CAPÍTULO 3
ZigBee.

Las redes inalámbricas de área personal (WPANs) se usan para la transmisión de información en distancias relativamente cortas. A diferencia de las redes inalámbricas de área local (WLANs), las conexiones en WPANs usan muy poca infraestructura; es esta característica la que permite que se puedan desarrollar tecnologías con dispositivos pequeños, con un buen rendimiento de potencia y de bajo costo.

ZigBee es una tecnología de relativa reciente aparición, está basada en el estándar IEEE 802.15.4: *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, pensada en aplicaciones donde la transferencia de datos no es muy grande y con la ventaja de tener una larga vida útil de sus baterías. Este estándar define las capas más bajas del Modelo de Referencia OSI, la capa física y la capa de enlace. Las capas superiores las define la tecnología ZigBee por medio de la ZigBee Alliance; estas capas son una de red y otra de aplicación, las cuales dependen de los requerimientos del sistema que queramos satisfacer.

Como ya se mencionó en el capítulo anterior, el trabajo de la ZigBee Alliance es promover el uso de esta tecnología y generar parámetros para estandarizar los dispositivos que deseen trabajar con ella. Para aplicaciones más generales hay regulaciones que permiten la interoperabilidad entre dispositivos de red. Para promover esta interoperabilidad entre diversas marcas de dispositivos de red y entre diferentes equipos de distintos fabricantes se creó el Modelo de Referencia OSI.

MODELO DE REFERENCIA OSI

Desde hace varios años se ha dado un crecimiento muy importante de las redes de comunicación porque las empresas se dieron cuenta de los beneficios que les traían. Los proveedores de soluciones y tecnología se dieron cuenta del gran mercado que esto representaba y se apresuraron a entregar diferentes soluciones que los posicionaran en el gusto de las empresas.

Durante algún tiempo, el desarrollo se dio sin ningún tipo de regulación, esto provocó que se presentaran diversos problemas de compatibilidad entre equipos de diferentes fabricantes que intentaban satisfacer la misma necesidad.

En un principio, los fabricantes tenían sus propias convenciones de comunicación para interconectar sus equipos, pero pronto se vio la utilidad y necesidad de conectar dispositivos de distintos fabricantes en una misma red.

Es en este marco que la Organización Internacional para la Estandarización (ISO, del inglés *International Organization for Standarization*) decidió desarrollar el Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI, del inglés *Open System Interconennection*), conocido de manera más general como Modelo de Referencia OSI.

Capítulo 3.

ZigBee.

En el año 1977, la ISO decidió crear un subcomité para satisfacer la apremiante necesidad de generar referencias estandarizadas para tener redes informáticas heterogéneas[1]. Este subcomité es el que conocemos como *Reference Model of Open Systems Interconnection* o Modelo de Referencia de Interconexión de Sistemas Abiertos (modelo OSI). La labor de este subcomité vio la luz en el año de 1979, cuando se aprobaron las recomendaciones de este grupo de trabajo.

Es importante señalar que, como su nombre lo indica, este es sólo un modelo, no un protocolo, es decir, es simplemente un marco de referencia para los distintos protocolos que se crean y se utilizan para la comunicación entre dispositivos.

La jerarquía del modelo de referencia OSI se compone de 7 niveles o capas. Cada capa se define por software, o en su caso hardware, y es claramente distinta de las otras. Estas capas no son protocolos por sí mismas pero proporcionan una forma de definir y separar protocolos para realizar transferencias de datos en forma estandarizada. Cada capa está diseñada para manejar mensajes que recibe de una capa inferior o una superior. Cada una también envía mensajes a una capa por arriba o por debajo de ella de acuerdo con instrucciones específicas. Entre sí, estas capas trabajan en forma autónoma, sólo saben que tienen que enviar o recibir hacia la capa inferior o superior respectivamente, sin intervenir con la función de la otra.

Los datos a enviar que dan origen a la transmisión pasan sin excepción alguna por cada una de las siete capas del modelo, en forma descendente desde el dispositivo de origen y en forma ascendente en el de destino. Para cada capa, según su función, existen distintos protocolos que se encargan de la prestación de los servicios de cada una. En la figura 3.1 vemos una imagen de la representación del modelo de referencia OSI.

A continuación se describe cada una de las capas del modelo.

- Capa 1: capa física. Esta capa es el medio de comunicación físico que soporta la transmisión de bits, métodos de comunicación, velocidades de transmisión de datos y funciones tales como la sincronización.
- Capa 2: enlace de datos. Esta capa provee la trama de enlace básica, incluyendo la información del paquete, inicio y encabezados, y un campo de revisión de error. Se asegura de que los paquetes sean entregados de manera confiable a través de la red.
- Capa 3: red. Esta capa determina la configuración de la red y la ruta que puede tomar la transmisión. Esta capa genera y lee la información de la dirección y controla el campo para propósitos de control de flujo.

[1] "OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection", ZIMMERMAN.

- Capa 4: transporte. Esta capa es responsable de proporcionar la transferencia de datos entre dos usuarios a un punto acordado de calidad de servicio (QoS).
- Capa 5: sesión. Esta capa maneja aspectos como administración y sincronización de las transmisiones de datos. Por lo común incluye procedimientos de ingreso (*log-on*) y salida (*log-off*), así como autorización del usuario. También determina la disponibilidad de red para procesamiento y almacenamiento de datos que se transmitirán.
- Capa 6: presentación. Esta capa se asegura de que los datos que llegan desde la red se puedan utilizar en la aplicación y garantiza que la información que envía la aplicación pueda transmitirse a través de la red.
- Capa 7: aplicación. Esta capa provee al usuario del programa de una interfaz para interactuar con el modelo OSI. Es la administradora general de la red o el proceso de comunicaciones. Su función principal es formatear y transferir archivos entre el mensaje de comunicaciones y el software de aplicaciones del usuario.

