Trabajo final integrador de especialización en Redes y Seguridad

ANÁLISIS DEL PROTOCOLO ZIGBEE

Alumno:

Jorge Pablo Dignani

Director:

Dr. Fernando G. Tinetti

Facultad de Informática
Universidad Nacional de La Plata
2011

Índice

1 Introducción

1.1 Contenido de este trabajo

En este trabajo se estudia el protocolo ZigBee de comunicaciones de datos en redes inalámbricas.

El trabajo comienza ubicando a ZigBee dentro del contexto de redes. Para esto, se clasifican las mismas según su cobertura en: redes de área geográfica o WAN (Wide Area Network), redes de área local o LAN (Local Area Network) y redes de área personal o PAN (Personal Area Network). También se clasifican de acuerdo al modo de conexión de sus nodos en: con cable o sin cable.

Se hace una comparación general de estándares inalámbricos en cuanto a consumo de potencia, capacidad de transmisión de datos y alcance. Con esto se ubica al estándar IEEE 802.15.4 destinado a cubrir con ventajas las aplicaciones de muy bajo consumo y baja velocidad de transmisión de datos. Se introduce el estándar ZigBee como una extensión del IEEE802.15.4

El trabajo continúa describiendo algunos de los muchos ejemplos de uso de ZigBee. Luego se estudia en profundidad cada una de las capas de ZigBee comenzando con la capa física hasta la capa aplicación. Se mencionan algunos aspectos de seguridad informática implementados en este protocolo.

Por último se hace una comparación de ZigBee con otras tecnologías como Bluetooth en diferentes escenarios haciendo hincapié en el consumo energético.

1.2 Motivaciones

El avance tecnológico en las dos últimas décadas en el área comunicaciones ha permitido el desarrollo de nuevos circuitos integrados de muy pequeño tamaño, alta eficiencia energética y bajo costo. Esto llevó a disponer de transmisores/receptores que operan en frecuencias de GHz. Aparece la explosión de redes inalámbricas (wireless) para aplicaciones con requerimientos disímiles en cuanto a transferencia de datos, alcance y costos.

El IEEE ha creado varios estándares dentro de la familia de 802.x que se han adoptado para las comunicaciones de datos inalámbricas. Hoy vemos en oficinas y casas la implementación de redes de área local inalámbricas (WLAN) basadas en el estándar IEEE 802.11. La utilización de teléfonos celulares para transmisión de datos prueba que las redes inalámbricas son aplicables a un costo relativamente bajo.

Hay muchas aplicaciones que requieren establecer una red de bajo alcance con baja tasa de transmisión. Estas redes se denominan LR-WPAN. (Low Rate Wireless Personal Area Network). Hay muchas soluciones propietarias para este tipo de redes, pero son caras, orientadas a un problema en particular e incompatibles entre ellas. El IEEE802.15.4 es un estándar para las LR-WPAN que provee una solución simple y de bajo costo. El ámbito de aplicación, entre otros, es el manejo de redes de sensores y activación de actuadores en domótica, monitoreo ambiental, industria, hospitales y hoteles. [2]. En el protocolo IEEE 802.15.4 se definen solo las 2 primeras capas ISO-

OSI (la capa física y la de enlace). Fue especialmente definido para estandarizar las redes de sensores WSN (wireless sensor network).

Cada vez más se irán conectando sensores y actuadores en casas, industrias y hospitales. ZigBee es uno de los protocolos dominantes en redes WPAN y es fundamental tener un conocimiento cabal del mismo para implementar redes de sensores y actuadores. La tendencia es que en un futuro cercano se tendrá la "Internet of things" en donde todas las cosas estarán conectadas. Más aún se habla hoy de BAN (Body Area Network), en donde hay una red de sensores dentro del cuerpo de una persona. Así, por ejemplo, un paciente puede medir su nivel de glucosa, ritmo cardíaco, temperatura y enviar los datos a un servidor, o alertar en una red por una situación de emergencia médica.

1.3 Objetivos

En este trabajo se pretende estudiar el protocolo ZigBee que es la ampliación más difundida del IEEE 802.15.4 y que es una alianza de las más grandes empresas creadoras de hardware y software. Se define su arquitectura alcances y limitaciones. Además se analiza la aplicabilidad de ZigBee a equipos alimentados a batería y se compara con otras tecnologías para mostrar que actualmente es la mejor alternativa para redes WPAN en donde el bajo consumo energético, el bajo costo y la simplicidad sean los compromisos de diseño.

1.4 ¿Qué es ZigBee?

ZigBee es un estándar que define un conjunto de protocolos para el armado de redes inalámbricas de corta distancia y baja velocidad de datos. Opera en las bandas de 868 MHz, 915 MHz y 2.4 GHz y puede transferir datos hasta 250Kbps.

Este estándar fue desarrollado por la Alianza ZigBee [1], que tiene a cientos de compañías desde fabricantes de semiconductores y desarrolladores de software a constructores de equipos OEMs e instaladores. Esta organización sin fines de lucro nace en el año 2002. Desarrolla un protocolo que adopta al estándar IEEE 802.15.4 para sus 2 primeras capas [2], es decir la capa física (PHY) y la subcapa de acceso al medio (MAC) y agrega la capa de red y de aplicación.

La idea de usar una conexión inalámbrica para controlar sensores y adquirir datos tiene muchos años. Existen numerosas soluciones propietarias usadas en domótica pero el gran inconveniente que tienen es la incompatibilidad entre sensores, controles y equipos de procesamiento de datos que obliga a hacer pasarelas (gateways) para interconectar dispositivos de diferentes marcas [3]

El estándar ZigBee fue diseñado con las siguientes especificaciones:

- Ultra bajo consumo que permita usar equipos a batería
- Bajo costo de dispositivos y de instalación y mantenimiento de ellos.
- Alcance corto (típico menor a 50 metros).
- Optimizado para ciclo efectivo de transmisión menor a 0.1 %
- Velocidad de transmisión menor que 250 kbps. Típica: menor que 20 kbps

Existen muchos estándares que se pueden usar en redes de corto alcance tales como el 802.11 y Bluetooth. Cada uno de estos está desarrollado para una clase de aplicación determinada. ZigBee es el estándar más aceptado hoy para usar en redes de sensores y actuadores que deban operar a batería.

1.5 Clasificación de redes

En la Figura 1 se observa un conjunto de estándares de redes inalámbricas clasificados según los ejes: velocidad de datos y alcance o cobertura.

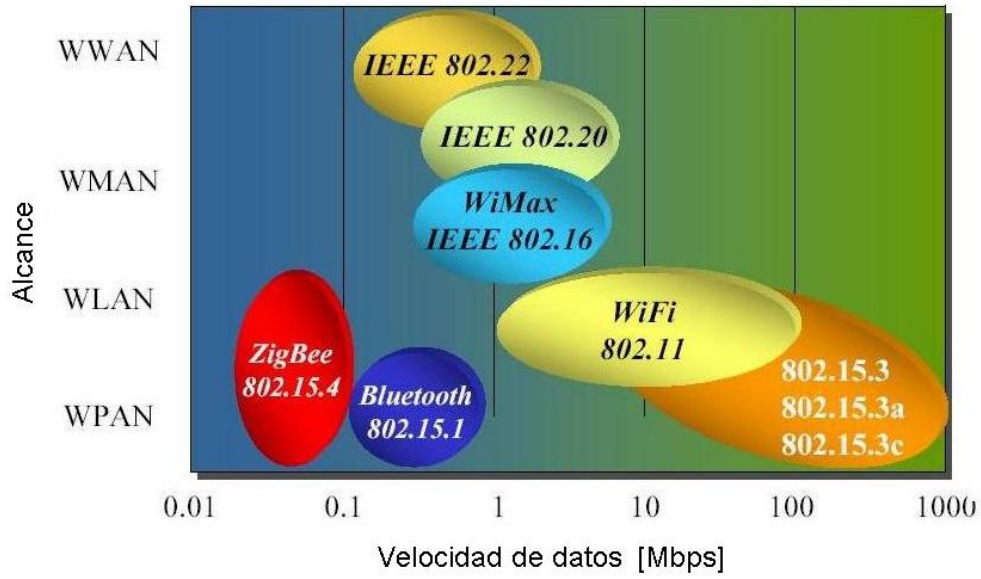

Figura 1: Clasificación de redes inalámbricas

De acuerdo a su cobertura las redes inalámbricas se clasifican en

- WPAN: Redes inalámbricas de área personal
- WLAN: Redes inalámbricas de área local
- WMAN: Redes inalámbricas de área metropolitana
- WWAN: Redes inalámbricas de área geográfica

La finalidad de una interfase que opera bajo IEEE 802.11 es brindar conexión a Internet inalámbrica. Una vez que un dispositivo WLAN se une a la red, se lo trata como a cualquier dispositivo cableado.

Las redes WPAN, no están pensadas para sustituir a un equipo cableado, más bien para proveer una comunicación en el espacio operativo personal (POS: Personal Operating Space) sin necesidad de infraestructura. El POS, es la región esférica de 10 m de radio que rodea al dispositivo [2]. A las redes WPAN se las divide a su vez en redes de alta, media y baja velocidad. IEEE802.15.3 es un ejemplo de red de alta velocidad que puede ser usada por ejemplo para transmitir video desde una cámara a un TV cercano. Bluetooth es un ejemplo de estándar de media velocidad. Puede ser usado para transmisión de música de alta calidad desde un equipo de audio a auriculares inalámbricos. También se emplea para conectar teclados, ratones y otros periféricos a computadoras. ZigBee, con una velocidad de datos máxima de 250 kbps, es considerada una red personal inalámbrica de baja velocidad.

2 Aplicaciones de ZigBee

2.1 Automatización en el hogar

Es una de las aplicaciones más usadas de ZigBee ya que es muy fácil la instalación de dispositivos y la modificación de posición de los mismos. Los usos típicos son:

2.1.1 Seguridad

Sensores de movimiento, de rotura de cristales, apertura de puertas y ventanas. A pesar de su baja velocidad también se usa para transmitir imágenes de cámara de seguridad de baja calidad.

2.1.2 Lectura de instrumentos de servicios

Los medidores de consumo de agua, gas y energía eléctrica deben leerse en forma regular a efecto de facturar los servicios. Es posible crear una red tipo malla para que la información de los medidores llegue directamente a la empresa de servicio. También los medidores ZigBee podrían comunicarse con los artefactos dentro de la casa. Por ejemplo ante un pico de consumo eléctrico se podría desconectar algún equipo de alto consumo. ZigBee ayuda a la creación de medidores inteligentes; en algunos países el valor de los servicios se factura en función de la hora en que se produce. En una hora pico se factura la energía a un precio más alto.

2.1.3 Sistema de riego automático

El uso de un medidor de humedad de suelo permite mejorar la eficiencia del consumo de agua. Se puede distribuir una red de sensores de humedad en un parque de modo que solo se riegue las zonas secas y controlar el tiempo de regado. Una red inalámbrica de sensores facilita enormemente la instalación y el mantenimiento.

2.1.4 Control de iluminación

Para poder controlar el encendido de una lámpara se necesita un cableado a una llave interruptora en una caja de una pared. ZigBee simplifica la instalación de nuevas lámparas ó controles en lugares donde no está la cañería para pasar un cable. En la Figura 2 se muestra la conexión de lámparas usando ZigBee.

Si bien el costo de la conexión inalámbrica es más elevado que el convencional cableado, brinda otras ventajas además de la facilidad de instalación. Es posible conectar un controlador inteligente que encienda/apague luces de acuerdo a una programación, la detección de presencia de personas ó algún otro criterio.

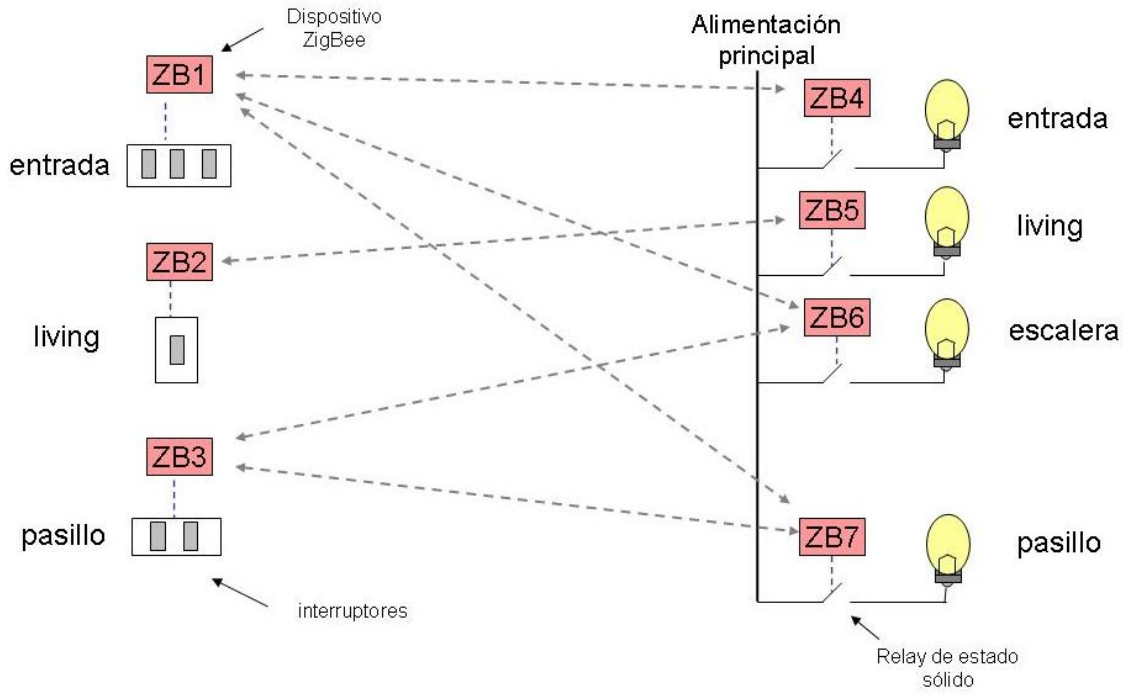

Figura 2: Control de luces en una casa usando ZigBee

2.1.5 Control de temperatura multizona

Los termostatos ZigBee se usan para controlar la temperatura de una casa. En los sistemas de aire acondicionado es posible controlar las rejillas deflectoras amortiguadora de aire de modo de tener control de temperatura separado para cada habitación.

