CAPÍTULO 3: ESTÁNDAR IEEE 802.15.4

“REDES ZIGBEE”

3.1 Introducción y características principales

Zigbee es un estándar de comunicaciones inalámbricas diseñado por la Zigbee Alliance. Es un conjunto estandarizado de soluciones que pueden ser implementadas por cualquier fabricante. Zigbee está basado en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (Wireless Personal Area Network, WPAN) y tiene como objetivo las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

Zigbee es un sistema ideal para redes domóticas, específicamente diseñado para reemplazar la proliferación de sensores/actuadores individuales. Zigbee fue creado para cubrir la necesidad del mercado de un sistema a bajo coste, un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable.

El nombre "Zigbee" se deriva de los patrones erráticos comunicativos que hacen muchas abejas entre las flores durante la recogida de polen. Esto es evocador de las redes invisibles de las conexiones existentes 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 un ordenador central.

Para llevar a cabo este sistema, un grupo de trabajo llamado Alianza Zigbee (Zigbee Alliance) formado por varias industrias, sin ánimo de lucro, la mayoría de ellas fabricantes de semiconductores, está desarrollando el estándar. La alianza de empresas está trabajando codo con codo con IEEE para asegurar una integración, completa y operativa.

Esta alianza en las cuales destacan empresas como Invensys, Mitsubishi, Philips y Motorola trabajan para crear un sistema estándar de comunicaciones, vía radio y 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 del Bluetooth.

Esta nueva aplicación, definida por la propia Zigbee Alliance como el nuevo estándar global para la automatización del hogar, permite que las aplicaciones domóticas desarrolladas por los fabricantes sean completamente ínter operables entre sí, garantizando así al cliente final fiabilidad, control, seguridad y comodidad.

Además la Zigbee Alliance también deja disponible para su acceso la Zigbee Cluster Library, ofreciendo de este modo a los ingenieros y demás integradores, deseosos de trabajar bajo este estándar mundial idóneo para los servicios domóticos, bloques de construcción para aplicaciones con necesidades bajo el denominador común de la automatización residencial, reduciendo de este modo las labores de desarrollo y permitiendo implementaciones más precisas.

3.2 Topologías y modelos de comunicación

3.2.1 Topologías

El protocoloZigbee permite tres topologías de red:

- Topología en estrella: el coordinador se sitúa en el centro.
- Topología en árbol: el coordinador será la raíz del árbol.
- Topología de malla: al menos uno de los nodos tendrá más de dos conexiones.

La figura 3.1 muestra las topologías de red Zigbee.

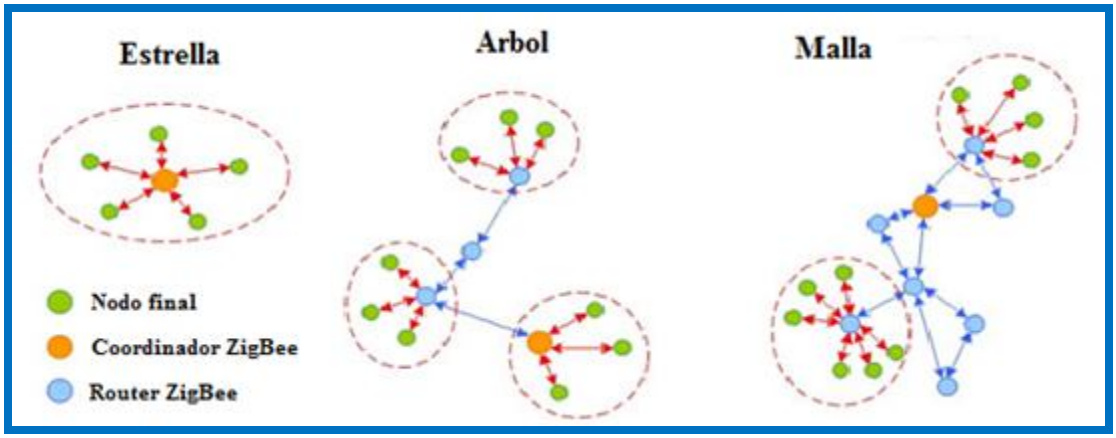

Figura 3.1 Topologías de redes Zigbee

La topología más interesante, y una de las causas por las que parece que puede triunfar Zigbee, es la topología de malla. Ésta permite que si, en un momento dado, un nodo del camino falla y se cae, pueda seguir la comunicación entre todos los demás nodos debido a que se rehacen todos los caminos. La administración de los caminos es tarea del coordinador.

3.2.2 Modelos de comunicación

Modelo de comunicación de alto nivel de Zigbee

Una aplicación consiste en un conjunto de objetos que se comunican entre sí y cooperan para llevar a cabo un trabajo. El propósito de Zigbee es distribuir este trabajo entre muchos nodos distintos que se asocian formando una red, este trabajo será en general local a cada nodo en gran parte, como por ejemplo el control de cada electrodoméstico individual dentro de una vivienda.

El conjunto de objetos que conforma la red se comunica utilizando los servicios de la subcapa de soporte de aplicación (APS), los cuales son el servicio necesario para la transmisión de datos y el transporte de datos de aplicación entre dos o más dispositivos en

la misma red, y el servicio de descubrimiento y enlace de dispositivos, supervisado a su vez por las interfaces ZDO (Zigbee Device Objects u Objetos de Dispositivo Zigbee). El nivel de aplicación sigue un diseño clásico de servicios estructurados en tipos petición-confirmación/indicación-respuesta. Dentro de un dispositivo puede haber hasta 240 objetos, con números entre 1 y 240 o se reserva para el interfaz de datos de ZDO y 255 para broadcast; el rango 241-254 se reserva para usos futuros.

Existen dos servicios utilizables por los objetos de aplicación:

- El servicio de pares clave-valor (key-value pair, KPV) se utiliza para realizar la configuración, definiendo, solicitando o modificando valores de atributos de objetos por medio de una interfaz simple basada en primitivas get/set, algunas de ellas con petición de respuesta. Se utiliza XML comprimido (extensible a XML puro) para lograr una solución sencilla y flexible.
- El servicio de mensajes está diseñado para ofrecer una aproximación general al tratamiento de información, sin necesidad de adaptar protocolos de aplicación y buscando evitar la sobrecarga que presenta KPV. Permite el envío de un payload (carga útil) arbitrario a través de tramas APS.