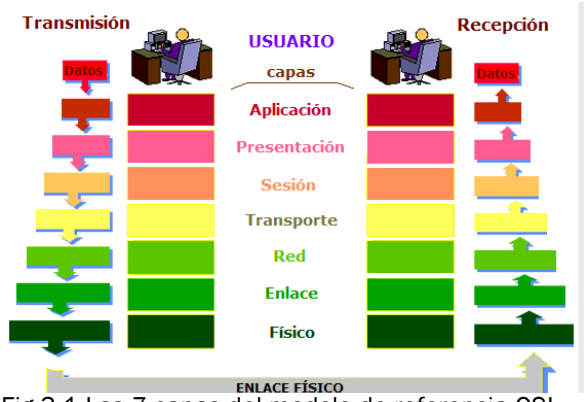

Fig 3.1 Las 7 capas del modelo de referencia OSI.
Imagen tomada de www.alegsa.com.ar/Dic/Modelo%20OSI.php

El proceso básico es que se añade o remueve información mientras se trasmiten los datos de una capa a otra.

RELACION DE ZigBee CON EL MODELO DE REFERENCIA OSI.

ZigBee es el nombre que tiene la tecnología cuya base es el estándar IEEE 802.15.4, el cual da las especificaciones de las dos primeras capas del modelo OSI, la capa física y la capa de enlace. Las capas superiores son las que definen propiamente a la tecnología ZigBee. La figura 3.2 nos muestra esto de manera gráfica.

El estándar IEEE 802.15.4 define a una LR-WPAN (*low rate wireless personal area network,* red inalámbrica de área personal de baja tasa). Esta es una red simple y de bajo costo que permite que exista comunicación en aplicaciones con potencia limitada. Las características principales de los dispositivos de las redes LR-WPAN son la facilidad de instalación, transferencia de datos confiable, rango de

operación corto, una razonable vida útil de las baterías y bajo costo, sin que esto signifique aumento en la complejidad del protocolo.

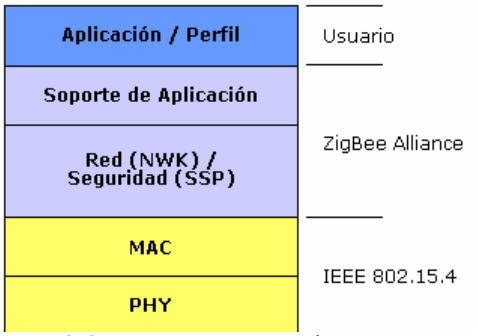

Fig 3.2 Pila de la tecnología ZigBee.
Imagen tomada de "El estándar inalámbrico ZigBee"

La primera aprobación de este estándar se dio en el año de 2003, sin embargo se hicieron algunos ajustes y mejoras a éste y actualmente los sistemas funcionan aplicando el estándar aprobado el 7 de Junio de 2006 con el nombre IEEE 802.15.4-2006.

Este estándar define el protocolo y la interconexión compatible para comunicación de datos usando dispositivos de baja tasa de transferencia, baja potencia y baja complejidad de transmisiones de radio de corto alcance en una red inalámbrica de área personal (WPAN). El estándar usa CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*, Acceso Múltiple por Detección de Portadora y Evasión de Colisiones) como mecanismo de acceso al medio y soporta topologías estrellas y punto a punto[2].

LA CAPA PHY DEL ESTÁNDAR

La capa más baja del estándar IEEE 802.15.4, y por lo tanto de la tecnología ZigBee, es la capa física. Esta tiene la función de ser el enlace entre la capa de enlace de datos y el canal físico de radio. Las tareas de las que esta capa es responsable son:

- activación y desactivación del transreceptor de radio
- detección de energía en el canal de radio actual
- indicar la calidad del enlace de los paquetes recibidos
- evaluación de la disponibilidad del canal para permitir CSMA-CA
- selección del canal de frecuencia
- transmisión y recepción de datos.

La PHY proporciona dos servicios: el servicio de datos PHY y el servicio de manejo de PHY que se comunica con el punto de acceso de servicio (SAP, *service access point*) de la entidad de manejo de la capa física (PLME, *physical layer management entity*) conocido como PLME-SAP. El servicio de datos PHY habilita la

[2] IEEE 802.15.4-2006

transmisión y recepción de las unidades de protocolo PHY (PPDUs, *PHY protocol data units*) a través del canal de radio físico.

Cada paquete PPDU que se transmite tiene los siguientes elementos básicos:

- un encabezado de sincronización (SHR, *synchronization header*) que permite al dispositivo receptor que se sincronice con la recepción del flujo de bits
- un encabezado PHY (PHR, *PHY header*) que contiene la información de la longitud de la trama
- una longitud de *payload* variable que acarrea la trama de la subcapa MAC.

La figura 3.3 muestra la estructura del paquete PPDU.

		OCTETOS		
		1		Variable
Preámbulo	SFD	Longitud de la trama (7 bits)	Reservado (1 bit)	PSDU
SHR		PHR		PHY payload

Figura 3.3 Formato de la PPDU
Como se muestra en IEEE 802.15.4-2006

La transmisión del paquete se hace como se ve en la figura 3.3, donde el campo de la extrema izquierda debe ser transmitido o recibido primero. Todos los campos de múltiples octetos deben ser transmitidos o recibidos a partir del octeto menos significativo y cada octeto enviará primero el bit menos significativo. El mismo orden de transmisión aplica para los campos de datos que se transfieren entre la capa PHY y la subcapa MAC.