2.1.6 Controles remotos

Tradicionalmente los controles remotos de TV, DVD y equipos de audio usan tecnología óptica infrarroja cuya limitación más importante es que solo funciona a muy poca distancia y sin obstáculos. No puede, por ejemplo, penetrar una pared. Además la comunicación es unidireccional. Como ZigBee usa radiofrecuencia, desaparecen estas limitaciones. Por ejemplo, alguien puede desde otra habitación manejar el equipo de audio y recibir en un display del control remoto, datos de la canción que está escuchando.

2.2 Automatización industrial

Para identificar piezas es necesario agregar alguna marca que dé alguna información. Actualmente se usan etiquetas de códigos de barra e identificadores de radiofrecuencia de tipo pasivo (passive RFID: Radio Frequency Identification). Estas, son marcas (tags) formadas por un circuito integrado de memoria que cuando se acercan a un campo electromagnético de determinada frecuencia, se pueden leer y grabar. El inconveniente mayor es que solo trabajan a pocos centímetros del lector. Usando ZigBee es posible construir marcas activas (active RFID) que se lean a mayor distancia y además usarse para brindar información indirecta sobre su localización usando tres o más nodos ZigBee de ubicación conocida [5].

2.3 Otros usos

En hospitales: para el control de pacientes, y medidores y alarma en terapia intensiva. En hoteles: para controlar el acceso a las habitaciones. En monitoreo ambiental: en aplicaciones de redes de sensores como temperatura, humedad, presión, redes de protección de incendio, etc. [6]

3 Características generales de 802.15.4

Entre las características más importantes se pueden mencionar:

- Puede trabajar tanto en las bandas de 2.4GHz como en la de 868/915MHz.
- Tasa de transmisión de hasta 250 kbps en 2.4 GHz, 40kbps en 915MHz y 20 kbps en 868 MHz.
- Optimizado para aplicaciones con ciclo efectivo menor a 0.1 %.
- Usa CSMA-CA (Carrier Sense Multiple Access Collision Avoidance) para acceso al canal.
- Produce alto rendimiento y baja latencia para dispositivos de bajo ciclo de trabajo, muy adecuado esto para sensores y controles.
- Baja potencia. Ideal para equipos a batería.
- 64 bits de direccionamiento determina una cantidad máxima de1.8.10 ^19 dispositivos.
- 16 bits para identificar redes que determina un total de 65536 redes.
- Permite el uso de ranuras de tiempo (time slots) para posibilitar aplicaciones de baja latencia.
- Protocolo con handshake (diálogo) para mejorar la seguridad en las transferencias.
- Rango: hasta 50 m (valor típico, depende del ambiente).

3.1 Tipos de tráfico

Las aplicaciones usadas en ZigBee tienen un tráfico que puede clasificarse en uno de los siguientes tipos:

a) **Datos periódicos (continuo):** La aplicación define una tasa de datos. Es un caso típico de sensores en donde por ejemplo un sensor necesita transmitir la temperatura cada 10 segundos.
b) **Datos intermitentes (por eventos):** En este caso la aplicación junto a otros estímulos externos al dispositivo definen la tasa de datos. Por ejemplo en un sistema domótico, los interruptores de luces transmiten solo ante un cambio de posición. Mientras tanto están desconectados (comúnmente denominado en modo dormir) y consumiendo una energía de batería mínima.
c) **Datos periódicos con comunicación garantizada (GTS) (**Guaranteed time slot): Hay aplicaciones de baja latencia que requieren comunicación libre de competencia por el canal. GTS es un método de calidad de servicio que garantiza la atención por un cierto Δt dentro de un período T llamado Supertrama. IEEE 802.15.4 provee un modo de trabajo denominado “con baliza” que sirve como multiplexación temporal. Se describirá con más profundidad en 4.3.1

3.2 Tipos de dispositivos

El estándar 802.15.4 define 2 tipos de dispositivos con el objeto de minimizar el costo del sistema:

a) **FFD (**Full Function Device**):** son dispositivos capaces de funcionar en cualquier topología, pueden ser coordinadores ó coordinadores de red. Este tipo de dispositivo puede dialogar con cualquier otro.

b) RFD (Reduced Function Device)**:** Pueden solamente ser miembros de una red con topología estrella. Solo pueden conversar con el coordinador de red. Son dispositivos de baja complejidad con bajo requerimiento de procesamiento y memoria.

En la Figura 3 se muestran distintas topologías de red.

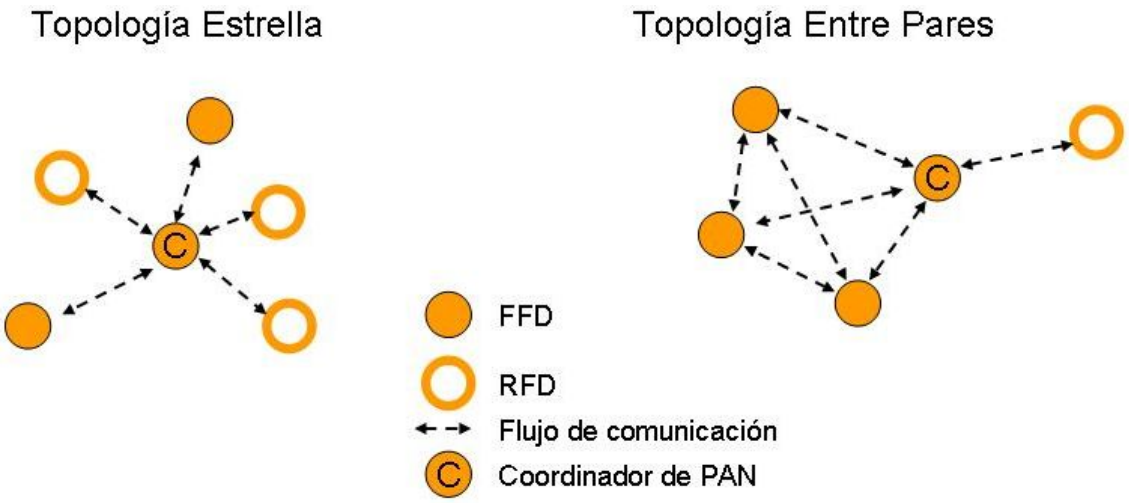

Figura 3: Topologías en IEEE 802.15.4

ZigBee requiere para sus redes que haya al menos 1 dispositivo de función completa (FFD) para que actúe como coordinador de red pero los nodos finales de la estrella pueden ser de función reducida para poder reducir costos.

3. 3 Modos de direccionamiento

Todos los dispositivos tienen direcciones de 64 bits. Se pueden usar direcciones de 16 bits para poder reducir el tamaño del paquete.

4 Las capas del protocolo ZigBee

4.1 Relación con el modelo ISO/OSI

En la Figura 4 se muestran las capas del protocolo ZigBee. Estas se basan en el modelo de referencia ISO para interconexión de sistemas abiertos OSI. Este modelo cuenta con 7 capas pero ZigBee usa solo 4 capas con el objeto de simplificar la arquitectura para el armado de una red de baja tasa de transmisión, simple y de bajo consumo. Las 2 capas inferiores, o sea la capa física (PHY) y la capa de acceso al medio (MAC) son las definidas por el Standard IEEE 802.15.4. Las capas de red (NWK) y de aplicación (APL) se definen en ZigBee. Cada capa se conecta con las capas adyacentes por medio de un SAP (Service Access Point). Un SAP es un lugar por donde una capa superior requiere un servicio a una capa inferior.

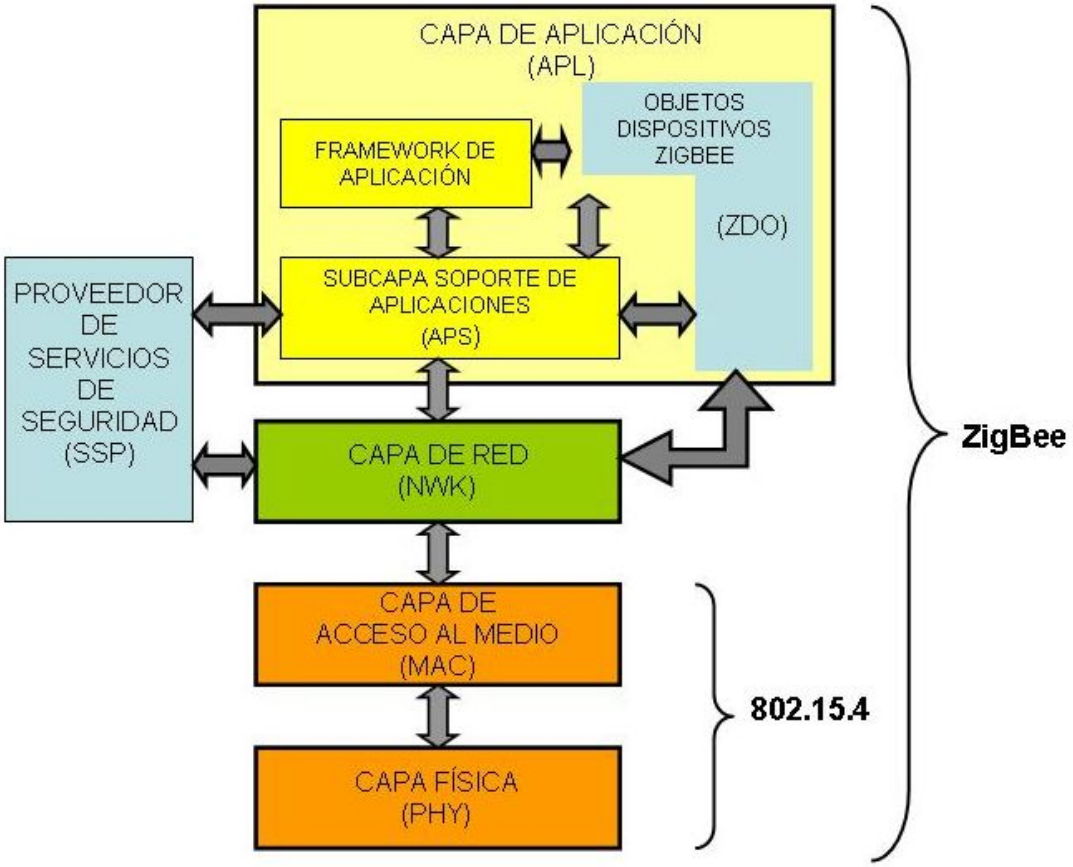

Figura 4: Capas de 802.15.4 y ZigBee

4. 2 La capa Física

Corresponde a IEEE 802.15.4. Además de definir las funciones y la relación con la capa MAC, define aspectos como la potencia del transmisor y la sensibilidad del receptor.

4.2.1 Canales:

En la primera versión de 802.15.4 se definían canales y cada uno de ellos representaba una frecuencia. Aparecía un límite de 27 canales con 1 en la banda de 868MHz, 10 en

la banda de 915MHz y 16 en la banda de 2.4GHz. En la versión IEEE 802.15.4 de 2006 se introduce el concepto de página para permitir la incorporación de nuevas formas de tecnologías a la capa física. En la Tabla 1 se muestra la asignación de canales.

Tabla 1: Asignación de canales

Nº de página	**Nº de Canal**	**Descripción**
0	0	868 MHz. (BPSK)
	1-10	915 MHz (BPSK)
	11-26	2.4 GHz (O-QPSK)
1	0	868 MHz (ASK)
	1-10	915 MHz (ASK)
	11-26	Reservado
2	0	868 MHz (O-QPSK)
	1-10	915 MHz (O-QPSK)
	11-26	Reservado
3-31	Reservado	Reservado

4.2.1.1 Numeración de canales

Cada canal se identifica con un número de canal. En todas las páginas el canal 0 se asigna a la banda de 868 Mhz con frecuencia central en 868.3 Mhz. La frecuencia central en cada canal de la banda de 915Mhz se calcula [2]:

FREC. central [Mhz]= 906 + 2 * (Nº canal -1)
Con $1 \leq$ Nº canal ≤ 10

Para la banda de 2.4 GHz la frecuencia central se calcula:

Frecuencia central [MHz]= 2405 + 5 * (Nº canal -1)
Con $11 \leq$ Nº canal ≤ 26

4.2.2 Detección de la energía

Antes de transmitir en un canal, el dispositivo debe medir el nivel de energía en ese canal. Para eso en modo recepción hace el valor medio de los valores medidos en un intervalo correspondiente a la duración de 8 símbolos. Esta medición solo indica si el canal está ocupado pero no se puede saber si esa energía corresponde a otro dispositivo 802.15.4 ó no.

La sensibilidad del receptor se define como la energía mínima necesaria de la señal entrante que permita ser detectada y demodulada con un error en los paquetes menor al 1 %. El estándar 802.15.4 admite una diferencia de 10dB entre la sensibilidad del receptor y el nivel mínimo de energía detectable. Por ejemplo si la sensibilidad del receptor es de -70dBm debe poder medir energías de -60dBm . El rango de medición que exige el protocolo es de 40 dB lo que en este ejemplo determinaría un intervalo de medición de energía de
-60dBm a -20 dBm.

La capa física provee el servicio de detección de energía en un canal dado y lo envía a la MAC por medio de un entero de 8 bits.

4.2.3 Sensado de Portadora (CS) (Carrier Sense)

A diferencia de la anterior el CS consiste en demodular la señal recibida para determinar si esta es compatible con el estándar. El canal se lo considera ocupado solo cuando hay una señal compatible 802.15.4.

4.2.4 Indicador de calidad del enlace (LQI) (Link Quality Indicator)

Esta es una indicación de la calidad de los paquetes recibidos por el receptor. Puede usarse la intensidad de señal de recepción ó la relación señal ruido. Cuanta más alta sea última se considera que habrá más garantía de que el mensaje llegue a destino. El LQI puede ser usado en una red ZigBee como mecanismo de ruteo en una malla. Así se elegirían las rutas de LQI más alto. Pero hay que destacar que hay otros factores a tener en cuenta en el ruteo. Uno muy importante es el gasto de energía de las baterías. Los nodos que intervengan más frecuentemente en el paso de mensajes agotarán sus baterías antes.