El direccionamiento es, a su vez, parte del nivel de aplicación. Un nodo está formado por un transceptor de radio compatible con 802.15.4 y una o más descripciones de dispositivo (colecciones de atributos que pueden consultarse o asignarse, o se pueden monitorizar por medio de eventos). El transceptor es la base del direccionamiento, mientras que los dispositivos dentro de un nodo se identifican por medio de un dispositivo final (endpoint) numerado entre 1 y 240.

3.3 Definición del estándar Zigbee

Zigbee es un protocolo de comunicaciones inalámbrico basado en el estándar de comunicaciones para redes inalámbricas IEEE 802.15.4. Creado por Zigbee Alliance, una organización, teóricamente sin ánimo de lucro, de más de 200 grandes empresas (destacan Mitsubishi, Honeywell, Philips, Motorola, entre otros), muchas de ellas fabricantes de semiconductores.

Este protocolo está siendo proyectado para permitir comunicación inalámbrica confiable, con bajo consumo de energía y bajas tasas de transmisión para aplicaciones de monitoreo y control.

Zigbee permite que dispositivos electrónicos de bajo consumo puedan realizar sus comunicaciones inalámbricas. Es especialmente útil para redes de sensores en entornos industriales, médicos y, sobre todo, domóticos.

Las comunicaciones Zigbee se realizan en la banda libre de 2.4GHz. A diferencia de Bluetooth no utiliza FHSS (Frequency hooping), sino que realiza las comunicaciones a través de una única frecuencia, es decir, de un canal. Normalmente puede escogerse un canal de entre 16 posibles. El alcance depende de la potencia de emisión del dispositivo así como el tipo de antenas utilizadas (cerámicas, dipolos).

El alcance normal con antena dipolo en visión directa suele ser aproximadamente (tomando como ejemplo el caso de Max Stream, en la versión de 1mW de potencia) de 100m y en interiores de unos 30m.

La velocidad de transmisión de datos de una red Zigbee es de hasta 256kbps. Por último decir que una red Zigbee la pueden formar, teóricamente, hasta 65535 equipos, es decir, el protocolo está preparado para poder controlar en la misma red esta cantidad enorme de dispositivos. La realidad es menor, siendo, de todas formas, de miles de equipos.

3.4 Tipos de dispositivos

Se definen tres tipos distintos de dispositivo Zigbee según su papel en la red:

- Coordinador Zigbee (Zigbee Coordinator, ZC). El tipo de dispositivo más completo. Debe existir uno por red. Sus funciones son las de encargarse de controlar la red y los caminos que deben seguir los dispositivos para conectarse entre ellos.
- Router Zigbee (Zigbee Router, ZR). Interconecta dispositivos separados en la topología de la red, además de ofrecer un nivel de aplicación para la ejecución de código de usuario.
- Dispositivo final (Zigbee End Device, ZED). 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.

Como ejemplo de aplicación en Domótica, en una habitación de la casa tendríamos diversos dispositivos finales como un interruptor y una lámpara y una red de interconexión realizada con Routers Zigbee y gobernada por el Coordinador. La figura 3.2 muestra los tipos de dispositivos Zigbee.

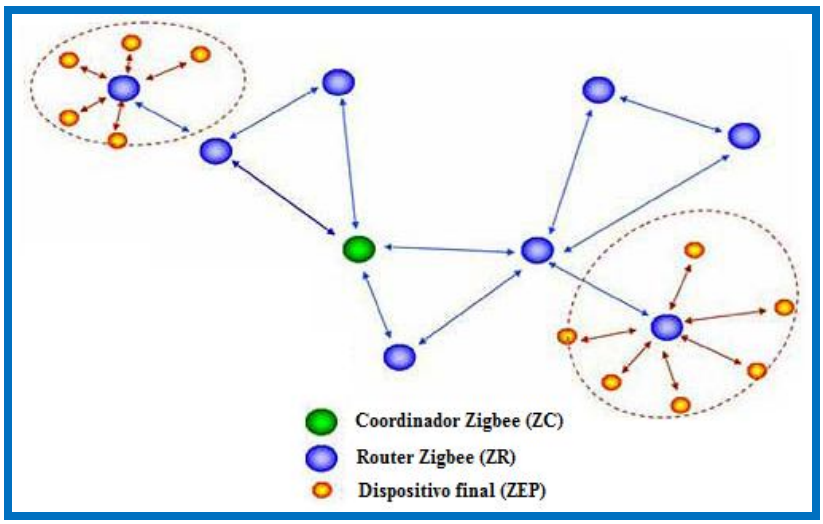

Figura 3.2 Dispositivos Zigbee.

3.5 Funcionalidad

Basándose en su funcionalidad, pueden plantearse dos modos de operación:

a) *Dispositivo de funcionalidad completa* (FFD): También conocidos como nodo activo. Es capaz de recibir mensajes en formato 802.15.4. Gracias a la memoria adicional y a la capacidad de procesar, puede funcionar como Coordinador o Router Zigbee, o puede ser usado en dispositivos de red que actúen de interface con los usuarios.
b) *Dispositivo de funcionalidad reducida* (RFD): También conocido como nodo pasivo. Tiene capacidad y funcionalidad limitadas (especificada en el estándar) con el objetivo de conseguir un bajo coste y una gran simplicidad. Básicamente, son los sensores/actuadores de la red.

Dispositivos FFD pueden comunicarse con dispositivos RDF o entre sí, mientras dispositivos RDF sólo pueden comunicarse con dispositivos FFD.

Un nodo Zigbee, tanto activo como pasivo, reduce su consumo gracias a que puede permanecer "dormido" la mayor parte del tiempo, incluso muchos días seguidos.

