts.pdf

21. Transmisión por ondas de luz
(Última revisión: 12-Agostto-2011)

http://es.wikipedia.org/wiki/Comunicaci%C3%B3n_%C3%B3ptica_por_el_espacio_libre