4.2.5 Evaluación de canal libre (CCA) (Clear Channel Assessment)

El mecanismo CSMA-CA hace que la MAC le pida a la capa Física que haga una evaluación del canal para ver que esté libre. El CCA es parte del área de manejo de la capa física. En 802.15.4 existen 3 modos de operación del CCA
Modo 1: Se usa el nivel de energía y un umbral a partir del cual el canal está ocupado.
Modo 2: Se usa el nivel CS para determinar la ocupación del canal.
Modo 3: Combinación AND u OR de los 2 modos anteriores.
AND: La energía pasa de un umbral Y la señal cumple con el estándar
OR: La energía supera a un umbral O es censada una señal que cumple con el estándar.

4.2.6 Concepto de cliente – servidor entre capas

IEEE 802.15.4 y ZigBee usan el nombre de “primitivas” para describir los servicios que una capa le provee a la capa siguiente superior. Las capas PHY, MAC y NWK tienen funciones diferentes pero las formas de requerir servicios son similares. La capa superior usa un servicio de puntos de acceso (SAP: Service Access Point) para requerir servicios. La capa inferior da la confirmación de la transmisión exitosa a la capa superior. En la Figura 5 se muestra la comunicación entre la capa que solicita y la que brinda el servicio. Las etapas son: Pedido, Confirmación, Respuesta e Indicación.

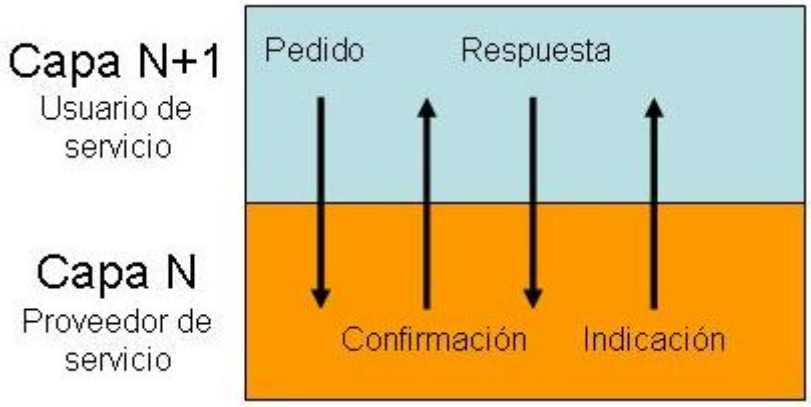

Figura 5: Comunicación entre capas

La Indicación se genera en la capa N y va al solicitante del servicio, para señalizar un evento que es importante para la capa N+1. Por ejemplo cuando la capa física recibe datos de otro dispositivo que deben ser pasados a la MAC la capa usa la primitiva *PD-Data.indication* para informarle a la MAC.

La primitiva Confirmación es usada por la capa N para indicar a la capa N+1 que se ha completado el servicio solicitado. El formato de todas las primitivas de 802.15.4 y ZigBee es

<primitiva>. request
<primitiva>. confirm
<primitiva>. response
<primitiva>. indication

<primitiva> es nombre y comienza con 3 letras indicando de qué capa es
Ej: *phyCurrentChannel.indication*
Phy indica que es una primitiva de la capa física. *CurrentChannel* es el nombre usado para indicar el canal de operación. Es una primitiva del tipo indication

4.2.7 Interfase entre capa Física y MAC

La Figura 6 muestra las 2 capas con 2 bloques SAP: Un SAP de datos (PD-SAP) y un SAP administrativo (PLME-SAP) que comunica a la administración de la capa física (PLME) con la administración de la capa MAC (MLME). Los datos recibidos en el receptor pasan a la MAC a través del PD-SAP.

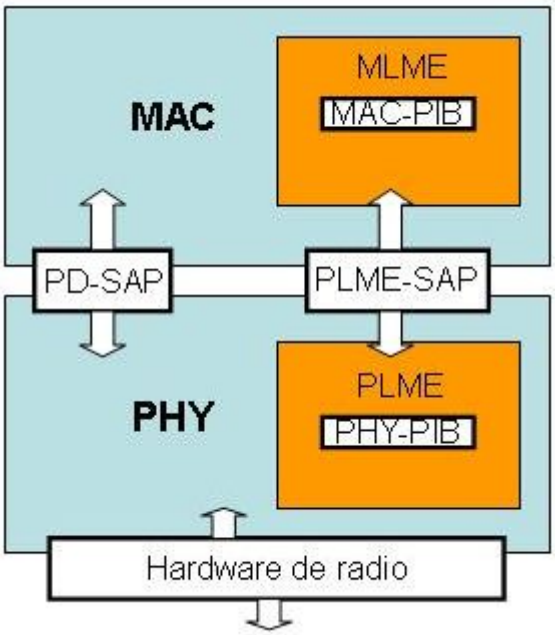

Figura 6: Interfase de servicio de datos y de manejo entre capas Física y Control de Acceso al medio

En la Figura 7 se ve el camino de comunicación entre la capa de aplicación de un dispositivo con la de otro. PDU (Protocol Data Unit) es la unidad de datos de cada capa. Al nombre se le antepone una letra que indica la capa a la que pertenece.

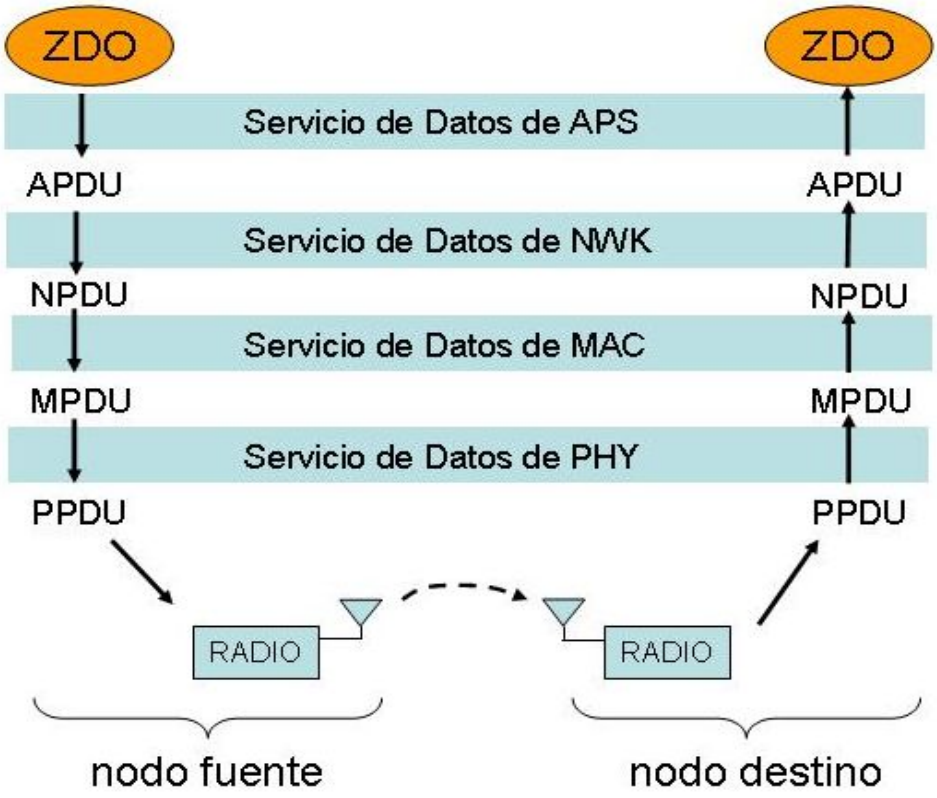

Figura 7: Comunicación de datos entre dos aplicaciones ZigBee pasando entre capas

4.2.8 Área Datos de la capa Física (PPDU: Physical PDU)

Para el caso de la transmisión de datos a otro dispositivo, estos provienen desde el área datos de la capa MAC (MPDU: MAC PDU). La MAC local genera el pedido de servicio, la capa física intenta satisfacerlo y responde indicando el resultado (transmisión exitosa ó falla). Las posibles causas de transmisión infructuosa son:

a) El transceptor estaba deshabilitado
b) El transceptor estaba en modo receptor. (La comunicación siempre es semi-duplex)
c) El transmisor estaba ocupado con otra transmisión previa.

Para el caso de la recepción, la unidad de datos de la capa física envía un aviso de la llegada de datos a la capa MAC. Además envía datos relacionados con la calidad del enlace (LQI)

4.3 La capa MAC de 802.15.4

La capa MAC provee una interfase entre la capa física y la próxima capa sobre la de MAC que en el caso de ZigBee es la de red. Como se dijo antes, el protocolo IEEE802.15.4 se compone de las especificaciones para PHY y MAC y por lo tanto la capa que sigue puede ser cualquiera de acuerdo al protocolo usado. En este trabajo se estudian los servicios de MAC en relación a la capa de red de ZigBee.

En la Figura 8 se ve el modelo de referencia con la subcapa MAC entre PHY y NWK. Aparece al igual que en otras capas 2 partes: una entidad de manejo de la capa MAC (MLME) que es la encargada de manejar los servicios y una unidad de datos. La MLME interactúa con sus vecinas NLME y PLME por medio de las SAP. La MAC tiene su propia base de datos llamada MAC-PIB. Todas las constantes y atributos están definidos en el estándar IEEE 802.15.4

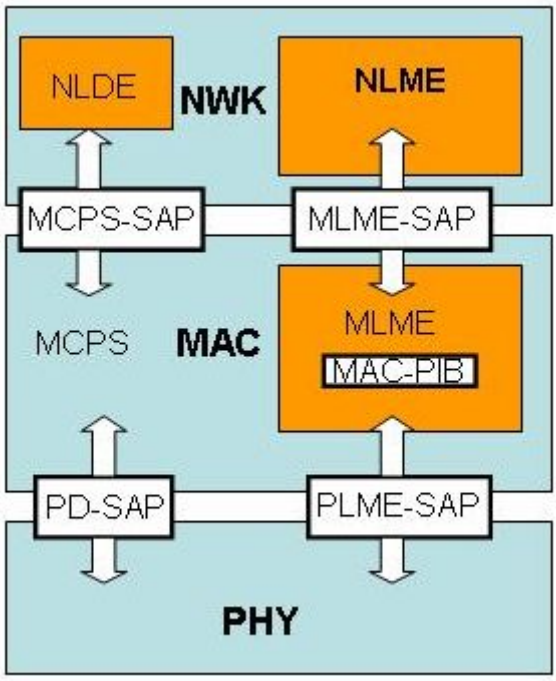

Figura 8: La interfase de la capa MAC con sus vecinas

4.3.1 Operación de la PAN usando balizas

El uso de balizas en la red permite disponer de ranuras de tiempo garantizadas (GTS). Para eso se crean tramas especiales MAC llamada tramas de baliza. Cuando se trabaja con baliza es posible usar una estructura especial llamada supertrama. En la Figura 9 se observan los tiempos de la supertrama. Las supertramas, que son opcionales en IEEE 802.15.4, están separadas por tramas de baliza.

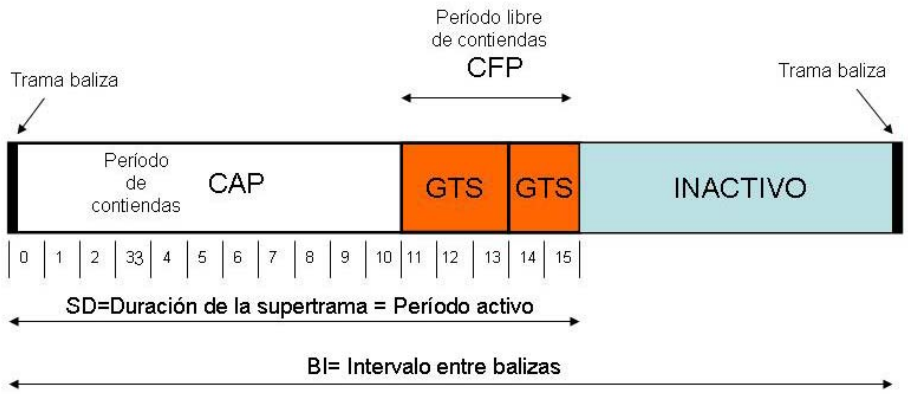

Figura 9: Estructura de una Supertrama

Una supertrama tiene tres tipos de períodos: Período de acceso en contienda (CAP), período libre de contiendas (CFP) y período inactivo. Los nodos que quieran transmitir durante el período CAP deben usar CSMA-CA para acceder a un canal que está disponible igualmente para todos los dispositivos. El primero que lo encuentre libre lo usará y lo tendrá disponible hasta que cese su transmisión. Si el dispositivo encuentra el canal ocupado, iniciará un período de espera aleatorio (back off) e intentará nuevamente usarlo. Las tramas MAC de comando se deben transmitir durante el CAP. No hay garantías dentro del CAP de que el dispositivo pueda usar el canal en el momento en que lo necesita ya que está en competencia con otros dispositivos.

En el período CFP, un dispositivo puede tener garantizada una ranura de tiempo (time slot), con lo que no necesita competir usando CSMA-CA. Esto es muy importante para aplicaciones de baja latencia. La suma de los períodos CAP y CFP constituye el período activo. Este se divide en 16 ranuras de idéntico tiempo. La baliza está en la primera ranura. Puede haber hasta 7 GTS en el CFP. Cada GTS puede durar una o más ranuras de tiempo.

La supertrama puede contener un período de inactividad. En éste, los dispositivos pueden apagar los transceptores de radio para conservar la energía. Es lo que se conoce como nodo en modo “dormir”. El coordinador es quien define los períodos de la supertrama dando valores a las constantes que determinan el intervalo entre balizas (BI) y la duración de la supertrama (SD).

4.3.2 Espaciado entre tramas

El espacio entre tramas consiste en una espera que hace el transmisor entre tramas para que el receptor tenga tiempo de procesarlas. Se lo conoce como IFS (Interframe spacing). De acuerdo al largo del MPDU se realiza un IFS corto (SIFS: Short IFS) o

largo (LIFS: Long IFS). Y existen dos formas de comunicación entre emisor y receptor del mensaje, esto es comunicación con confirmación (ACK: Acknowledge) o sin ella. En la Figura 10 se ve que en el caso de usar ACK el IFS comienza luego de la recepción del ACK.