Cuando se requiere su uso, el nodo Zigbee es capaz de "despertar" en un tiempo muy corto, para volverse a dormir cuando deje de ser requerido. Un nodo cualquiera "despierta" en aproximadamente 15 ms. Además de este tiempo, se muestran otras medidas de tiempo de funciones comunes:

- Nueva enumeración de los nodos esclavo (por parte del coordinador): aproximadamente 30 ms.
- Acceso al canal entre un nodo activo y uno pasivo: aproximadamente 15 ms.

3.6 Espectro Zigbee

Respecto al espectro Zigbee tenemos lo siguiente:

- Un canal entre 868MHz y 868.6MHz, Ch1 hasta Ch10.
- Diez canales entre 902.0MHz y 928.0MHz, Ch1 hasta Ch10.
- Dieciséis canales entre 2.4GHz y 2.4835GHz, Ch1 hasta Ch26.

El estándar ZigBee especifica una sensibilidad en el receptor de -85dBm en la banda de los 2.4GHz. Y un sensibilidad de -92dBm en la banda 865/915MHz.

La figura 3.3 muestra el espectro Zigbee y sus similitudes con el espectro WiFi.

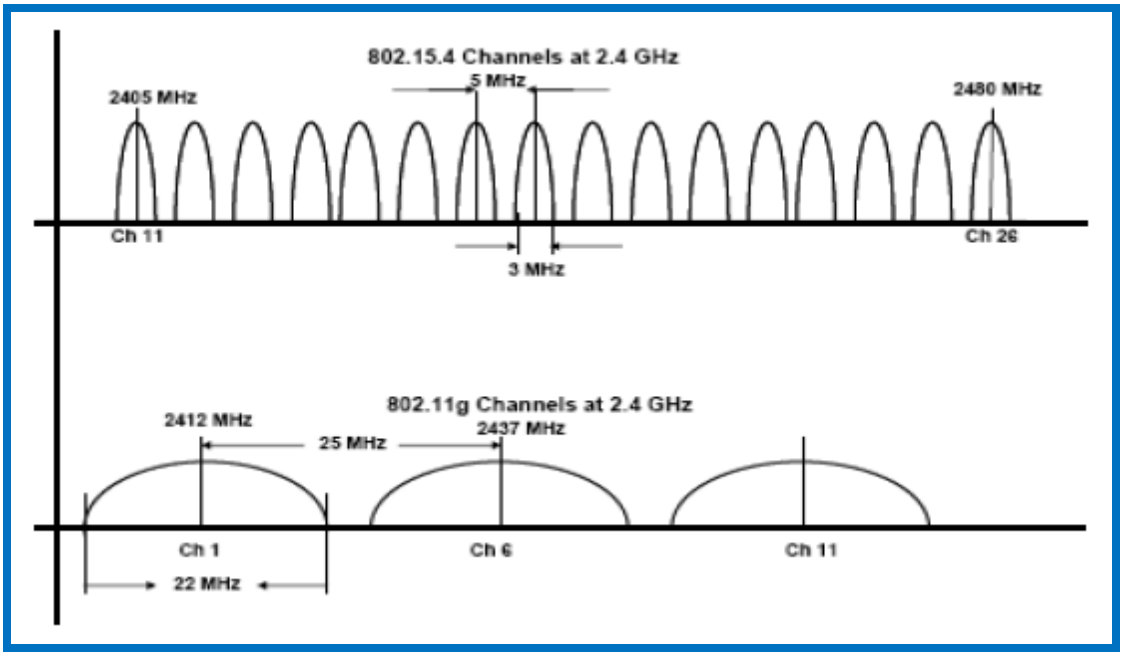

Figura 3.3 Zigbee y su espectro compartido con WiFi.

Técnicas de Modulación

a) Modulación OQPSK (Offset Quadrature Phase Shift Keying)
La modulación OQPSK consiste en realizar una transición de fase en cada intervalo de señalización de bits, por portadora en cuadratura.

b) Modulación BPSK (Binary Phase Shift Keying)
En esta modulación se tiene como resultados posibles dos fases de salida para la portadora con una sola frecuencia. Una fase de salida representa un 1 lógico y la otra un 0 lógico. Conforme la señal digital de entrada cambia de estado, la fase de la portadora de salida se desplaza entre dos ángulos que están 180° fuera de fase.(Ver tabla 3.1).

Banda de frecuencia (MHz)	Parametros de difusión		Parametros de datos		
	Tasa de chip (kchip/s)	Modulación	Tasa de bits (kb/s)	Velocidad de simbolo (ksymbol/s)	Simbolos
868-868.6	300	BPSK	20	20	BINARIO
902-928	600	BPSK	40	40	BINARIO
2400-2483.5	2000	O-QPSK	250	62.5	HEXADECIMAL

Tabla 3.1 Tasa de datos asociada a la frecuencia de operación.

Independientemente de la banda de frecuencia a la que se transmita, la trama procesada en la capa física se muestra en la figura 3.4:

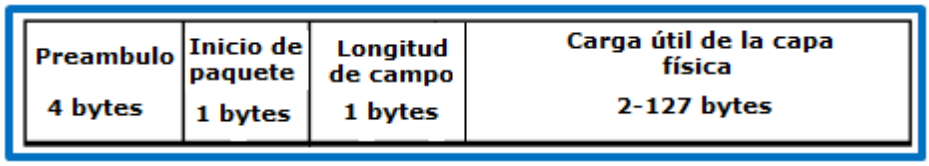

Figura 3.4 Trama Zigbee

3.7 Protocolos

Los protocolos se basan en investigaciones recientes sobre algoritmos de red para la construcción de redes ad-hoc de baja velocidad. La mayoría de redes grandes están pensadas para formar un cluster de clusters. También puede estructurarse en forma de malla o como un solo cluster. Los perfiles actuales de los protocolos soportan redes que utilicen o no facilidades de balizado, quees un mecanismo de control del consumo de potencia en la red.

Las redes sin balizas acceden al canal por medio de CSMA/CA (Carrier Sense Multiple Access Collision Avoidance o acceso múltiple por detección de portadora con prevención de colisiones), que es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Los routers suelen estar activos todo el tiempo, por lo que requieren una alimentación estable en general. Esto, a cambio, permite redes en las que algunos dispositivos pueden estar transmitiendo todo el tiempo, mientras que otros sólo transmiten ante la presencia de estímulos externos.