El campo del preámbulo se usa por el transreceptor para obtener sincronización del símbolo y el *chip* con el mensaje entrante. Para el caso de la banda de 2.4 GHz, la longitud de este campo es de 8 símbolos o 4 octetos y dura 120 nanosegundos.

El campo SFD (*start-of-frame delimiter*, limitador del inicio de la trama) indica el final del SHR y el inicio del paquete de datos. Su longitud es de 2 símbolos o 1 octeto.

El campo de longitud de la trama es de 7 bits y especifica el número total de octetos contenidos en el PSDU.

El campo PSDU (*PHY service data unit,* unidad de datos de servicio de la PHY) es de longitud variable y contiene el dato del paquete PHY.

Capítulo 3.

ZigBee.

Las capas físicas que define este estándar son cuatro, cada una con una tasa de transferencia diferente y distinta modulación. Todas usan espectro disperso para evitar el desvanecimiento y aumentar la robustez.

Las capas físicas especificadas son las siguientes:

- 868/915 MHz usando DSSS con modulación BPSK (*binary phase-shift keying*)
- 868/915 MHz usando DSSS con modulación O-QPSK (*offset quadrature phase-shift keying).*
- 868/915 MHz usando PSSS (*parallel sequence spread spectrum*) con modulación BPSK y ASK (*amplitud shift keying*).
- 2450 MHz usando DSSS y modulación O-QPSK.

Las primeras tres capas físicas soportan tasas de 20 kbps, 40 kbps y hasta 100 kbps y 250 kbps. La capa de 2450 MHz soporta tasas de 250 kbps. La banda de 868 MHz es para aplicaciones en el continente europeo, la banda de 915 MHz en el norte del continente americano y la banda de 2450 MHz es aplicable en el mundo entero, por lo que la mayoría de los fabricantes deciden trabajar en ella.

Estas tres bandas pertenecen a las bandas ISM por lo que está definido también que los sistemas deben aceptar las interferencias provocadas por los equipos que pertenezcan a ese grupo y no deben causarles ningún tipo de interferencia a aquellos.

La tabla 3.1 presenta los diferentes parámetros de los canales de transmisión de la capa física con los que debe cumplir un dispositivo para trabajar en el mismo.

CANAL	FRECUENCIA (MHz)	Parámetros de dispersión		Parámetros de los datos		
		Tasa de chip (kchip/s)	Modulación	Tasa de bits (kb/s)	Tasa de símbolo (ksímbolo/s)	Símbolos
868/915	868 – 868.6	300	BPSK	20	20	Binario
	902 – 928	600	BPSK	40	40	Binario
868/915 (opcional)	868 – 868.6	400	ASK	250	12.5	20-bit PSSS
	902 – 928	1600	ASK	250	50	5-bit PSSS
868/915 (opcional)	868 – 868.6	400	O-QPSK	100	25	Base 16 ortogonal
	902 – 928	1000	O-QPSK	250	62.5	Base 16 ortogonal
2450	2400 – 2483.5	2000	O-QPSK	250	62.5	Base 16 ortogonal

Tabla 3.1 Bandas de frecuencia y tasas de transferencia de IEEE 802.15.4

Capítulo 3.

ZigBee.

Todas las comunicaciones se dan con espectro disperso. La modulación en la banda de 2.4 GHz usa un código pseudoaleatorio con una longitud de 32 elementos y un ancho de banda de 2 MHz. Para la banda de 868 MHz se usa un código PN (*pseudonoise*) de 15 elementos de longitud y opera con un ancho de banda de 600 KHz. En la banda de 915 MHz se usa el mismo código PN con un ancho de banda de 1200 KHz.

En el apéndice A se explica con mayor detalle el funcionamiento de la técnica de espectro disperso y los códigos pseudoaleatorios.

Además del uso de SS, ZigBee usa FDMA (*frequency division multiple access*) para mejorar la coexistencia de los sistemas que usen esta tecnología con otras; esto es, que divide la banda en un número de canales que no se traslapen entre sí.

Hay un total de 27 canales disponibles a lo largo de las tres bandas de frecuencia. En la banda de 868 MHz hay un canal (canal 0), en la banda de 915 MHz hay 10 canales (del canal 1 al canal 10), y hay 16 canales disponibles en la banda de 2.4 GHz (del canal 11 al canal 26).

Las asignaciones de las frecuencias centrales de estos canales se hacen por medio de las fórmulas que se presentan a continuación:

$F_c = 863.3$ para $k = 0$

$F_c = 906 + 2(k-1)$ para $k = 1,2,\ldots,10$

$F_c = 2405 + 2(k-11)$ para $k = 11,12,\ldots,26$

donde k es el número del canal.

En nuestro caso la capa PHY más conveniente es la de 2450 MHz por la cantidad de información que permite manejar y porque es una banda libre en todo el mundo. La especificación indica que la tasa de transferencia en este caso es de 250 Kbps usando una técnica de modulación base 16 cuasi-ortogonal. Esta relativamente alta tasa de transmisión, reduce el tiempo de transmisión así como la energía por cada bit de dato enviado y transmitido. Durante el período de cada símbolo se usan 4 bits de información para seleccionar una de 16 secuencias de ruido pseudoaleatorio ortogonal. La secuencia pseudoaleatoria para los símbolos siguientes están concatenados y la secuencia de chip se modula con la portadora usando O-QPSK.