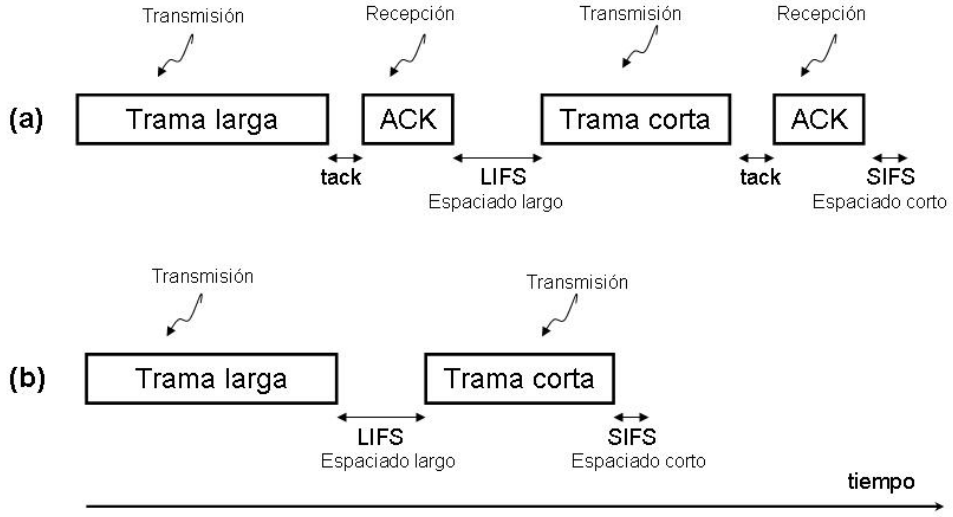

Figura 10: Espaciado entre tramas: (a) trabajo con ACK, (b) trabajo sin ACK

4.3.3 CSMA-CA

Cuando un dispositivo desea transmitir, previamente verifica que el canal no esté en uso por otro dispositivo. Si está libre comienza a transmitir. Hay transmisiones que se hacen sin verificación previa. Estas son

- Transmisión de balizas
- Transmisión durante el período CFP
- Transmisión después de haber dado ACK a un comando de pedido de datos.

El uso del CSMA-CA tiene en cuenta si se está trabajando con supertrama o no. Si es el primer caso, el tiempo activo se divide en 16 ranuras iguales, entonces el tiempo de back off debe ser alineado para que caiga en el CAP. Este caso se llama CSMA-CA ranurado. Cuando no se trabaja con supertrama, no se necesita sincronizar el back off. Este caso se denomina CSMA-CA no ranurado.

4.3.4 Los problemas del nodo oculto y del nodo expuesto.

El algoritmo de CSMA-CA tiene problemas cuando aparece un nodo oculto (Figura 11). Si los nodos A y C están fuera de alcance entre ellos pero existe un nodo B que puede comunicarse tanto con A como con C. Entonces cuando A transmita algo a B, el nodo C no se enterará. Análogamente cuando C transmita a B, A no lo recibirá. Si por alguna razón transmiten A y C en el mismo canal y en el mismo momento, esto creará una colisión de paquetes en B. Una forma de resolver este problema es aumentando la potencia en los nodos A y C de modo que A reciba a C y viceversa.

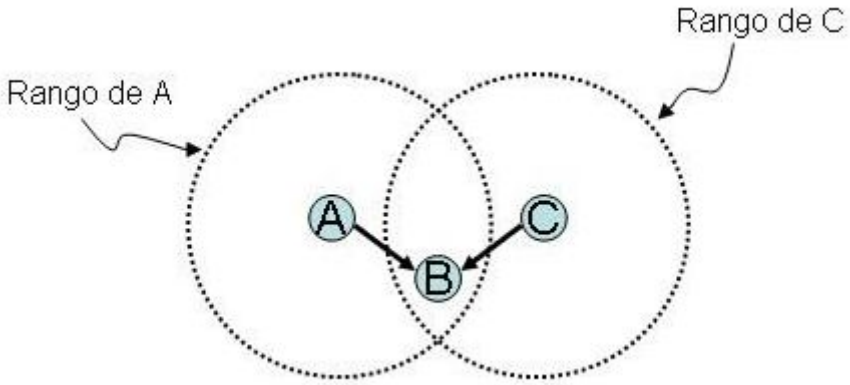

Figura 11: El problema del nodo oculto

En la MAC de 802.15.4 a diferencia de IEEE 802.11, no hay un mecanismo de diálogo (handshake) que soporte RTS/CTS (Request To Send/Clear To Send) así que no hay solución a nivel software de MAC.

El otro problema es el del nodo expuesto. En la figura 12, el nodo E le transmite un mensaje a D mientras que en el mismo momento F le transmite a G. El nodo D está fuera de alcance del nodo F por lo tanto E y F podrían transmitir en simultáneo sin colisiones. Pero el nodo E cuando aplique el algoritmo de CSMA-CA percibirá la transmisión del nodo F, considerará que el canal está ocupado y no transmitirá. A esto se lo denomina el problema del nodo expuesto. En este caso el problema se podría solucionar disminuyendo la potencia a la mínima necesaria para que el receptor reciba correctamente la información, cambiando la ubicación de los nodos, o usando RTS/CTS que como se dijo no está soportado en IEEE802.15.4

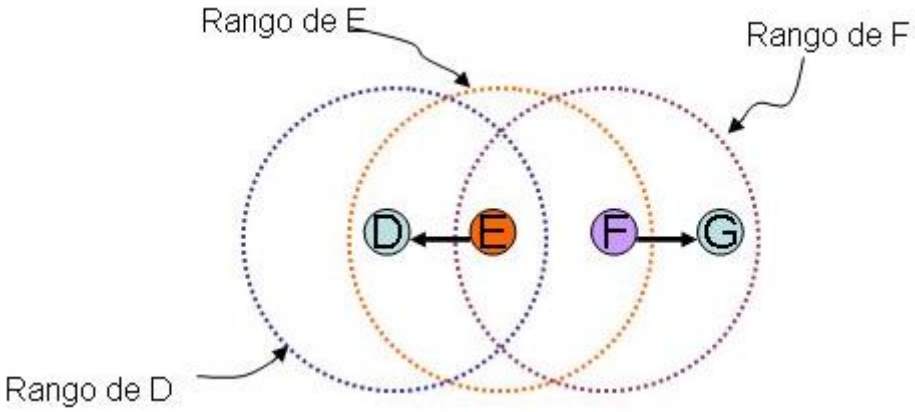

Figura 12: El problema del nodo expuesto

4.3.5 Servicios de MAC

La MAC está dividida en 2 partes principales: el área de datos (MCPS) y el área de manejo (MLME) que equivale a una unidad de control. La primera tiene que ver con la comunicación de la información hacia las capas vecinas de red y física según se trate de una recepción o una transmisión. Es relativamente simple pero debe ser optimizada ya que es la que se accede con más frecuencia. La parte de control (MLME) es la encargada de recibir los comandos desde la capa de red y decodificarlos. Lo mismo para las indicaciones y confirmaciones desde la capa física.

4.3.5.1 Servicios de Asociación y Desasociación

La asociación es el proceso mediante el cual un dispositivo se une a una red. La capa de red (NWK) es la que maneja la formación de la red e instruye a la capa MAC para hacerlo. Se usan 4 primitivas :
MLME-Associate.request
MLME-Associate.indication (opcional para RFD)
MLME-Associate.response (opcional para RFD)
MLME-Associate.confirm

La capa de red hace el pedido al coordinador de red para unirse a su red. En ese pedido le pasa una lista de sus capacidades tal como si es un dispositivo FFD ó RFD. La capa MAC del dispositivo hace el pedido hasta que llega hasta la MAC del coordinador (pasando por la capa física y radio). En la Figura 13 se observan todas las señales pedido, confirmación e indicación que garantizan que las capas de red se comuniquen entre sí por medio del servicio MAC:

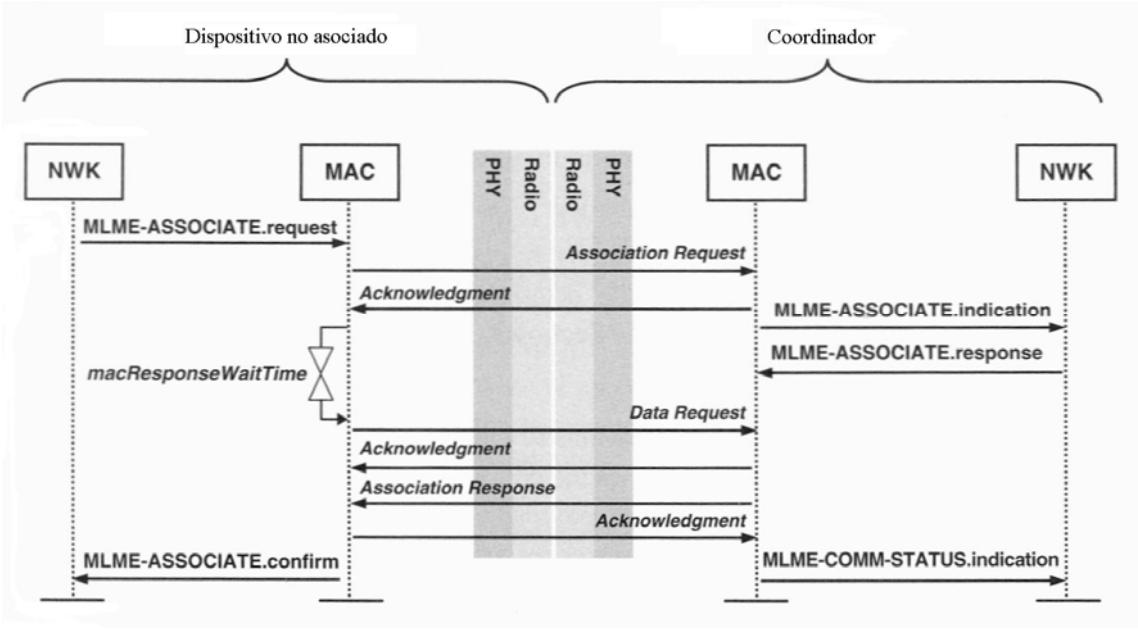

Figura 13: La secuencia de Asociación de un dispositivo a la red

El proceso de desasociación puede ser originado por el dispositivo que quiere irse de la red ó bien por el coordinador que desea expulsar al dispositivo. En la Figura 14 se observa la secuencia para una desasociación iniciada por el dispositivo.

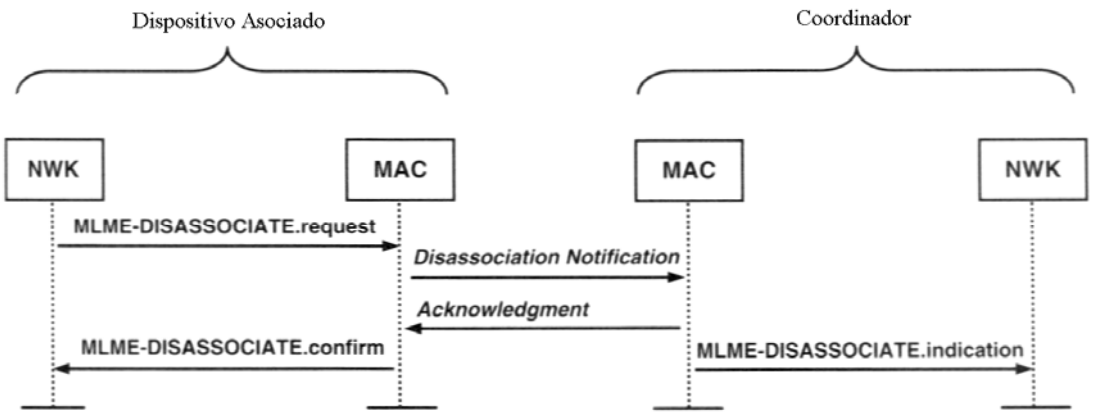

Figura 14 : Desasociación iniciada por un dispositivo

En la figura 15 se observa la secuencia para una desasociación iniciada por el coordinador. En ambos casos, la secuencia termina con la señal de confirmación que le llega al originador del pedido para confirmar la desasociación.

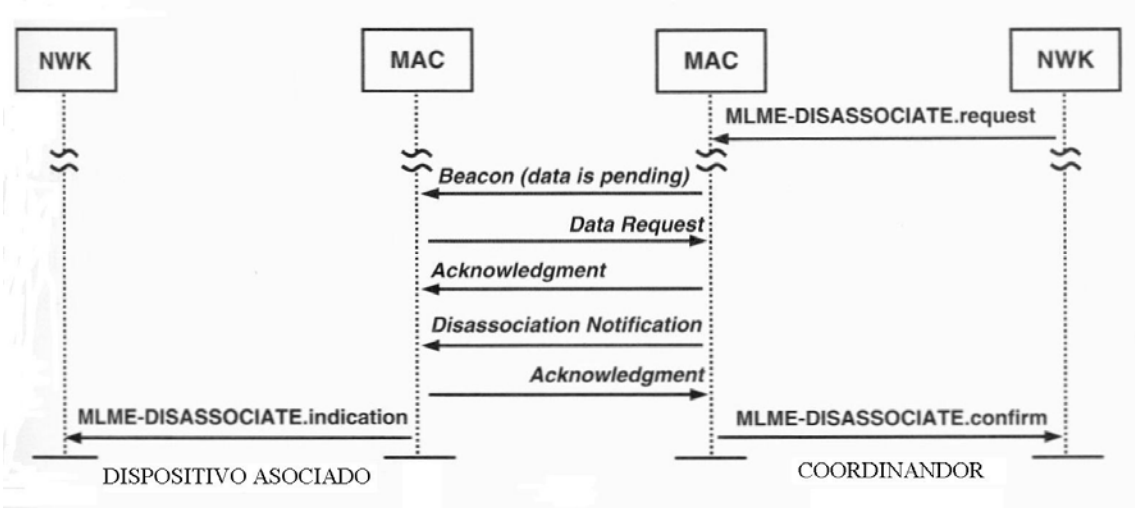

Figura 15: Desasociación iniciada por el coordinador

4.3.5.2 Servicio de Notificación de Baliza

Cuando la capa MAC recibe una señal de baliza, la MLME manda todos los parámetros a la capa NWK indicando el LQI y el tiempo en que se recibió.