Si la red utiliza balizas, los routers las generan periódicamente para confirmar su presencia a otros nodos. Los nodos pueden desactivarse entre las recepciones de balizas reduciendo su ciclo de servicio. Los intervalos de balizado pueden ir desde 5,36 ms a 15,36 ms * 2^{14} = 251,65824 segundos a 250 Kbps; de 24 ms a 24 ms * 2^{14} = 393,216 segundos a 40 Kbps; y de 48 ms a 48 ms * 2^{14} = 786,432 segundos a 20 Kbps. Sin embargo, los periodos largos con ciclos de servicio cortos necesitan que una temporización precisa, lo que puede ir en contra del principio de bajo costo.

En general, los protocolos Zigbee minimizan el tiempo de actividad de la radio para evitar el uso de energía. En las redes con balizas los nodos sólo necesitan estar despiertos mientras se transmiten las balizas, además de cuando se les asigna tiempo para transmitir. Si no hay balizas, el consumo es asimétrico repartido en dispositivos permanentemente activos y otros que sólo no están esporádicamente.

Los dispositivos Zigbee deben respetar el estándar de WPAN de baja tasa de transmisión IEEE 802.15.4-2003. Éste define los niveles más bajos: el nivel físico y el control de acceso al medio. El estándar trabaja sobre las bandas ISM(Industrial, Scientific and Medical o industriales, científicas y médicas)de uso no regulado, que son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en dichas

áreas. Se definen hasta 16 canales en el rango de 2,4 GHz, cada uno de ellos con un ancho de banda de 5 MHz.

Las radios utilizan un espectro de dispersión de secuencia directa. Se utiliza BPSK en los dos rangos menores de frecuencia, así como un QPSK ortogonal que transmite dos bits por símbolo en la banda de 2,4 Ghz. Ésta permite tasas de transmisión en el aire de hasta 250 Kbps, mientras que las bandas inferiores se han ampliado con la última revisión a esta tasa desde los 40 Kbps de la primera versión. Los rangos de transmisión oscilan entre los 10 y 75 metros, aunque depende bastante del entorno. La potencia de salida de las radios suele ser de 1 mW.

Si bien en general se utiliza CSMA/CA para evitar colisiones en la transmisión, hay algunas excepciones a su uso, por una parte, las tramas siguen una temporización fija que debe ser respetada; por otra, las confirmaciones de envíos tampoco siguen esta disciplina; por último, si se asignan slots de tiempo garantizados para una transmisión tampoco es posible que exista contención.

3.7.1 Arquitectura de los protocolos

La figura 3.5 muestra la pila de protocolos Zigbee.

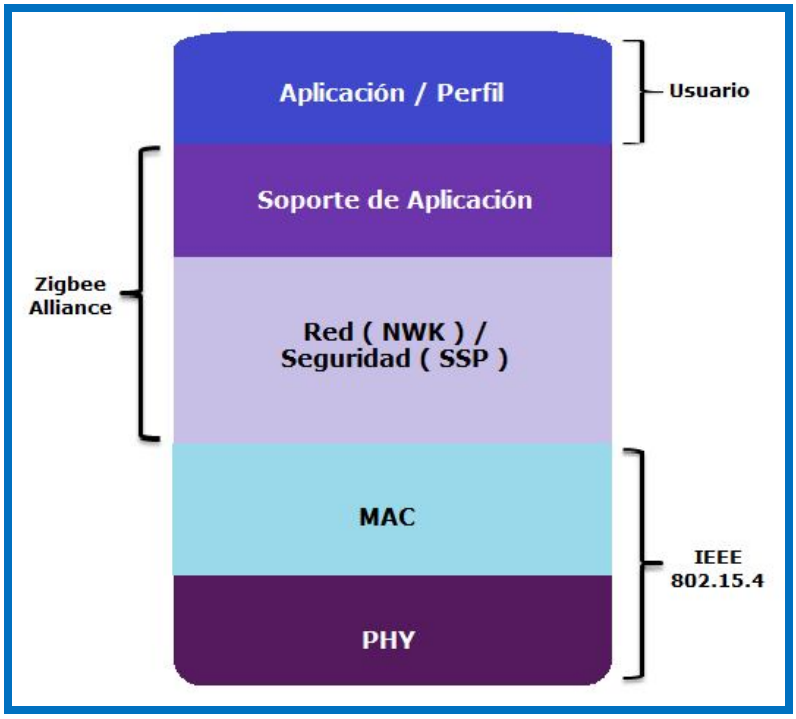

Figura 3.5 Pila de protocolos IEEE 802.15.4.

La capa de más bajo nivel es la capa física (PHY), que en conjunto con la capa de acceso al medio (MAC), brindan los servicios de transmisión de datos por el aire, punto a punto. Estas dos capas esta descritas en el estándar IEEE 802.15.4–2003.

El estándar trabaja sobre las bandas ISM de uso no regulado, dónde se definen hasta 16 canales en el rango de 2.4 GHz, cada una de ellas con un ancho de banda de 5 Mhz. Se utilizan radios con un *espectro de dispersión de secuencia directa*, lográndose tasas de transmisión en el aire de hasta 250 Kbps en rangos que oscilan entre los 10 y 75 m, los cuales dependen bastante del entorno.
La capa de red (NWK) 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 tener en cuenta que el algoritmo de enrutamiento que se usa es el de enrutamiento de malla, el cual se basa en el protocolo 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. Es en esta capa en donde se implementan las distintas topologías de red que Zigbee soporta.

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 de 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 están definidas por la Zigbee Alliance.

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. Es en esta capa donde se encuentran los ZDO que se encargan de definir el papel del dispositivo en la red, si el actuará como coordinador, ruteador o dispositivo final; la subcapa APS y los objetos de aplicación definidos por cada uno de los fabricantes.