La figura 3.4 muestra los pasos que se siguen en la capa PHY para la transmisión de información en la banda de 2.4 GHz.

Capítulo 3.

ZigBee.

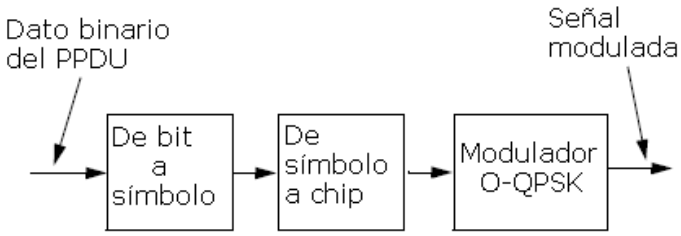

Figura 3.4 Diagrama de modulación y dispersión de la señal.
Como se muestra en IEEE 802.15.4-2006

La información del PPDU que viene en código binario se mapea en símbolos. Los cuatro bits menos significativos (b_0, b_1, b_2, b_3) de cada octeto se mapean en un símbolo, y los cuatro bits más significativos (b_4, b_5, b_6, b_7) del mismo octeto se mapean en otro símbolo. Cada octeto del PPDU sigue este procedimiento iniciando con el campo de preámbulo y terminando con el último octeto del PSDU.

Cada símbolo de dato se mapea en secuencia de pseudoruido de 32 chips, tal y como se especifica en la tabla 3.2. Estas secuencias se relacionan entre sí a través de cambios cíclicos y/o conjugaciones.

Símbolo de dato (decimal)	Símbolo de dato (binario)	Valores de chip
0	0000	11011001110000110101001000101110
1	1000	11101101100111000011010100100010
2	0100	00101110110110011100001101010010
3	1100	00100010111011011001110000110101
4	0010	01010010000101110110110011100011
5	1010	00110101001000101110110110011100
6	0110	11000011010100100010111011011001
7	1110	10011100001101010010001011101101
8	0001	10001100100101100000011101111011
9	1001	10111000110010010110000001110111
10	0101	01111011100011001001011000000111
11	1101	01110111101110001100100101100000
12	0011	00000111011110111000110010010110
13	1011	01100000011101111011100011001001
14	0111	10010110000001110111101110001100
15	1111	11001001011000000111011110111000

Tabla 3.2 Tabla de mapeo símbolo a chip como se muestra en IEEE 802.15.4

La secuencia de chips que representa cada símbolo se modula en la portadora usando O-QPSK con un conformado de pulso de medio seno. Los chips indexados pares se modulan en la portadora de fase de entrada (I) y los chips indexados impares se modulan en la portadora de cuadratura de fase (Q). Ya que cada símbolo está representado por una secuencia de 32 chips, la tasa de chip (nominalmente 2.0 Mchip/s) es 32 veces la tasa de símbolo. Para formar el offset entre la fase-I y la fase-Q, los chips de la fase-Q deberán ser retardados por T_c con respecto a los chips de la fase-I, donde T_c es el inverso de la tasa de chip. Véase la figura 3.5.

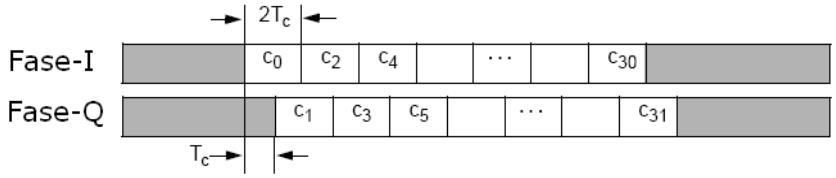

Figura 3.5 Offset de los chips de O-QPSK.
Como se muestra en IEEE 802.15.4-2006

Durante cada periodo de símbolo, el chip menos significativo, c_0, se transmite primero y el chip más significativo, c_{31}, se transmite al final.

Para esta banda, el conformado de pulsos que representa cada chip banda base se define por:

$$p(t) = \begin{cases} \sin(\pi \frac{t}{2T_c}, 0 \le t \le 2T_c \\ 0, \quad \text{cualquier otro caso} \end{cases}$$

donde T_c es el inverso de la tasa de chip.

La tasa de transmisión en la capa física en la banda de 2.4GHz deberá ser de 62.5 Ksímbolos/seg ± 40 ppm.

Un dispositivo que cumpla con todas las especificaciones que se establecen en el estándar deberá ser capaz de alcanzar una sensibilidad de -85 dBm o mejor.

Para que un dispositivo opere de conformidad al estándar, debe ser capaz de transmitir cuando menos una señal de -3 dBm. La máxima potencia de transmisión queda limitada por los organismos reguladores locales. El receptor deberá recibir una señal mayor o igual a -20 dBm.

Los niveles de resistencia contra el *jamming* se definen en dos partes, la que se acepta de los canales adyacentes y la de que se acepta de los canales alternos. Los primeros son los que se encuentran a los lados del canal deseado y los alternos son los que se encuentran más alejados, junto a los canales adyacentes. De los canales adyacentes se aceptan 0 dB y de los canales alternos se aceptan 30 dB.

Capítulo 3.

ZigBee.