4.3.5.3 Servicio de Habilitación, Deshabilitación del receptor

La capa NWK puede pedir que se habilite el receptor durante un cierto intervalo. Es un servicio opcional tanto para FFD como RFD.

4.3.5.4 Servicio para generar GTS cuando se trabaja en modo baliza

Usado para reservar ranuras de tiempo cuando se trabaja en modo baliza.

4.3.5.5 Servicio de Reset

Resetea a la capa MAC llevando los parámetros a los valores por defecto de la PIB.

4.3.5.6 Servicio de Arranque

Arranca a la capa MAC e inicializa el dispositivo. Se la llama normalmente luego del reset.

4.3.5.7 Servicio de Notificación de orfandad

Un dispositivo debe pertenecer a una red para poder establecer una comunicación con otros. Cuando el dispositivo de desengancha de la red sin el proceso de desasociación se lo considera huérfano. Esto puede ocurrir por algún tipo de falla o bien porque se movió y quedó fuera de rango de alcance. Cuando la capa NWK recibe repetidas fallas en la comunicación ó no recibe ACK (parámetros ajustables en la base de datos.), concluye que está huérfana. En ese caso instruye a la MAC a resetearse e intentar una nueva asociación ó bien iniciar un procedimiento de reenganche de dispositivo huérfano. En la Figura 16 se ve como es el procedimiento de reenganche en la red. Consiste en una trama broadcast para encontrar a sus padres. Si el coordinador lo tenía registrado lo reenganchará a la red.

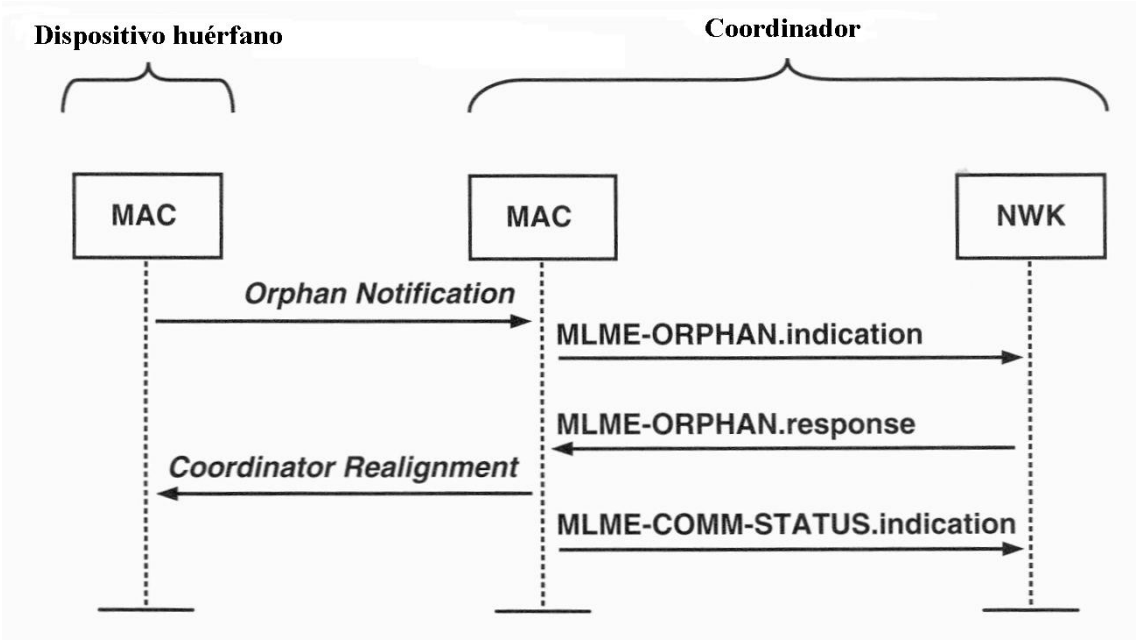

Figura 16: Secuencia de notificación de dispositivo huérfano

4.3.5.8 Servicio de Barrido de Canales

El barrido de canales es un servicio de la MAC para darle información a la NWK sobre la actividad que hay en el POS. Hay 4 tipos de barridos:

- Barrido de energía ED. Con esto determina la energía de cada canal usando para eso el servicio de detección de ED de la capa PHY
- Barrido de nodo huérfano: Cuando el nodo está huérfano trata de encontrar a qué PAN está asociado enviando una notificación en cada canal y esperando que le contesten en alguno.

- Barrido activo: El dispositivo manda una trama de baliza y espera respuesta. Esto lo pueden usar los coordinadores para descubrir los identificadores que se están usando en su área (POS)
- Barrido pasivo: Similar al caso anterior pero no hay una señal previa de baliza.

4.3.5.9 Servicios de Sincronismo y notificación de Pérdida de Sincronismo

Cuando se trabaja con baliza el dispositivo debe sincronizarse al coordinador. Entonces enciende el receptor en determinado momento justo antes del comienzo de la baliza. Si no escucha la baliza en un cierto intervalo entonces la capa NWK le ordenará a la MAC que informe al coordinador de la pérdida de sincronismo.

Servicio de Encuesta (Poll): La capa NWK puede pedir a la MAC que ésta le haga un pedido de datos al coordinador. Esta primitiva se usa como un método indirecto de pedido de datos que puede ser usado tanto en sistemas con balizas como en sistemas sin ellas.

4.3.6 Formato de la trama MAC

Hay 4 tipos de tramas MAC: de baliza, de dato, de confirmación (ack) y de comando. Todas las tramas tienen 3 partes: un encabezado (MHR), una carga útil (payload) y un pie (MFR). El encabezado contiene información sobre el tipo de trama, campos de direcciones y banderas de control. La carga útil tiene un largo variable y contiene comandos o datos ó nada (cero bytes). El MFR contiene una secuencia de chequeo (FCS) para verificar los datos basada en el clásico polinomio cíclico redundante [6] (CRC). Las figuras 17, 18, 19 y 20 muestran los diferentes formatos que puede tener la trama MAC [2].

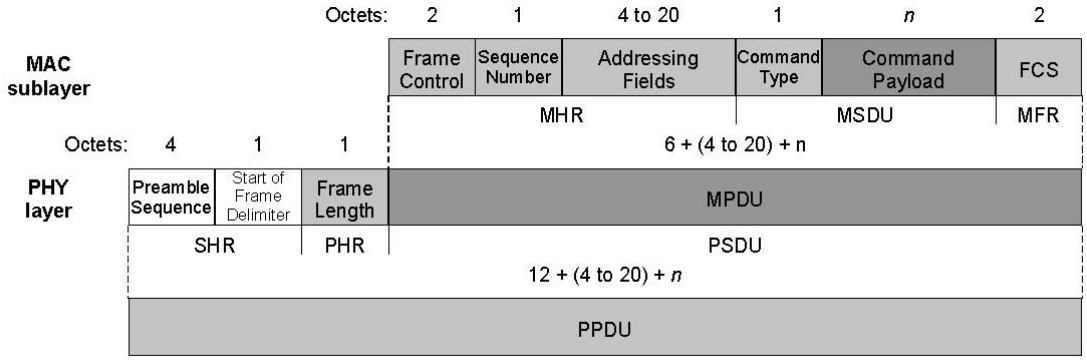

Figura 17: Estándar 802.15.4. Trama de comando

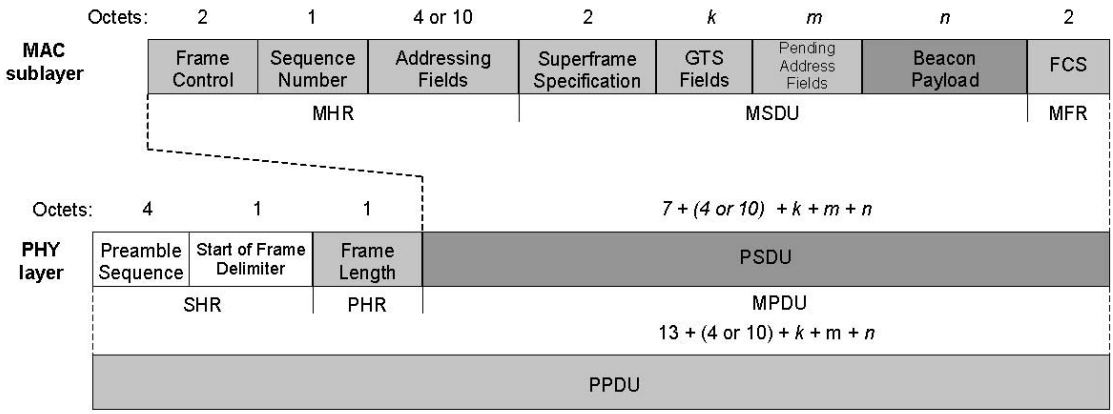

Figura 18: Estándar 80215.4. Trama de baliza

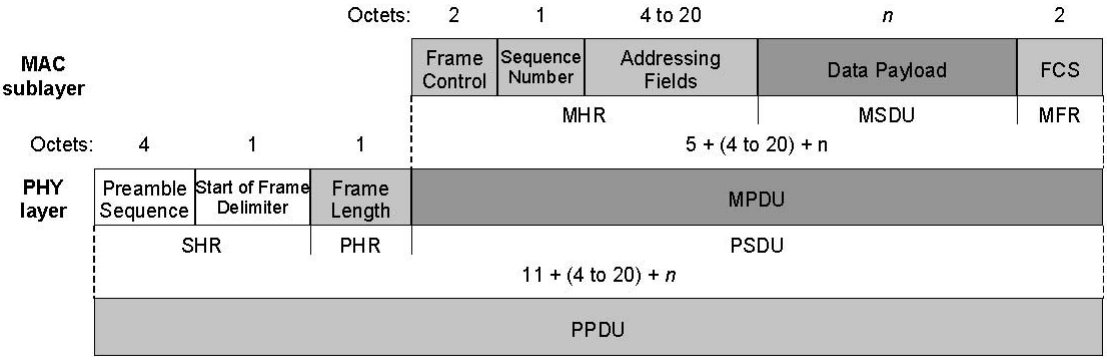

Figura 19: Estándar 802.15.4 . Trama de dato

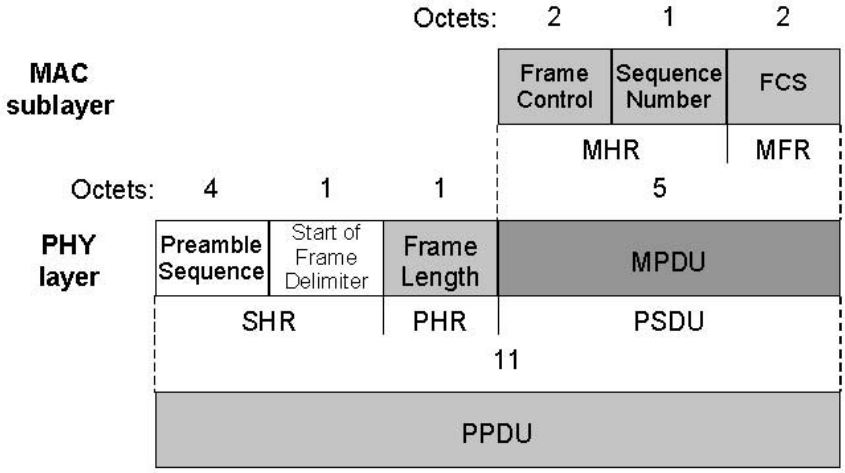

Figura 20: Estándar 802.15.4. Trama de acknowledge.

4.3.7 Resumen de las responsabilidades de la capa MAC

Las responsabilidades de la capa MAC se puede resumir como:

- Puede generar balizas si es coordinador.
- Usa CSMA-CA como método de compartir el canal.

- Provee el manejo, sincronización y GTS cuando se usa balizas.
- Provee un enlace seguro entre las MACs de dos dispositivos.
- Provee servicios de asociación desasociación.
- Provee un mecanismo de seguridad cuyo nivel estará determinado por lo solicitado desde las capas superiores.

4.4 La capa de Red ZigBee

La capa de red provee a Zigbee funciones para el armado y manejo de redes y una interfaz simple para relacionarla con las aplicaciones de los usuarios. Al igual que las otras capas provee 2 tipos de servicios: de datos a través de la NLDE y de control o manejo por medio de la NLME. Cada una de estas entidades se comunica con sus homólogas en las capas MAC y APL por medio de los respectivos puntos de acceso (SAP). La capa de red tiene sus propios atributos y constantes que se guardan en una base de datos (NIB) dentro del NLME. En la Figura 21 se observa la relación de la capa de red con sus vecinas

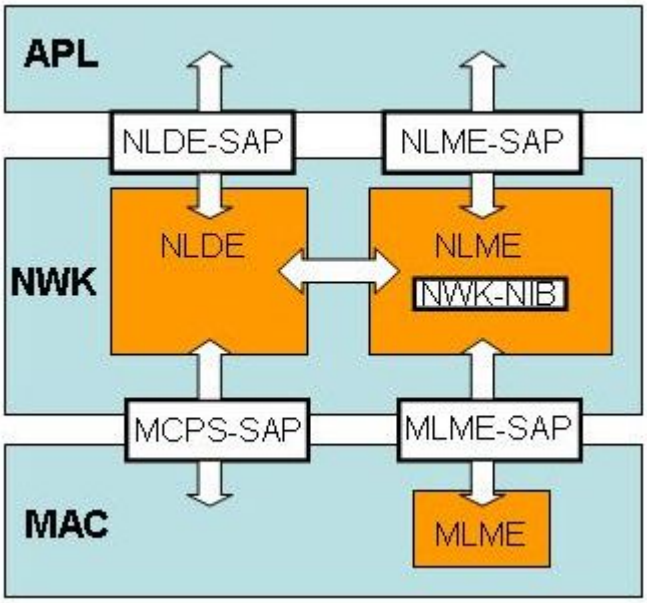

Figura 21: Interfase de la capa de red

La capa de red del coordinador asigna direcciones de 16 bits a cada miembro de la PAN. Esa dirección asignada NTW debe ser idéntica a la dirección corta (16 bits) de la MAC 802.15.4. Cada trama de red lleva un parámetro llamado radio que indica la cantidad de saltos máximos que esta puede llegar a realizar. Este parámetro se va decrementando en uno en cada salto. Cuando llega a cero, esa trama no será retransmitida a otro dispositivo. Existen 3 tipos de comunicación de mensajes: broadcast, multicast y unicast:
Un mensaje tipo broadcast tiene como destino a todo dispositivo que lo pueda recibir.
Un mensje multicast se envía solo a un grupo de dispositivos.
Un mensaje unicast contiene la dirección de un único dispositivo.