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

3.8 Empaquetamiento y direccionamiento

En Zigbee, el empaquetamiento se realiza en cuatro tipos diferentes de paquetes básicos, los cuales son: datos, ACK, MAC y baliza. En la figura 3.6 se muestran los campos de los cuatro tipos de paquetes básicos.

El paquete de datos tiene una carga de datos de hasta 104 bytes. La trama esta numerada para asegurar que todos los paquetes llegan a su destino. Un campo nos 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 dónde se realiza una realimentación desde el receptor al emisor, de esta 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. La figura 3.6 muestra los paquetes básicos de Zigbee.

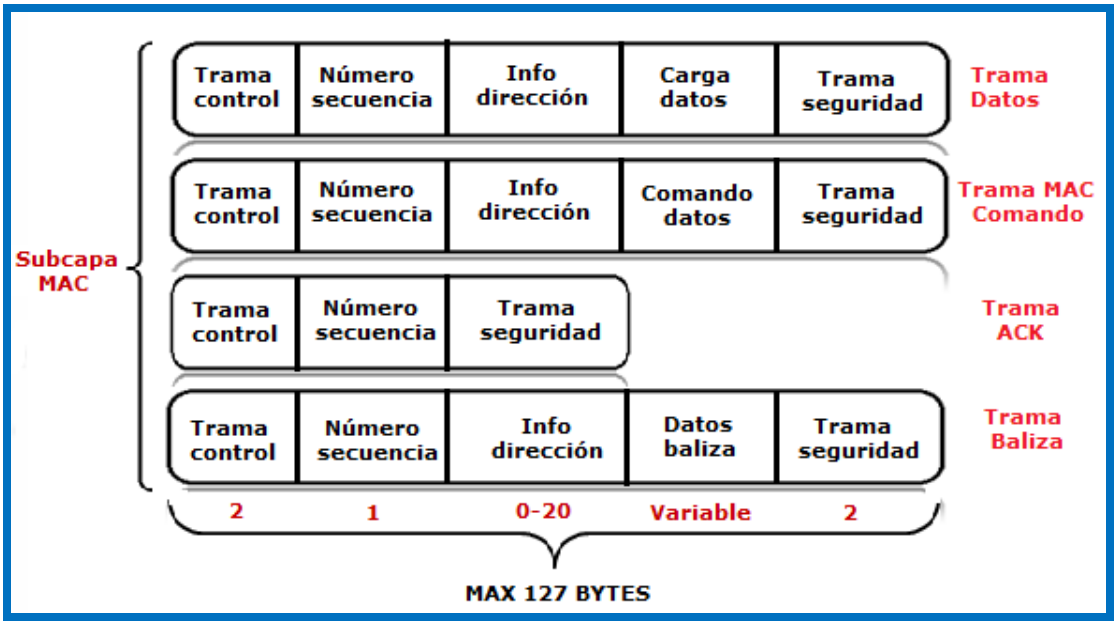

Figura 3.6 Campos de los cuatro tipos de paquetes básicos de Zigbee.

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 dónde se implementan dos mecanismos de acceso al canal y una o más descripciones de dispositivo que son colecciones de atributos que pueden consultarse o asignarse, o se pueden monitorear por medio de eventos. El transceptor es la base del direccionamiento, mientras que los dispositivos dentro de un nodo se identifican por medio de un end point(dispositivo final) numerado entre 1 y 240.

Los dispositivos se direccionan empleando 64-bits y un direccionamiento corto opcional de 16 bits. El campo de dirección incluido en MAC puede contener información de direccionamiento de ambos orígenes y destinos, necesarios para operar punto a punto. Este doble direccionamiento es usado para prevenir un fallo dentro de la red.

Los dos mecanismos de acceso al canal que se implementan en Zigbee corresponden para 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, puede ocurrir que el dispositivo destino puede no escuchar 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 rompimiento de cristales, duermen prácticamente todo el tiempo. Para que se les tenga 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 super trama para controlar el acceso al canal, esta super trama es estudiada por el coordinador de red para transmitir “tramas baliza” cada ciertos intervalos (múltiples cada de 15.38 ms hasta cada 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 denominado "balizamiento". Un dispositivo que quiera intervenir, lo primero que tendrá que hacer es registrarse para el coordinador, y es entonces cuando mira si hay mensajes para él. En el caso de que no haya mensajes, este dispositivo vuelve a "dormir", y se despierta de acuerdo a un horario que ha establecido previamente el coordinador. En cuanto el coordinador termina el "balizamiento", vuelve a "dormirse".

3.9 Ventajas y desventajas de Zigbee

Zigbee al igual que todas las tecnologías de comunicación tiene su lado positivo y sus inconvenientes:

Ventajas

- Ideal para conexiones punto a punto y punto a multipunto
- Diseñado para el direccionamiento de información y el refrescamiento de la red.
- Opera en la banda libre de ISM 2.4 GHz para conexiones inalámbricas.
- Óptimo para redes de baja tasa de transferencia de datos.
- Alojamiento de 16 bits a 64 bits de dirección extendida.
- Reduce tiempos de espera en el envío y recepción de paquetes.

- Detección de Energía (ED).
- Baja ciclo de trabajo - Proporciona larga duración de la batería.
- Soporte para múltiples topologías de red: Estática, dinámica, estrella y malla.
- Hasta 65.000 nodos en una red.
- 128-bit AES de cifrado - Provee conexiones seguras entre dispositivos.
- Son más baratos y de construcción más sencilla.
- Zigbee tiene un bajo nivel de radiación y, por tanto, se puede utilizar en el sector médico.
- Rango de 10 m a 75m.

Desventajas

- La tasa de transferencia es muy baja.
- Solo manipula textos pequeños comparados con otras tecnologías.
- Zigbee trabaja de manera que no puede ser compatible con Bluetooth en todos sus aspectos porque no llegan a tener las mismas tasas de transferencia, ni la misma capacidad de soporte para nodos.
- Tiene menor cobertura porque pertenece a redes inalámbricas de tipo WPAN.

3.10 Seguridad Zigbee

La seguridad de las transmisiones y de los datos son puntos clave en la tecnología Zigbee. Zigbee utiliza el modelo de seguridad de la subcapa MAC IEEE 802.15.4, la cual especifica 4 servicios de seguridad.