SUBCAPA MAC DEL ESTANDAR

El estándar de la IEEE en el que se basa ZigBee también define la subcapa MAC de la capa de enlace del modelo OSI. Esta subcapa sirve de enlace entre la capa física y la capa de red. Las tareas de esta capa son:

- generar *beacons* de red si el dispositivo es un coordinador
- sincronización de los *beacons* de red
- soportar asociación y disociación de la red PAN
- soportar la seguridad del dispositivo
- emplear el mecanismo CSMA-CA para el acceso al canal
- manejar y mantener el mecanismo GTS (*guaranteed time slot*)
- proveer un enlace confiable entre dos entidades MAC

La subcapa MAC proporciona una interfaz entre la SSCS (*service-specific convergence sublayer,* subcapa de convergencia de servicios específicos) y la PHY. Conceptualmente, la subcapa MAC incluye una entidad de manejo llamada MLME (*MAC sublayer management entity,* entidad de manejo de la subcapa MAC). Esta entidad proporciona la interfaz de servicio a través de la cual se pueden invocar las tareas de función de la capa. La MLME también es responsable de mantener una base de datos de los objetos que se manejan que pertenecen a la subcapa MAC.

La subcapa MAC proporciona dos servicios: el servicio de datos MAC y el servicio de manejo MAC, que se comunica con el punto de acceso de servicio (SAP) de la MLME conocida como MLME-SAP. El servicio de datos MAC habilita la transmisión y recepción de las unidades de protocolo de datos MAC (MPDU, *MAC protocol data unit*).

Cada trama MPDU tiene tres componentes principales:

a) un MAC *header* (MHR, encabezado MAC) que incluye un control de trama, número de secuencia, información de la dirección e información relacionada con la seguridad
b) un *payload* de MAC, de longitud variable, que contiene la información específica del tipo de trama
c) un MAC *footer* (MFR, campo terminal MAC) que contiene una secuencia de revisión de la trama (FCS, *frame check sequence*).

Las tramas de la subcapa MAC se describen como una secuencia de campos en un orden específico. El formato que se presenta en la figura 3.6, muestra cómo lo transmite la capa PHY, de izquierda a derecha, en donde el bit de la extrema izquierda se transmite primero. Los bits de cada campo se numeran desde 0 (extrema izquierda y menos significativo) hasta $k-1$ (extrema derecha y más significativo), donde la longitud del campo es de k bits.

Los campos que tienen una longitud mayor a un octeto se envían a la PHY en orden desde el octeto que contiene los bits numerados más bajos hasta el octeto que contiene los bits numerados mayores.

La figura 3.6 muestra el formato general de la trama MAC:

Octetos	2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	Variable	2
	Control de la trama	Número de secuencia	Identificador de la PAN destino	Dirección del destino	Identificador de la PAN origen	Dirección de la fuente	Encabezado de seguridad auxiliar	Payload de la trama	FCS
			Campos de direccionamiento						
	MHR							Payload de la MAC	MFR

Figura 3.6 Formato general de la trama MAC.
Como se muestra en IEEE 802.15.4-2006

El campo de control de la trama tiene una longitud de 2 octetos y contiene información que define el tipo de trama, campos de direccionamiento y otras banderas de control.

El campo del número de secuencia es un octeto de longitud y especifica un identificador de secuencia de la trama.

El campo de identificador de la PAN destino, cuando está presente, es de 2 octetos de longitud y especifica un identificador único de la PAN a la que se pretende enviar la trama.

El campo de dirección del destino, cuando está presente, es de 2 u 8 octetos de longitud, dependiendo del valor especificado en el modo de direccionamiento del destino, y proporciona la dirección del dispositivo al que va dirigida la trama.

El campo de identificador de la PAN origen, es de dos octetos de longitud cuando está presente, y especifica el identificador único de la PAN de la que proviene la trama.

El campo de dirección de la fuente, es de 2 u 8 octetos de longitud cuando está presente, de acuerdo al valor especificado en el modo de direccionamiento de la fuente, y especifica la dirección del generador de la trama.

El encabezado de seguridad auxiliar especifica la información requerida para el proceso de seguridad, incluyendo cómo está protegida la trama.

El campo de *payload* de la trama contiene información específica de cada trama.

El campo FCS (*frame check sequence*, secuencia de revisión de la trama) es un mecanismo que se usa para detectar errores en los bits y se usa para verificar si se presentó algún error en la trama. Contiene un ITU-T CRC (*International Telecommunication Union – Telecommunication Standarization Sector Cyclic Redundancy Check*) de 16 bits para tal propósito.

Para asegurar el éxito de las transmisiones, se usa CSMA-CA, un reconocimiento de *frames* y verificación de datos. Este estándar usa dos tipos de mecanismos de acceso al medio dependiendo de la configuración de la red.

1. Las PANs que no tienen habilitado un *beacon*, usan un mecanismo CSMA-CA sin *slots*. Cada vez que un dispositivo desea transmitir, espera durante un tiempo aleatorio. Si el canal está disponible después del tiempo que esperó, el dispositivo empieza a transmitir. Si el canal está ocupado después del tiempo de espera, el dispositivo espera otro tiempo aleatorio antes de intentar accesar de nuevo al canal.
2. Las PANs que tienen habilitado un *beacon* usan CSMA-CA con *slots* donde los *slots* de respaldo se alinean con el inicio de la transmisión del *beacon*. Los *slots* de respaldo de todos los dispositivos dentro de una PAN se alinean con el coordinador PAN. Cada vez que un dispositivo desea transmitir *frames* de datos durante el CAP (*contention access period*), localiza el límite del siguiente *slot* de respaldo y luego espera un número aleatorio de *slots* de respaldo. Si el canal está ocupado después de este período aleatorio, el dispositivo espera otro número aleatorio de *slots* de respaldo antes de intentar acceder al canal de nuevo. Si el canal está disponible, el dispositivo comienza a transmitir en el siguiente *slot* de respaldo disponible.