4.4.1 Tipos de nodos ZigBee

El estándar especifica 3 tipos de nodos que pueden estar en una red: coordinador, ruteador y dispositivo final.

4.4.1.1 Coordinador

Es obligatoria la presencia de uno y solo un nodo coordinador dentro de la red. Actúa como nodo raíz en la topología árbol y es responsable de:

- Arranque de la red.
- Configuración de los parámetros de red.
- Admisión de nodos a la red.
- Asignación de direcciones de red.

El coordinador requiere de un dispositivo de función completa (FFD) ya que necesita más potencia de cómputo. También es importante que la fuente de alimentación sea permanente y segura ya que este dispositivo nunca entrará en modo "dormir".

4.4.1.2 Ruteador

Es un nodo de tipo FFD pero que no es el coordinador. La utilidad de éstos es para extender la cobertura de la red y para aumentar la confiabilidad con la creación de rutas adicionales de datos.

4.4.1.3 Dispositivo final

Estos nodos se comunican con un nodo ruteador ó un nodo coordinador. Estos nodos tienen menos potencia de cómputo y usualmente son alimentados a batería. Son dispositivos de funcionalidad reducida (RFD) según el estándar IEEE 802.15.4.

4.4.2 Topologías

ZigBee usa las topologías de IEEE 802.15.4 para transferencia de datos y agrega las topologías de árbol y de malla. Debido al poco alcance de cada nodo, frecuentemente un paquete debe ser retransmitido varias veces por intermedio de ruteadores. Lo destacable es que el ruteo en cualquier topología usada se hace en la capa de red y entonces no es necesaria ninguna programación adicional en la capa de aplicación. En la Figura 22 aparecen las topologías estrella, árbol y malla.

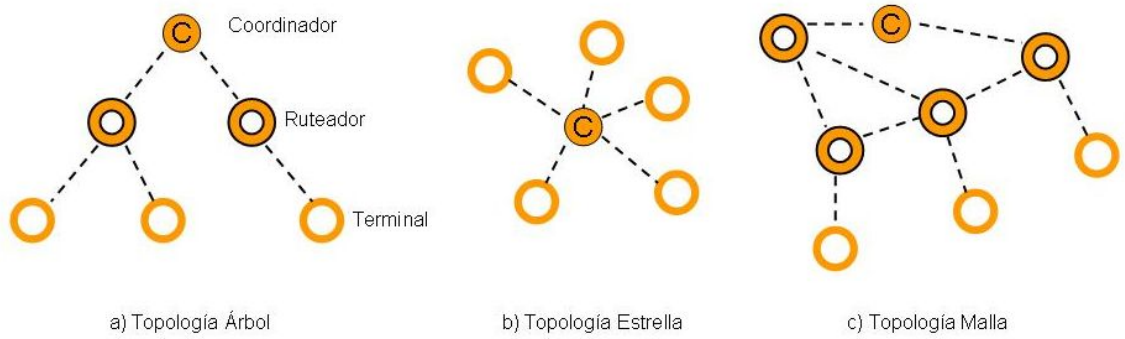

Figura 22: Topologías ZigBee

4.4.2.1 Topología estrella

Es la más sencilla. Corresponde a la topología estrella de la IEEE 802.15.4.

Características:

- Un coordinador con uno ó varios nodos hijos.
- El rango de la red está limitado al rango de transmisión del coordinador.
- La red es fácil de configurar.
- El coordinador es el único nodo que rutea paquetes.

Es un caso especial de la topología árbol. Es un árbol con profundidad máxima 1

4.4.2.2 Topología árbol

4.4.2.2.1 Características

Entre las más importantes se pueden mencionar:

- Los nodos ruteadores pueden tener nodos hijos
- Hay comunicación directa solo a través de la relación padre-hijo
- Ruteo jerárquico con un único camino posible entre 2 nodos

4.4.2.2.2 Relación padre-hijo

Los ruteadores y dispositivos finales se asocian con nodos presentes en la red. El nodo hijo es el que recientemente ha entrado en la red. El nodo padre es el nodo que le ha dado al hijo acceso a la red

4.4.2.2.1 Propiedades de la relación padre-hijo

Las propiedades más importantes son:

- Solo pueden ser padres el nodo coordinador ó los nodos ruteadores.
- En cada momento el nodo hijo tiene solo un padre.
- Un hijo puede cambiar de padre.
- La jerarquía ZigBee puede interpretarse como un árbol en donde el coordinador es la raíz y los nodos finales son las hojas.

Cuando se configura la red se deben indicar los siguientes parámetros

1. Número máximo de hijos directos: Es la máxima cantidad de ramas que puede tener cada nodo.
2. Máxima profundidad de la red: Es la profundidad del árbol
3. Direccionamiento de nodos: Cada nodo que entra a una red recibe una dirección de 16 bits. Esta dirección se usa en comunicaciones a nivel red. ZigBee ofrece una alternativa de asignación por defecto de direcciones a cada elemento que ingresa al árbol. La numeración depende de la configuración de hijos máximos y profundidad máxima con que se ha configurado el árbol.

En la Figura 23 se ve un ejemplo de numeración para un árbol [4]. Lo interesante es que cada ruteador sabe cómo encaminar cada mensaje hacia un destino Z comparando su propia dirección con la del destino. Esto elimina el problema de ruteo.

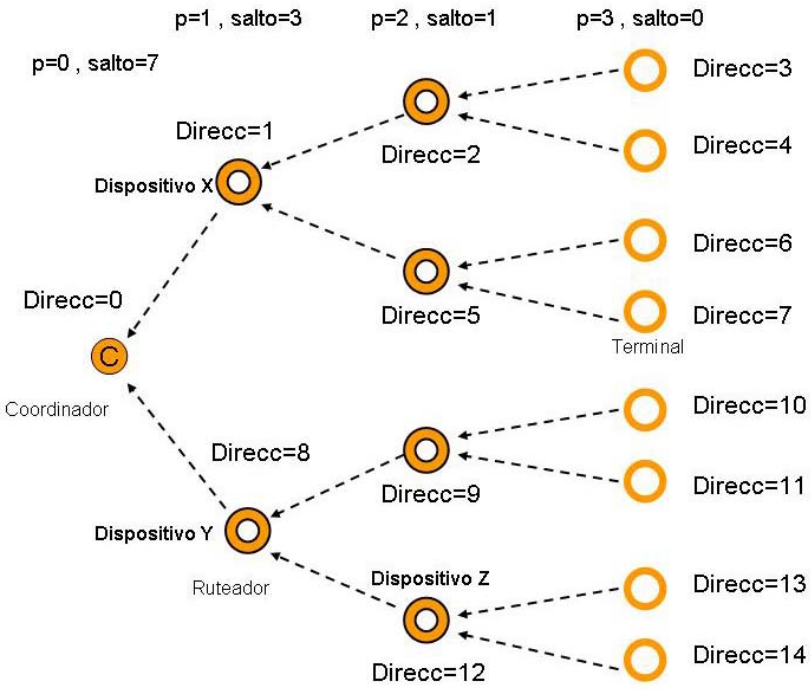

Figura 23: Asignación de direcciones por defecto en topología árbol

En la figura, *p* representa la profundidad en la que se encuentra ubicado el nodo dentro del árbol y salto(d) representa el corrimiento que tendrán entre sí los hijos de un padre. Por ejemplo, en la Figura 23, el dispositivo X tiene dirección 1, por lo tanto el dispositivo Y tendrá dirección
Direc Y = Direc X + salto (0) = 1 + 7 = 8

Los nodos con salto=0 solo pueden ser terminales. Es fácil para un nodo Y determinar para dónde retransmitir un mensaje con una dirección de destino D. Un nodo D es descendiente de Y si se cumple
Y < D < Y + salto(p-1)
En la Figura 23 la dirección del dispositivo Y es 8 y está a profundidad p=1. Si la dirección destino es D=11 entonces
8< 11 < 8+7
Se cumple en este caso que el destino es un descendiente de Y

Si el destino es un hijo la resolución de la transferencia es trivial. Si el destino no es hijo pero sí descendiente entonces:
Dirección del próximo salto = Y + 1 + int [(D- (Y+1))/salto(p)] * salto(p)
En el ejemplo:
Dirección del próximo salto = 8 + 1 + int[(11-(8+1))/3] * 3 =9
El nodo Y retransmitirá el mensaje hacia el nodo 9.

Como se ve, la topología árbol con asignación de direcciones por defecto simplifica enormemente la lógica de los nodos ruteadores ya que no necesitan armar tablas para determinar cómo retransmitir un mensaje.

4.4.2.3 Topología malla

Es una extensión de la topología de comunicación entre pares (peer to peer). Características:

- Los nodos ruteadores pueden tener nodos hijos.
- Hay comunicación directa entre dos nodos FFD siempre que estén separados a una distancia menor al rango de transmisión entre ellos.
- Los nodos terminales solo pueden intercambiar datos con sus respectivos nodos padres.
- Es posible el ruteo dinámico. El mejor paso es una optimización de gasto energético, tiempo, seguridad y confiabilidad.

4.4.2.3.1 Mecanismos de ruteo

En el algoritmo implementado en la capa de red hay un balance entre costo por unidad, gasto de batería, complejidad de implementación para lograr una relación costo desempeño adecuada a la aplicación. Un algoritmo muy utilizado por su simplicidad y bajo requerimiento de procesamiento es el AODV (Ad hoc On-Demand distance Vector) [14]. En AODV los nodos mantienen una tabla de ruteo para los destinos conocidos. En el comienzo esta tabla la integran sus vecinos. Solo se agrandará la tabla cuando aparezca algún nodo con camino desconocido. En este caso se envía mensajes de descubrimiento que se propagan entre los nodos hasta llegar al destino. Desde el destino se inicia el camino inverso hasta llegar al nodo origen. Todos los nodos actualizarán sus tablas.

4.4.3 Resumen de las responsabilidades de la capa de red

Las tareas más importantes de la capa de red serían:

- Establecer una nueva red brindando topologías como árbol ó malla.
- Agregar o quitar a un dispositivo a/de la red.
- Garantizar la comunicación dentro de toda la red más allá del alcance de un único nodo.
- Configurar a un nuevo dispositivo para que pueda operar en la red.
- Asignar direcciones de red a los dispositivos brindando una interfase unificada para todos ellos.
- Sincronizar entre dispositivos usando balizas ó encuestas.
- Proveer seguridad.
- Rutear tramas a sus destinos.

4.5 Capa de aplicación

Consiste en la subcapa APS (Application Support) y la ZDO (ZigBee Device Object). Responsabilidades: mantener las tablas para los enlaces (binding) que consiste en balancear o adaptar dos dispositivos entre ellos basados en los servicios y necesidades. Cada subcapa se puede definir con:

- APS: trata de descubrir también a otros dispositivos que están operando en su mismo espacio operativo.
- ZDO: Define el rol de un dispositivo dentro de la red.

En la capa de aplicación se inician o responden pedidos de enlace y se establece una relación segura entre dispositivos seleccionando un método de seguridad como una clave.

4.5.1 Capa soporte de aplicación (APS)

4.5.1.1 Servicios

Descubrimiento: Determina qué otros dispositivos operan en el espacio del dispositivo.
Enlace: Enlaza dos o más dispositivos basados en sus servicios y necesidades y manda mensajes entre estos.
La capa de aplicación (APL) en ZigBee es la que se encarga de las aplicaciones específicas de los usuarios. El desarrollo de las aplicaciones se ve facilitado por el hecho de que la APL tiene interfases a la capa RED.

4.5.1.2 Perfiles

En la capa aplicación hay perfiles que se diseñaron para unificar el intercambio de datos en esta capa. Un perfil caracteriza tipos de dispositivos, formato de los mensajes y acciones y funciones que se usarán en ciertas aplicaciones. Los perfiles pueden ser:

- Perfiles públicos: los especifican la Alianza ZigBee para proveer algún tipo de interoperabilidad entre dispositivos de distintos fabricantes.
- Perfiles privados: los especifica un fabricante o un usuario para sus aplicaciones específicas que no pueden realizarse con un perfil público.

Un cluster es un mensaje especial definido dentro de un perfil. Cada cluster tiene ciertos atributos que se transmiten dentro del mensaje. Por ejemplo: el control de encendido/ apagado de las luces de una casa y el control de los atenuadores de luz son diferentes clusters dentro del perfil Automatización hogareño (HA).

ZigBee define puntos finales de aplicaciones que son los destinos de las mismas. Estos actúan como puertos de comunicación en la capa aplicación. Por ejemplo un control remoto que encienda /apague luces y que controle la temperatura de un equipo de aire acondicionados maneja 2 aplicaciones diferentes y por esto tiene 2 puntos finales de aplicación. Un nodo en ZigBee puede tener hasta 240 puntos finales de aplicación

El enlace: es un procedimiento en el que se realiza la conexión virtual entre puntos finales de aplicación. Los enlaces pueden ser: (Figura 24):

- Uno a Uno: Ejemplo: un sensor que se conecta a un nodo central.
- Muchos a Uno: Ejemplo: muchos sensores del mismo tipo se conectan a la misma central.
- Uno a muchos: Ejemplo: un interruptor que controla muchas luces.