- **Control de accesos:** El dispositivo mantiene una lista de los dispositivos comprobados en la red.
- **Datos Encriptados:** Los cuales usan una encriptación con un código de 128 bits.
- **Integración de tramas:** Protegen los datos de ser modificados por otros.
- **Secuencias de refresco:** Comprueban que las tramas no han sido reemplazadas por otras. El controlador de red comprueba estas tramas de refresco y su valor, para ver si son las esperadas.

3.10.1 Modelo básico de seguridad.

En Zigbee las claves son la base de la arquitectura de seguridad por lo tanto, su protección es fundamental para la integridad del sistema.

Las claves nunca deben transportarse utilizando un canal inseguro, si bien existe una excepción momentánea que se da en la fase inicial de la unión de un dispositivo desconfigurado a una red.

La red Zigbee debe tener particular cuidado, pues una red ad hoc puede ser accesible físicamente a cualquier dispositivo externo y el entorno de trabajo no se puede conocer de antemano. Las aplicaciones que se ejecutan en concurrencia utilizando el mismo transceptor de la misma manera deben confiar entre sí, ya que por motivos de coste no se

asume la existencia de un cortafuegos (firewall) entre las distintas entidades del nivel de aplicación.

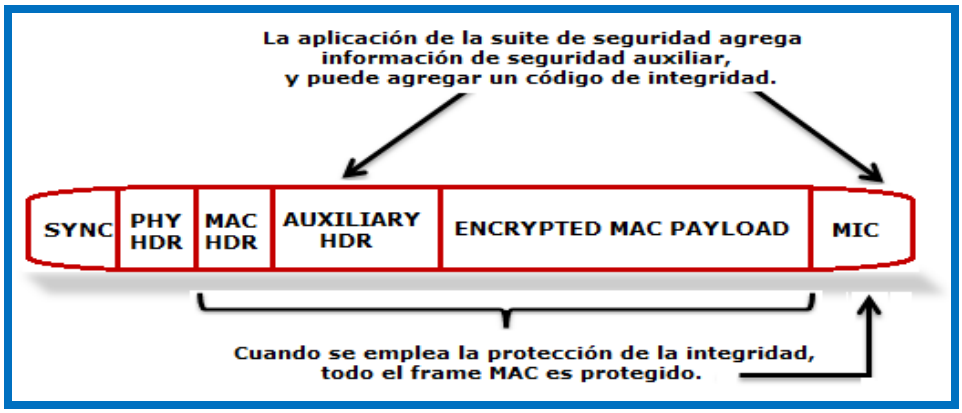

Figura 3.7 Seguridad Zigbee.

Los distintos niveles definidos dentro de la pila de protocolos no están separados criptográficamente, por lo se necesitan políticas de acceso, que se asumen correctas en su diseño. Este modelo de confianza abierta (open trust) posibilita la compartición de claves disminuyendo el coste de forma significativa. No obstante, el nivel que genera una trama es siempre el responsable de su seguridad. Todos los datos de las tramas del nivel de red han de estar cifradas, ya que podría haber dispositivos maliciosos, de forma que el tráfico no autorizado se previene de raíz. De nuevo, la excepción es la transmisión de la clave de red a un dispositivo nuevo, lo que dota a toda la red de un nivel de seguridad único. También es posible utilizar criptografía en enlaces punto a punto.

3.10.2 Arquitectura de seguridad.

Zigbee utiliza claves de 128 bits en sus mecanismos de seguridad. Una clave puede asociarse a una red, que es utilizable por los niveles de Zigbee y el subnivel MAC, o a un enlace.

Las claves de enlace se establecen en base a una clave maestra que controla la correspondencia entre claves de enlace. Como mínimo la clave maestra inicial debe obtenerse por medios seguros ya sea transporte o preinstalación, ya que la seguridad de toda la red depende de ella en última instancia. Los distintos servicios usarán variaciones unidireccionales de la clave de enlace para evitar riesgos de seguridad. Por lo tanto la distribución de claves es una de las funciones de seguridad más importantes.

Una red segura atribuye a un dispositivo especial la distribución de claves: el denominado centro de confianza o trust center. En un caso ideal los dispositivos llevarán precargados de fábrica la dirección del centro de confianza y la clave maestra inicial. Si se permiten vulnerabilidades momentáneas, se puede realizar el transporte como se ha descrito. Las aplicaciones que no requieran un nivel especialmente alto de seguridad utilizarán una clave enviada por el centro de confianza a través del canal inseguro transitorio.

Por tanto, el centro de confianza controla la clave de red y la seguridad punto a punto. Un dispositivo sólo aceptará conexiones que se originen con una clave enviada por el centro de confianza, salvo en el caso de la clave maestra inicial. La arquitectura de seguridad está distribuida entre los distintos niveles de la siguiente manera:

El subnivel MAC puede llevar a cabo comunicaciones fiables de un solo salto. En general, utiliza el nivel de seguridad indicado por los niveles superiores.

El nivel de red gestiona el ruteo, procesando los mensajes recibidos y pudiendo hacer broadcast de peticiones. Las tramas salientes usarán la clave de enlace correspondiente al ruteo realizado, si está disponible; en otro caso, se usará la clave de red.

El nivel de aplicación ofrece servicios de establecimiento de claves al ZDO y las aplicaciones, y es responsable de la difusión de los cambios que se produzcan en sus dispositivos a la red.

Estos cambios podrían estar provocados por los propios dispositivos o en el centro de confianza, que puede ordenar la eliminación de un dispositivo de la red, por ejemplo.

También encamina peticiones de los dispositivos al centro de seguridad y propaga a todos los dispositivos las renovaciones de la clave de red realizadas por el centro. El ZDO mantiene las políticas de seguridad del dispositivo.

3.11 El futuro de Zigbee

Zigbee tiene un gran potencial para el futuro. Los beneficios son numerosos para los propietarios de edificios, consultores, personal de mantenimiento, instaladores y usuarios finales. Las aplicaciones también son infinitas.