El uso de CSMA-CA permite que coexistan varios dispositivos en una misma vecindad, sin importar si son de otra red, otra tecnología o de la misma. El principio de esta técnica es “escuchar el medio” para saber si hay una transmisión en proceso o si el medio está disponible para transmitir y evitar las colisiones por múltiples intentos de transmisión simultáneas. Si cuando un dispositivo intenta comunicarse con el coordinador de su red el medio está ocupado, espera un tiempo aleatorio para revisar de nuevo y repite esta operación hasta 4 veces para accesar al medio o dejar de intentarlo y definir una falla de comunicación. Este método ha sido usado satisfactoriamente por años en las redes Ethernet y tiene la virtud de que no necesita sincronía entre los dispositivos.

PILA ZigBee

Como ya se mencionó, ZigBee define las dos capas superiores sobre el estándar IEEE 802.15.4, la capa de red y la de aplicación. La figura 3.7 nos muestra el detalle de las capas de la Pila de ZigBee.

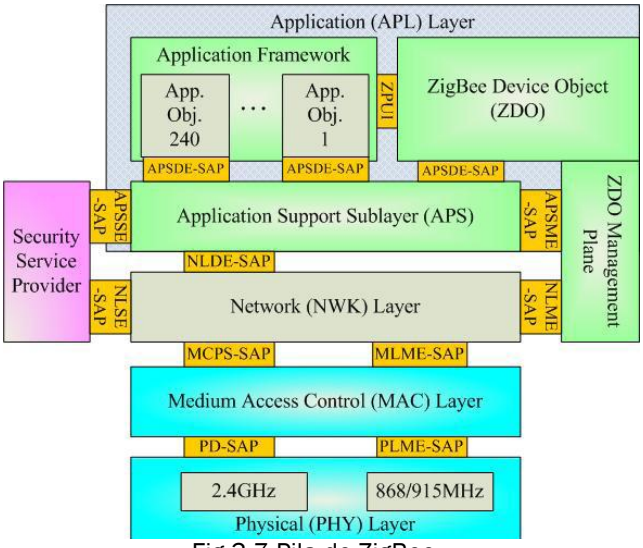

Fig 3.7 Pila de ZigBee.
Imagen tomada de "The Wireless Sensor Network for Home-Care System Using ZigBee"

La capa de red (NWK) es la responsable de iniciar la red, proporcionar la configuración de dicha red, unirse o abandonar una red, configurar un nuevo dispositivo, asignar la dirección a los dispositivos que se agregan a la red, rutea las tramas a los destinos asignados, agrega seguridad a las tramas de salida y se la quita a las tramas de terminación.

En general, la función principal de la capa de red es hacer que los datos lleguen a destino y, para ello, busca la mejor manera de hacerlo. La manera de hacerlo es que la capa de red selecciona un modo de operación apropiado para un nodo y determina cuáles son los vecinos más convenientes para asociarse y formar enlaces de comunicación. La topología de la red se actualiza cuando un nodo falla o cada determinado intervalo de tiempo para garantizar la conectividad de la red.

La capa de aplicación (APL) se encarga de enlazar dos dispositivos basados en sus servicios y necesidades así como reenviar los mensajes entre los dispositivos enlazados. Se encarga de asignar la función del dispositivo y descubre cuando un nuevo dispositivo se encuentra en el área de operación (POS, *personal operating space*).

Esta capa ofrece servicios de red y la funcionalidad en sí del nodo. En esta capa, se generan los datos a transmitir propiamente dichos. En general, el usuario no hace uso de la capa de aplicación en forma directa, sino que emplea una aplicación que es la que comunica con esta y elimina así la complejidad que podría producir.

DISPOSITIVOS QUE CONFORMAN UNA RED ZigBee

Los dispositivos que forman parte de las redes se clasifican en dos tipos con base en su funcionalidad; dispositivos de funcionamiento completo (FFD, *Full*

Function Device) y dispositivos de funcionamiento reducido (RFD, *Reduced Function Device*).

- Los dispositivos FFD pueden funcionar de tres maneras: como coordinador de la WPAN, como coordinador o como un dispositivo final.
- Los dispositivos RFD tienen capacidades y funcionalidad limitadas ya que están pensados en ser los sensores de la red.

Los primeros funcionan en cualquier topología; pueden comunicarse con cualquier dispositivo, tanto con RFD como con otro FFD; descubren la existencia de otros FFDs o RFDs en su vecindad para establecer la comunicación y típicamente usan la energía de la línea de alimentación del edificio.

Los dispositivos RFD están limitados a topología de estrella; son implementados con mínima memoria RAM y ROM; no pueden ser coordinadores de la red y sólo se pueden comunicar con un coordinador de red; sólo están asociados a un FFD coordinador a la vez; automáticamente buscan la red disponible en su alcance; envían información de la aplicación sólo si es necesario; determinan si hay datos pendientes; piden información al coordinador de la red y duermen durante largos períodos de tiempo para alargar la vida útil de las baterías. Los menores requerimientos de estos permiten que se usen circuitos integrados más baratos en su implementación.

Las redes deben tener por lo menos un FFD que funcione como coordinador de la red.

Esto nos lleva a establecer una segunda clasificación, con base en el trabajo que desempeñan en la red. La figura 3.8 nos muestra que, de acuerdo con su papel en la red, los dispositivos pueden clasificarse también como coordinadores (ZC, *ZigBee coordinator*), ruteadores (ZR, *ZigBee router*) y dispositivos finales (ZED, *ZigBee end device*).