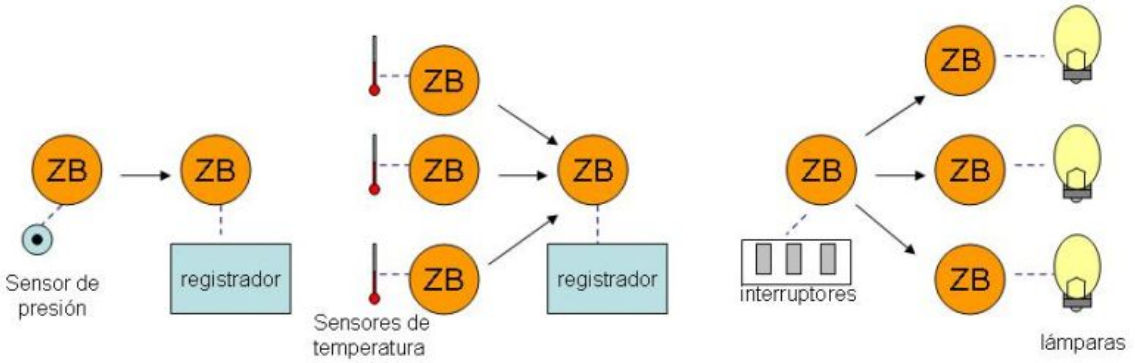

Figura 24: Enlaces uno a uno, varios a uno y uno a varios

4.5.2 Objetos ZigBee (ZDO)

Fueron creados para simplificar el manejo de la red por las aplicaciones de los usuarios. Los objetos ZigBee contienen perfiles de dispositivos ZigBee (ZDP: ZigBee Device Profile) que solo se ocupan del manejo de red y no del intercambio de datos específico de la aplicación. ZDP provee de un conjunto de comandos y respuestas para:

- Realizar una exploración del canal.
- Descubrir dispositivos.
- Manejo de la potencia de transmisión.

4.6 Seguridad

4.6.1 Seguridad en ZigBee

Dadas las características inalámbricas de la red ZigBee, un mensaje puede ser recibido por cualquier dispositivo cercano. Esto puede no ser un inconveniente en algunas aplicaciones pero en otras un intruso podría violar la privacidad de las personas, producir algún daño o inhabilitar algún sistema. Por ejemplo alguien podría deshabilitar una alarma o también podría obtener algún dato privado. ZigBee soporta el uso de protocolos estándar de encriptación y autenticación. El diseñador de la red tiene que hacer un compromiso entre nivel de seguridad, complejidad y costo de los dispositivos ya que el aumento de seguridad requiere más capacidad de cómputo y más memoria y esto también incrementa el gasto energético.

ZigBee utiliza AES (Advance Encryption Standard) del NIST (National Institute of Standards and Technology) como técnica de encriptación [15]. Un punto fundamental es el mecanismo por el cual cada dispositivo obtiene la clave. Hay 3 métodos para obtener la clave:

a) Preinstalación: El fabricante embebe la clave en el dispositivo. Con un conjunto de minillaves tipo piano o jumpers el usuario puede seleccionar luego alguna clave.
b) Transporte de clave: El dispositivo pide a un centro de confianza para que le mande una clave. En este caso hay un momento de vulnerabilidad cuando se envía la clave.
c) Establecimiento de clave sin comunicación: Es un método de generar claves al azar para dos dispositivos sin necesidad de comunicarlos. Este servicio ZigBee se basa en el protocolo SKKE (Symmetric-Key Key Establishment). Los dispositivos destino de la clave ya tienen que tener una clave común llamada clave maestra que pudo haber sido pasada de acuerdo al método a) ó b).

Los detalles del protocolo SKKE se pueden encontrar en la especificación ZigBee [1]. La principal limitación que existe en la implementación de mecanismos de seguridad es la escasez de los recursos. Los nodos en su mayoría son alimentados a batería, tienen poco poder de cómputo y poca memoria. Son dispositivos de bajo costo que no resisten un posible ataque. Un intruso puede simplemente leer la clave directamente de la memoria de un dispositivo. Agregando un poco más de complejidad a los dispositivos se puede lograr una defensa contra la lectura directa de información sensible.

El centro de confianza tiene 2 modos de operación:

- **Modo comercial**: en este modo mantiene una lista de dispositivos, claves maestras, claves de enlaces y claves de red. El espacio de memoria requerido aumenta con la cantidad de dispositivos en la red.
- **Modo residencial**: La única clave que es obligatorio mantener en el centro de confianza es la clave de red. No se hace ningún control para verificar si algún intruso modificó el contador de tramas.

En la red ZigBee cada capa del protocolo (APS, NWK y MAC) es responsable de la seguridad de las tramas iniciadas en esa capa. Por simplicidad se usa una misma clave para todas las capas.

4.6.2 Autenticación

ZigBee soporta autenticación de dispositivos y de datos. El propósito de la autenticación de datos es asegurar que los mismos son válidos y que no sufrieron transformación alguna. Para eso el transmisor acompaña al mensaje un código especial que en ZigBee lo llaman Código de Integridad de Mensaje (MIC: Message Integrity Code). El MIC se genera con un método que conocen tanto el emisor como el receptor. Un dispositivo no autorizado no debería poder crear este MIC. Cuando recibe el mensaje el receptor calcula el MIC y si éste coincide con el que envía el transmisor, el mensaje se considera auténtico. El nivel de seguridad en el control se incrementa con el número de bits del MIC. ZigBee y 802.15.4 soportan MIC de 32, 64 y 128 bits.
Si lo que se desea es tener confidencialidad lo que se debe hacer es encriptar el mensaje. EL MIC en ZigBee se genera usando el protocolo CCM* (enhanced Counter with Cipher Block Chaining Message Authentication Code). El CCM* se usa en conjunción con AES de 128 bit y comparten la misma clave de seguridad. En la Figura 25 se ve el uso de AES-CCM* para lograr autenticación y confidencialidad en el mensaje

En la Figura 26 se ven 3 entradas a la AES-CCM*: los datos, la clave y la cadena especial de 13 bytes apodado *nonce* construido a partir de datos de un header auxiliar que contiene bits control de seguridad, bits del contador de trama (frame) y el campo dirección fuente de un encabezado auxiliar. El AES usa el nonce como parte del algoritmo. El nonce no se repite para dos mensajes transmitidos con la misma clave porque se va incrementando el contador de trama. El uso del nonce apunta a garantizar la “frescura del mensaje”. Si un intruso retiene el mensaje y lo envía más tarde, el contador de trama indicará que el mensaje se había recibido previamente. Si intentara modificar el contador de trama antes de retransmitir el mensaje, el receptor notaría la modificación no autorizada, porque el MIC calculado no coincide con el MIC que trae el mensaje. EL MIC es un poderoso control de modificaciones intencionales y accidentales.

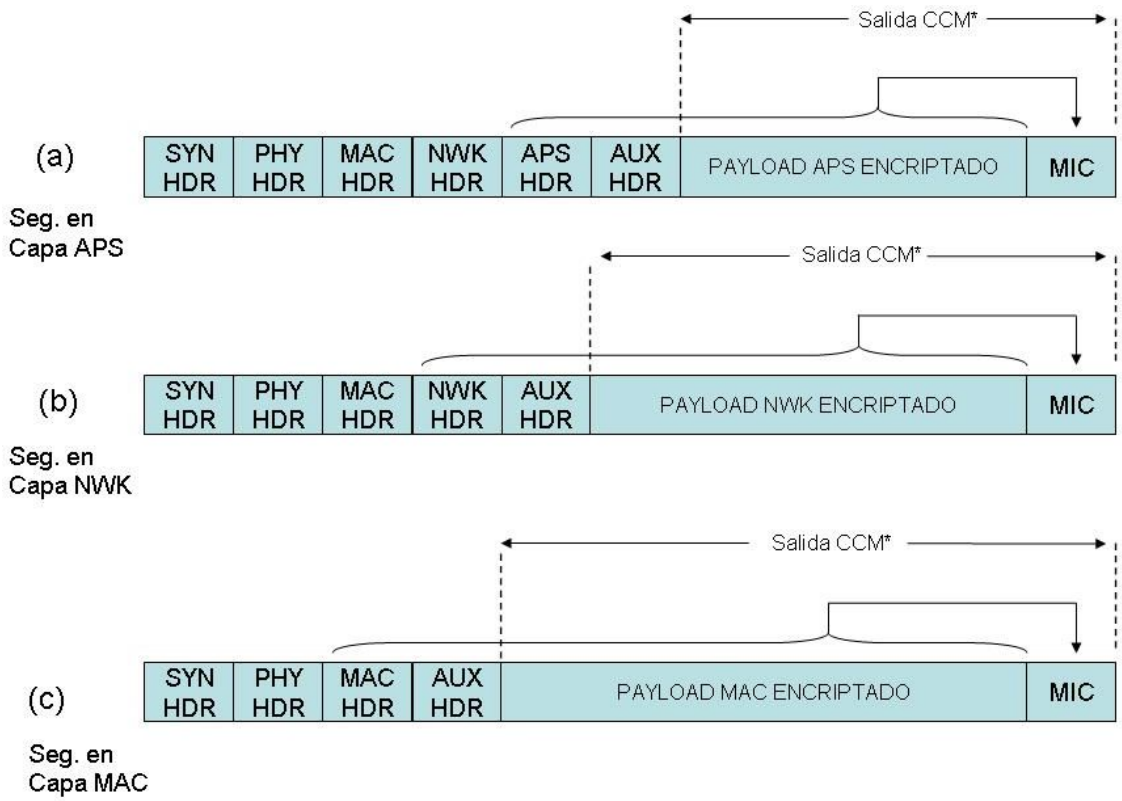

Figura 25: El uso de seguridad por capas aplicando AES

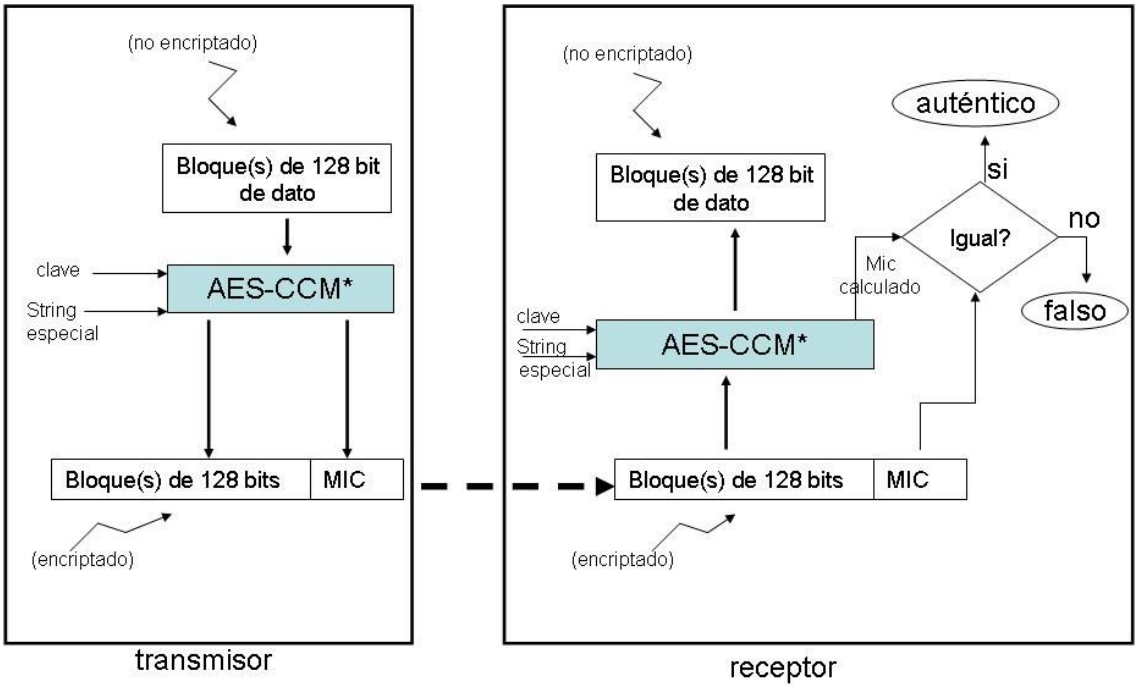

Figura 26: El proceso de encriptación, desencriptación en AES

5 Estudio comparativo de Zigbee con otras tecnologías

5.1 Zigbee vs. Bluetooth

Es inevitable la comparación entre dos estándares de redes WPAN. Bluetooth es un protocolo que se ha popularizado en los últimos años [9]. Su objetivo de diseño fue la eliminación de cables de interconexión de datos entre equipos de consumo masivo como: teléfonos celulares, notebooks, netbooks, pdas, equipos de audio, televisión. Así es posible escuchar temas musicales por la radio del auto transmitidos desde el teléfono celular ó conectar un GPS a una netbook.

Zigbee está especialmente diseñado para el manejo de controles, recolección de datos de sensores, preparado para trabajar con muchos (centenas hasta miles) dispositivos de tipo portátiles en donde la duración de las baterías es un factor crítico.

5.1.1 Interfase de comunicación radial.

Ambas usan la técnica de espectro extendido. Bluetooth usa FHSS y Zigbee usa DSSS. En la Tabla 2 se muestra una comparación de ZigBee y Bluetooth.

Tabla 2: Comparación ZigBee Bluetooth

Característica	**ZigBee**	**Bluetooth**
Modulación	DSSS	FHSS
	11 chips/símbolo	1600 saltos/segundo
	62.5 Ksimbolo/segundo	1 Msímbolo/segundo
	4 bits/símbolo	1 bit/símbolo
Tasa de información pico	~ 127 Kbit/segundo	~ 108-723 kbit/segundo
Tiempo de enumeración	30 ms típico	≥ 3 s , típico 20 s
Tiempo de transición de dormido a activo	15 ms típico	3 s típico
Tiempo de un esclavo activo de acceso al canal	15 ms típico	2 ms típico

5.1.2 Comparación en gasto de batería.

El consumo de energía es directamente proporcional al tiempo que los dispositivos estén en transmisión/recepción y esto está relacionado al tamaño del paquete ya que cuanto más pequeño es el paquete antes los dispositivos entrarán en modo dormir. Por otro lado, cuanto más grande sea el paquete más se acerca la tasa efectiva de datos a la velocidad plana de la interfase.

Bluetooth es un protocolo que se maneja en base a ranuras de tiempo. La comunicación puede ocurrir en 1 ranura = 625µs, 3 ranuras= 1875µs ó 5 ranuras = 3125µs. Considerando que después de cada transmisión llega un ACK en la próxima ranura, se muestran en la Tabla 3 los tiempos en función de los tipos de paquetes.