En el futuro, se vislumbra el uso del protocolo Zigbee en los sistemas de manejo de activos y de rastreo, generadores, elevadores, etc., compartiendo datos que pueden ser transformados en información viable, y permitiendo a los usuarios explotar sus negocios de manera más eficiente. Con el paso de los años, los fabricantes han desarrollado muchos lenguajes, incluyendo los inalámbricos, pero por primera vez ZigBee está en capacidad de dirigir los problemas de interoperabilidad, duración de la batería y costos.

Varias compañías están activamente integradas a Zigbee Alliance para poder ofrecer el soporte y la experiencia necesaria para desarrollar esta tecnología para futuras aplicaciones en la automatización de edificios.

Se espera que los módulos Zigbee sean los transmisores inalámbricos más baratos de la historia, y además producidos de forma masiva. Tendrán un costo nunca antes visto, y dispondrán de una antena integrada, control de frecuencia y una pequeña batería. Ofrecerán una solución tan económica porque la radio se puede fabricar con muchos menos circuitos analógicos de los que se necesitan habitualmente.

3.12 Recomendaciones

- ✓ Zigbee está diseñado específicamente para ser la solución a problemas inalámbricos siendo una unidad pequeña capaz de proveer monitoreo remoto inalámbrico a sensores y a unidades simples de entrada como controles de luces.

- ✓ Zigee Alliance propone a Zigbee como el nuevo estándar global para la automatización del hogar, porque permite que las aplicaciones domóticas desarrolladas por los fabricantes sean completamente interoperables entre sí, garantizando así al cliente final fiabilidad, control, seguridad y comodidad.

- ✓ Zigee es un estándar abierto, permitiendo que terceros mejoren la interoperabilidad entre dispositivos y las características generales del estándar.

- ✓ Zigbee es una tecnología WPAN que tiene la habilidad de formar una red de malla entre nodos permitiendo que el corto alcance entre nodos individuales sea expandido y multiplicado cubriendo un área mayor.

- ✓ Esta nueva aplicación fue creada para cubrir la necesidad del mercado de un sistema a bajo coste, un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable.

3.13 Áreas de aplicación

El mercado para las redes Zigbee comprende una amplia variedad de aplicaciones. En la actualidad un gran número de las compañías que forman parte de la Zigbee Alliance se encuentran desarrollando productos que van desde electrodomésticos hasta teléfonos celulares, impulsando el área que más les interesa.

Hay que tener en cuenta que Zigbee está diseñado para aplicaciones que transmiten unos cuantos bytes esporádicamente, que es el caso de una aplicación para automatizar el hogar. Al usar esta tecnología no habría la necesidad de cablear los interruptores, los cuales podrían ser cambiados de un lugar a otro con plena libertad, pudiendo por ejemplo, prender o apagar las luces de tu casa a través de Internet o utilizando tu teléfono celular en cualquier momento.

Una de las área de aplicación que ha tomado fuerza, es la de los sistemas de medición avanzada, medidores de agua, luz y gas que forman parte de una red con otros dispositivos como displays ubicados dentro de las casas, que pueden monitorear el consumo de energía y no sólo eso, sino que también pueden interactuar con electrodomésticos o cualquier otro sistema eléctrico como bombas de agua o calefacción, con la finalidad de aprovechar mejor la energía. Zigbee goza de un importante respaldo para la gestión energética y para las soluciones de consumo eficiente por parte de la industria de los servicios públicos; y por parte de los patrocinadores de las redes energéticas inteligentes en varios países.

Otra área de aplicación prometedora es el rastreo de bienes, también está en la lista la identificación vehicular, nodos ubicados en vehículos que permiten identificar al vehículo a distancia y descargar información que ha recopilado por un periodo de tiempo determinado, monitoreo médico de pacientes y cuidado personal, control de máquinas y herramientas y redes de sensores para el control industrial de plantas de proceso. Este tipo de escenarios se encuentran al alcance de la tecnología actual. Las anteriores son sólo algunas de las múltiples aplicaciones que se le pueden dar a las redes en cuestión. (Ver figura 3.8).

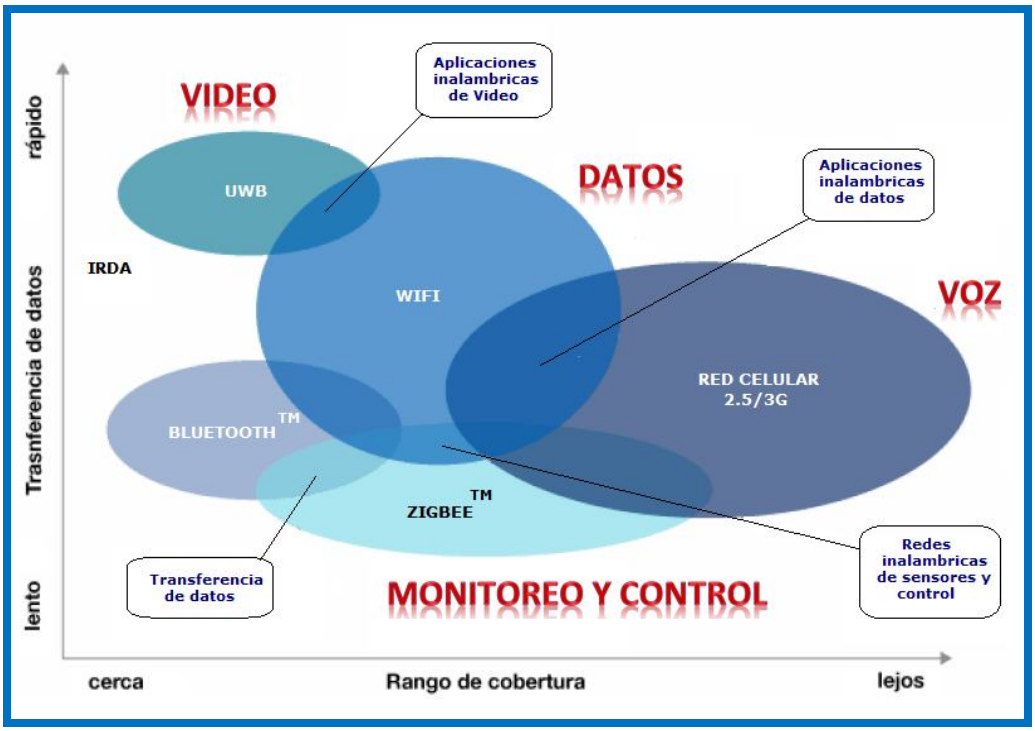

Figura 3.8. Grupos de aplicaciones que están en la mira de ZigBee.