- ZC. Es el dispositivo más completo ya que se encarga de controlar la red, coordinar a todos los nodos y almacenar la información de los mismos. Controla los caminos que deben seguir los dispositivos para comunicarse entre ellos. Requiere memoria y capacidad de computación.
- ZR. Interconecta los dispositivos dentro de la red.
- ZED. Es el elemento más simple, sólo puede comunicarse con un ZR o un ZC, es decir, sólo con un FFD. Este tipo de dispositivos tiene requerimientos mínimos de memoria. Puede estar dormido la mayor parte del tiempo, lo que aumenta la vida útil de las baterías. En este dispositivo quedan representadas las características principales de ZigBee: bajo consumo y bajo costo.

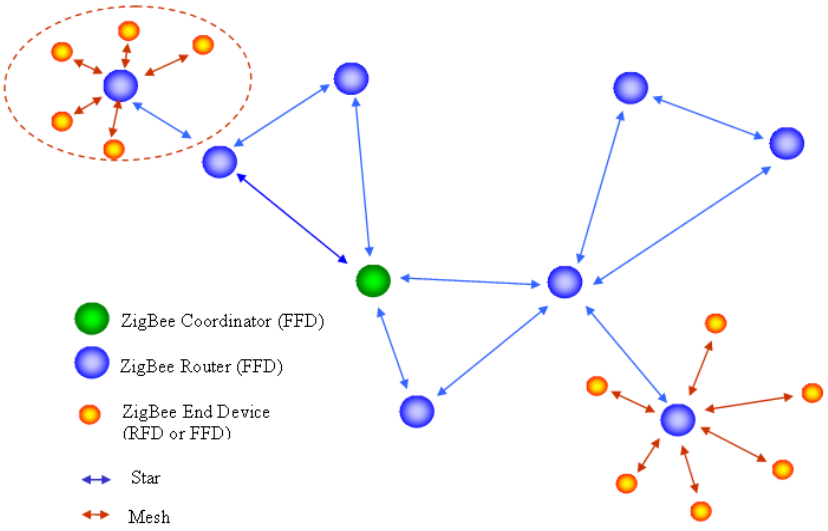

Fig 3.8 Elementos que conforman a una red ZigBee y su función en ella.
Figura tomada de "ZigBee technology: wireless control that simply works"

TOPOLOGIA DE LA RED

El estándar IEEE 802.15.4 define dos tipos de topología dependiendo de los requerimientos de la aplicación; topología estrella y topología punto a punto. Ambas configuraciones se muestran en la figura 3.9.

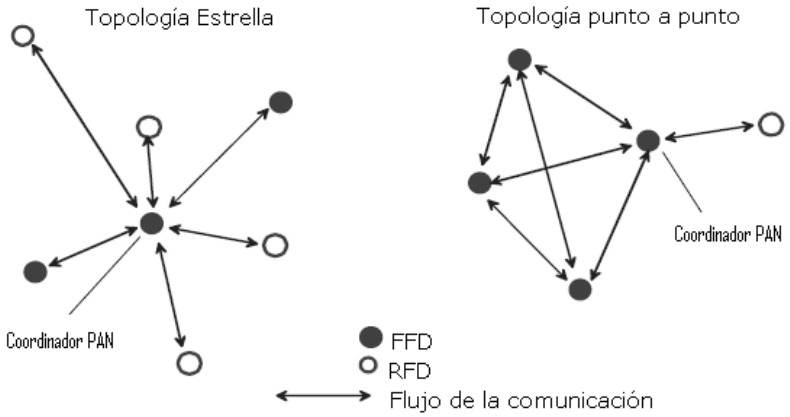

Fig 3.9 Topologías que se pueden presentar en una red ZigBee.
Como se muestra en IEEE 802.15.4-2006

En la topología de estrella la comunicación se da de los dispositivos a un coordinador central llamado coordinador PAN. Los dispositivos tienen aplicaciones específicas, pueden ser puntos de inicio o final de la red. El coordinador PAN también puede tener una aplicación específica pero se puede usar para iniciar, finalizar o enrutar la comunicación alrededor de la red. Las aplicaciones que se benefician de esta topología son las relacionadas con cuidado de la salud, automatización de hogares, equipo periférico de computadoras personales y juguetes.

Capítulo 3.

ZigBee.

La topología punto a punto también tiene un coordinador PAN, sin embargo, difiere de la topología en estrella en que en este caso los dispositivos pueden comunicarse entre ellos además de hacerlo con el coordinador PAN, siempre y cuando se encuentren en su rango de alcance. Este tipo de topología permite formaciones de red más complejas como la mesh. Aplicaciones como control y monitoreo industrial, redes de sensores inalámbricos, inventarios, rastreo de bienes y seguridad, se benefician con esta topología. Una red punto a punto puede ser del tipo ad-hoc, autoorganizable y autoconfigurable. También puede permitir múltiples saltos para enrutar la información de un dispositivo a cualquier otro dentro de la red. Dichas funciones se definen en la capa de red.

Todos los dispositivos que operen en cualquiera de las dos topologías deben tener direcciones únicas de 64 bits. Estas direcciones pueden ser usadas para comunicación directa dentro de la misma PAN. El coordinador PAN normalmente estará conectado a la alimentación eléctrica mientras que los dispositivos se alimentarán con baterías. La formación de las redes se determina en la capa de red que ya no forma parte del estándar sino de la aplicación de la propia tecnología ZigBee.