Tabla 3: Características de velocidad de transferencia de los paquetes Bluetooth

Tipo de paquete	Nº de ranuras	Carga máx. de inform. [bytes]	Tiempo total [us]	Tasa efectiva [kb/s]
DH1	1	27	1250	172.8
DH3	3	183	2500	585.6
DH5	5	339	3750	723.2

En la Figura 27 se puede ver cómo aparecen picos en la tasa efectiva de datos de Bluetooth. La carga se manda en ranuras y se debe usar una ranura tanto para enviar 2 bytes como para 5, 8 ó 27.

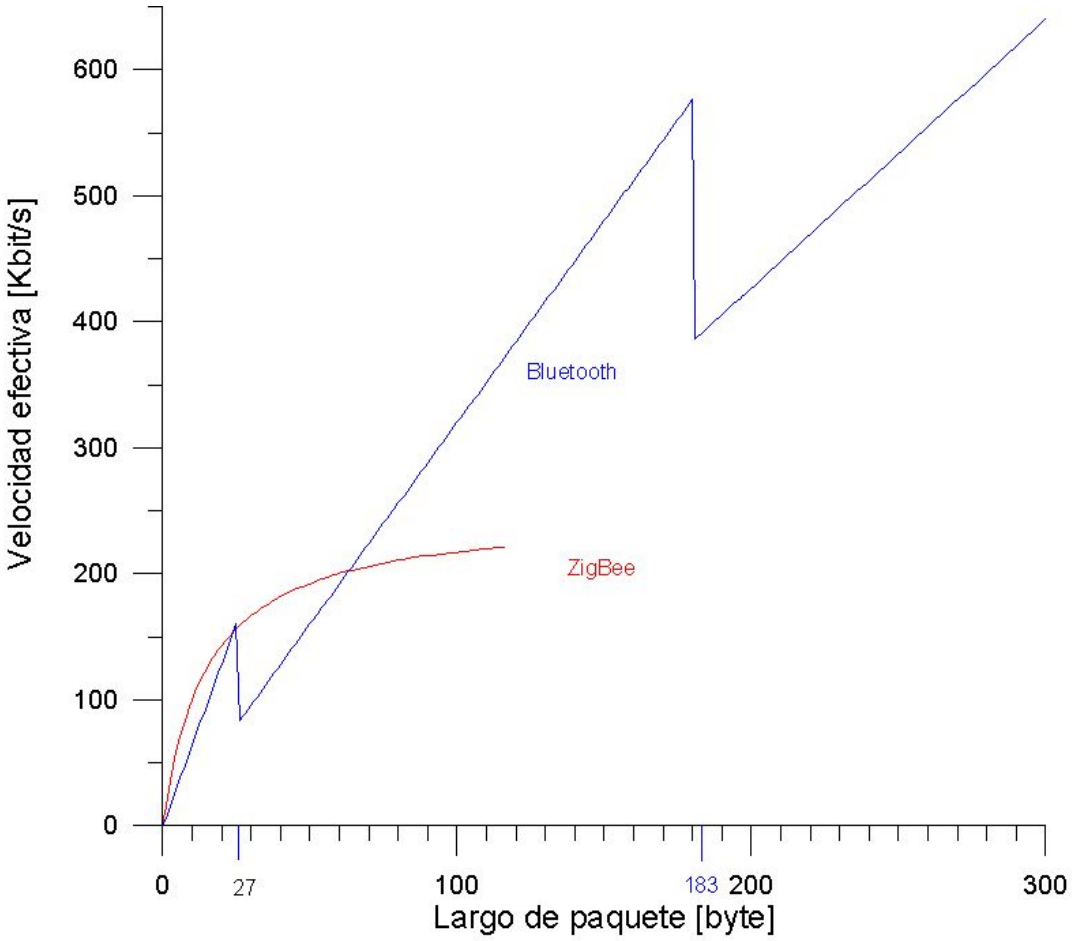

Figura 27: Comparación de velocidad efectiva entre ZigBee y Bluetooth en base a largo de paquete

Zigbee fue diseñado pensando en paquetes pequeños y se puede observar que para paquetes de menos de 75 bytes, Zigbee tiene, a pesar de su baja velocidad física de transmisión de datos, una velocidad efectiva mayor que Bluetooth. Por lo tanto, para pequeños paquetes Bluetooth va a gastar mayor energía debido a que necesita mayor tiempo de transmisión/recepción. La gráfica se basa en los protocolos Bluetooth v1.1 y el IEEE 802.15.4 en condiciones ideales, esto es: el canal está vacío, no hay errores y no se necesita retransmisión.

Otra diferencia notable es en el tiempo de enumeración. En Bluetooth se requieren típicamente 20 segundos contra 15 ms de Zigbee. En conclusión como Zigbee está muy bien preparado para realizar rápidamente el proceso de conexión y desconexión a la red, esto determina que se requiera la centésima parte de la energía que requiere Bluetooth para esta misma tarea.

Además, el protocolo Bluetooth se basa en encuestar a cada dispositivo esclavo y en cambio Zigbee se basa en CSMA-CA, que debe esperar a tener el canal libre. Esto no representa un problema porque en redes de muy bajo tráfico como redes de sensores, no hay competencia por el canal.

Como corolario, el bajo consumo energético de Zigbee, permite usar pilas alcalinas tipo AA por más de 6 meses (hasta 2 años típico). Lo típico en Bluetooth es usar baterías recargables con periodicidad de carga de algunos días. ZigBee y Bluetooth son dos soluciones pensadas para aplicaciones diferentes. Bluetooth es apto para aplicaciones de baja latencia como audio y video. Es un protocolo maestro-esclavo para unos pocos dispositivos. Zigbee está diseñado para uso de sensores y controles que usan mensajes cortos. Está preparado para redes tipo estrella ó entre pares de cientos de dispositivos. Estas diferencias entre ZigBee y Bluetooth se originan en las arquitecturas de cada uno de estos protocolos y no parece probable que los cambios de versiones modificaría la situación.

5.2 Otras tecnologías WPAN

Existen varios estándares además de ZigBee que usan el IEEE802.15.4 como base de su protocolo. Los más conocidos son 6LoWPAN y WirelessHART. También existen otros protocolos que no usan IEEE802.15.4. Se destacan entre estos Z-wave, Bluetooth y ULP Bluetooth.

5.2.1 El protocolo 6LoWPAN

La filosofía de este protocolo es poder transmitir paquetes de tipo Ipv6 para simplificar la interfase entre redes de sensores e Internet [10]. La ventaja natural es la facilidad de conexión de la red WPAN a Internet. La desventaja es que los nodos de sensores tienen limitaciones en capacidad de procesamiento. IPV6 requiere soporte de paquetes más grande que lo que brinda IEEE 802.15.4. El payload máximo de IEEE 802.15.4 es de 128 bytes contra 1280 bytes requeridos por IPV6 por lo que requiere una fragmentación. Para eso se agrega una capa en 6LOWPAN llamada capa de adaptación que fragmenta y rearma los paquetes.

La comparación con ZigBee indica que para aplicaciones de paquetes pequeños con baja interacción con dispositivos IP es más eficiente ZigBee. La interacción con Internet la puede hacer un dispositivo puente.

5.2.2 WirelessHart

HART es un protocolo usado en la industria para control de procesos, diagnóstico y control [11]. Es un protocolo para usar en redes cableadas. WirelessHart es la extensión a redes inalámbricas que usa la banda de 2.4 GHz y para seguridad aplica AES-128 tal como ZigBee. Si bien usa la misma base de IEEE 802.15.4 que ZigBee, utiliza

potencias más elevadas, y programa la capa física para poder hacer saltos de canal paquete a paquete. Tanto ZigBee como WirelessHart se usan en ambientes industriales. La ventaja de este último protocolo es la compatibilidad hacia atrás con las redes HART.

5.2.3 Z-wave

Fue desarrollado por la Alianza Z-wave [12]. No adopta IEEE 802.15.4. Usa la banda de 900MHz en un sistema de banda angosta. Usa FSK con velocidad de datos de 40kbps. Z-Wave soporta direccionamiento de 8 bits contra los 16 bits de direccionamiento de ZigBee. Usa una variante de DES (Data Encryption Standard) como método de seguridad. Para algunas aplicaciones esta seguridad puede ser insuficiente ya que usa una clave de solo 56 bits. ZigBee ofrece más velocidad, seguridad y mayor cantidad de nodos en una red. Z-wave es más simple y consecuentemente tiene más bajo costo por nodo.

5.2.4 ULP Bluetooth

Ya se comparó ZigBee con Bluetooth y se remarcó el gran gasto energético de este último. ULP Bluetooth es un estándar desarrollado para comunicaciones con bajo ciclo efectivo con el objeto de reducir el consumo energético [13]. ULP no soporta redes tipo malla. ULP compite con ZigBee en aplicaciones punto a punto. Hay algunos dispositivos Bluetooth llamados de modo dual que pueden hacer de interfase entre los dispositivos ULP y los Bluetooth clásicos ya que trabajan en los dos modos.

6 Conclusiones y Trabajo Futuro

La alianza ZigBee compuesta por importantes firmas desarrolladoras de hardware y software ha impuesto su "estándar" frente a otras alianzas que desarrollaron protocolos para un uso más específico. Hay muchos protocolos propietarios que fundamentalmente en redes pequeñas pueden ser más eficaces pero la estandarización de productos hace que sea más simple y seguro adoptar un estándar ampliamente difundido.

Hay todo un campo específico de aplicación en sistemas de baja transferencia de datos y baja energía y bajo costo en el cual ZigBee compite favorablemente. A pesar de su relativa simplicidad comparada con otros estándares, ZigBee provee confiabilidad, flexibilidad y escalabilidad.

Para desarrollar su estándar, la alianza ZigBee se ha valido de otros estándares: IEEE802.15.4 para sus capas inferiores y algoritmos clásicos para ruteo y seguridad. Con los perfiles que los fabricantes usan en sus dispositivos es fácil para el usuario configurar una red.

Como trabajo futuro se piensa profundizar la investigación en los mecanismos de ruteo. Con la aparición de redes ZigBee compuestas por decenas o centenas de dispositivos cobran importancia los algoritmos de ruteo y la forma de minimizar el gasto de batería de los nodos ruteadores. Tradicionalmente, el costo de una ruta se mide en cantidad de saltos y/o calidad de enlace, pero es importante encontrar otros algoritmos basados en métricas tales como: gastos de energía y/o energía remanente en un nodo y que a su vez sean lo suficientemente simples de implementar. Para el análisis de estos algoritmos en diferentes situaciones se deberán perfeccionar los modelos existentes para redes ZigBee en simuladores como NS-2. Se han propuesto muchos algoritmos, cada uno de ellos con ventajas en determinado escenario. Se podrían diseñar herramientas que ayuden a los implementadores de redes a simular el comportamiento de las mismas.

ACRÓNIMOS

AES Advance Encryption Standard
A0DV Ad Hoc On-Demand Distance Vector
APDU Application Support Sublayer Protocol Data Unit
APL Application Layer
APSDE Application Support Sublayer Data Entity
APSME Application Support Sublayer Management Entity
ASDU APS Service Data Unit
CAP Contention Access Period
CBC-MAC Cipher Block Chaining Message Authentication Code
CCA Clear Channel Assessment
CCM Counter with CBC-MAC
CCM* CCM versión extendida.
CFP Contention Free Period
CSMA-CA Carrier Sense Multiple Access with Collision Avoidance
DES Data Encryption Standard
DSSS Direct Sequence Spread Spectrum
ED Energy Detection
FCS Frame check Sequence
FFD Full Function Device
GTS Guaranteed Time Slot
HDR Header
IB Information Base
ISM Industrial, Scientific and Medical
LQI Link Quality Indicator
LR-WPAN Low-Rate Wireless Persona Area Network
MAC Medium Access Control
MIC Message Integrity Code
MPDU MAC protocol Data Unit
MSDU MAC Service Data Unit
MLME MAC Layer Management Entity
MLME-SAP Mac Layer Management Entity Service Access Point
NLDE Network Layer Data Entity
NLME Network Layer Management Entity
NPDU Network Protocol Data Unit
NSDU Network Service Data Unit
NWK Network Layer
O-QPSK Offset Quadrature Phase Shift Keying
OSI Open System Interconnection
PAN Personal Area Network
PD Physical Data
PHY Physical Layer
PIB Pan Information Base
PLME Physical Layer Management Entity
POS Personal Operating Space
PPDU Physical Prococol Data Unit
PSDU Physical Service Data Unit
PIB Pan Information Base
QOS Quality of Service

RFD Reduced Function Device
RX Receptor
SAP Service Access Point
SKKE Symmetric-Key Key Establishment
SNR Signal to Noise Ratio
SSP Secure Service Provider
WLAN Wireless Personal Area Network
WPAN Wireless Personal Area Network
ZDO ZigBee Device Object

Referencias

[1] ZigBee Specification 05347r17 , Enero 2008 , disponible en Zigbee Alliance, www.zigee.org

[2] IEEE 802.15.4 Wireless Medium Access Control and Physical Layer Specifications for Low –Rate Wireless Personal Area Networks, Sept 2006

[3] J. Dignani, S. Drangosh, "Interconectando sistemas de domótica". WICC 2008

[4] S. Farahani, "ZigBee Wireless Networks and transceivers", Elsevier ,2008

[5] P: Bahl , V. Padmanabhan, " RADAR: An In-Building RF-Based User Location and Tracking System", IEEE INFOCOM, Marzo 2000

[6] E. Sosa, "Contribuciones al establecimiento de una red global de sensores inalámbricos interconectados", tesis doctoral UNLP, febrero 2011

[7] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, U.S. Department of Commerce/NIST,Springfield, VA, Noviembre 2001, disponible en http://csrc.nist.gov/.

[8] A. Tanenbaum, "Computer Networks", cuarta edición, Prentice Hall, 2002

[9] Bluetooth Standard, disponible en www.Bluetooth.com

[10] Ipv6 over IEEE 802.15.4 (6LoWPAN), disponible en http://6lowpan.net/.

[11] WirelessHART, disponible en www.hartcomm.org

[12] Z-wave Alliance, disponible en www.z-wavealliance.org

[13] Wibree, disponible en www.wibree.com

[14] C. E. Perkins, E. M. Belding-Royer, and S. R. Das ,Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561: IETF, 2003.

[15] Advanced Encryption Standard (AES) , Federal Information Processing Standards Publication 197, US Department of Commerce/NIST, Springfield, VA, 2001, disponible en http://csrc.nist.gov