En general, Zigbee resulta ideal para redes estáticas, escalables y con muchos dispositivos, pocos requisitos de ancho de banda y uso poco frecuente, y dónde se requiera una duración muy prolongada de la batería.

En ciertas condiciones y para determinadas aplicaciones puede ser una buena alternativa a otras tecnologías inalámbricas ya consolidadas en el mercado, como WiFi y Bluetooth, aunque la falta del soporte de TCP/IP no lo hace adecuado, por sí solo, para la interconexión de redes de comunicaciones IP. Por tanto, la introducción de Zigbee no acabará con otras tecnologías ya establecidas, sino que convivirá con ellas y encontrará sus propios rubros de aplicación.

3.13.1 Aplicaciones de alto nivel

No existen muchas aplicaciones de cara al usuario en los que Zigbee esté presente, sin embargo existen unos pocos pero que son bastante interesantes. En la figura 3.9 se observan algunas de las aplicaciones que tiene Zigbee.

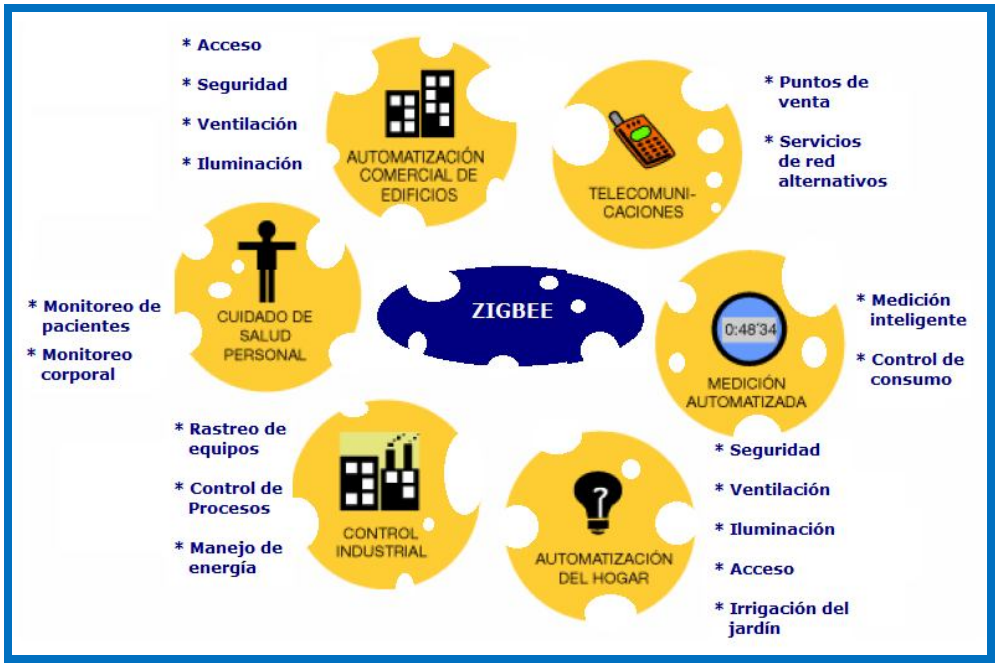

Figura 3.9. Diversos grupos de aplicaciones para Zigbee.

3.14 Zigbee vs Bluetooth

Como hemos visto Zigbee es muy similar al Bluetooth pero con algunas diferencias, entre estas diferencias tenemos principalmente las siguientes:

- 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 (Piconet) Bluetooth.
- Menor consumo eléctrico que el de Bluetooth. En términos exactos, Zigbee tiene un consumo de 30mA transmitiendo y de 3uA en reposo, frente a los 40mA transmitiendo y 0.2mA en reposo que tiene el 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 un 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 que el otro para ciertas cosas. Por ejemplo, mientras que el Bluetooth se usa para aplicaciones como los teléfonos móviles y la informática casera, la velocidad del Zigbee se hace insuficiente para estas tareas, desviándolo 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.

La tabla 3.2 ilustra una comparativa puntual de las principales características de desempeño y seguridad de Bluetooth y Zigbee, resaltando sus diferencias y similitudes para así escoger entre ambas e incluso complementar alguna con la otra.

Comparación de Bluetooth y Zigbee		
	Bluetooth	**Zigbee**
Bandas de frecuencias	**2.4 GHz**	**2.4 GHz, 868/915 MHz**
Tamaño de pila	**1 Mb**	**20 Mb**
Tasa de transferencia	**1 Mbps**	**250 kbps (2.4 GHz)** **40 kbps (915 MHz)** **20 kbps (868 MHz)**
Número de canales	**79**	**16 (2.4 GHz)** **10 (915 MHz)** **1 kbps (868 MHz)**
Tipos de datos	**Digital, Audio**	**Digital (Texto)**
Rango de nodos internos	**10m-100m**	**10m-100m**
Número de dispositivos	**8**	**255 / 65535**
Requisitos de alimentación	**Media – Días de bateria**	**Muy baja – Años de bateria**
Introducción al mercado	**Media**	**Baja**
Arquitecturas	**Estrella**	**Estrella, árbol y malla**
Mejoras de aplicaciones	**Computadoras y teléfonos**	**Control de bajo costo y monitoreo**
Consumo de potencia	**400 ma transmitiendo** **20 ma en reposo**	**30 ma transmitiendo** **3 ma en reposo**
Complejidad	**Complejo**	**Simple**
Precio	**Accesible**	**Bajo**
Seguridad	**64 bits, 128 bits**	**AES de 128 bits y definidas por el usuario a nivel de aplicación.**

Tabla 3.2 Zigbee vs Bluetooth.