Usando estas dos topologías como "topologías base", podemos definir una tercera que se especifica en la capa de red de la pila de ZigBee: la topología *cluster tree.*

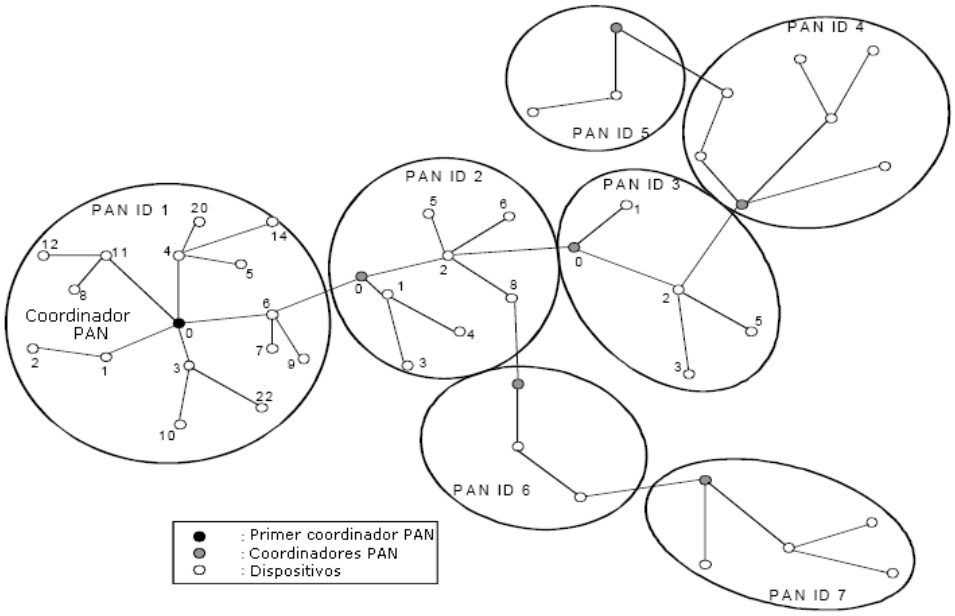

Fig 3.10 Topología cluster tree.
Como se muestra en IEEE 802.15.4-2006

Como vemos en la figura 3.10, en este tipo de red, la mayoría de los dispositivos son FFD. Los dispositivos RFD se conectan al final de la rama porque no permiten que otros dispositivos se asocien a ellos. Cualquier dispositivo de los FFD puede actuar como coordinador y proporcionar servicios de sincronización a otros dispositivos u otros coordinadores.

Sólo uno de estos dispositivos puede ser el coordinador PAN principal, el cual debe tener mayor cantidad de recursos computacionales que cualquier otro dispositivo de la red. El coordinador PAN forma el primer *cluster* escogiendo un identificador PAN disponible y transmitiendo tramas de *beacons* a los dispositivos vecinos. Un dispositivo que recibe la trama de *beacon* puede pedir permiso al coordinador PAN para unirse a la red. Si el coordinador PAN le permite al dispositivo que se una, suma al nuevo dispositivo como dispositivo hijo en su lista de vecinos; entonces el nuevo dispositivo integrado a la red, agrega al coordinador PAN como su padre en su lista de vecinos y comienza a transmitir *beacons* de manera periódica; otros dispositivos se pueden unir a la red a través de ese dispositivo. Si un nuevo dispositivo no se puede unir a la red a través de ese dispositivo, buscará otro dispositivo para que sea su padre.

El estándar también es responsable de controlar el flujo de información con *acknowledgement* y retransmisión de los paquetes, validación de la estructura y sincronización de la red. Los canales de acceso soportan un tamaño máximo de paquetes de 128 bytes con un *payload* de 104 bytes. La cantidad de nodos soportados (65 000 nodos) se da por las de direcciones de 64 bits definidas por el estándar y un direccionamiento corto de 64 bits más.

TRÁFICO EN LA RED

La subcapa MAC del estándar es flexible y permite tener diferentes tipos de configuraciones para definir el tráfico de la información en términos de la cantidad de datos y la frecuencia con la que se comunican los dispositivos:

- Cuando el dato es periódico: en este caso la aplicación dicta la proporción de la periodicidad. Los datos se manejan usando un sistema de *beacons* donde el sensor se despierta en un tiempo fijado previamente, revisa el *beacon* del coordinador PAN, si lo encuentra solicita su incorporación a la red, después de aceptada esta solicitud transmite la información y vuelve a dormirse; esto permite tener ciclos de trabajo muy bajos y asegurar una larga vida útil de las baterías.
- Cuando el dato es intermitente: en este tipo de tráfico la aplicación o algún estímulo externo determina la periodicidad, como el caso de un detector de humo. Los datos se pueden manejar sin *beacons* ya que el dispositivo sólo necesita conectarse a la red cuando tiene un evento que informar.
- Cuando el dato es repetitivo: la proporción se fija *a priori*, en este caso los dispositivos operan durante intervalos de tiempo fijos. Esta configuración usa un sistema de seguridad de asignación de *slots* de tiempo. Estas aplicaciones pueden usar la capacidad GTS (*guaranteed time slot*). Este es un método de QoS en las que se asigna un determinado tiempo en la supertrama a cada dispositivo para que haga lo que quiera sin tiempos de contención ni retrasos, de modo que no hay competencia por el medio ya que cada dispositivo tiene un tiempo asignado para la transmisión.

Capítulo 3.

ZigBee.

En el estándar IEEE 802.15.4 se definen dos tipos de estrategias para la comunicación entre los dispositivos: con balizas y sin balizas. Ya hemos mencionado que las redes ZigBee están pensadas para que los dispositivos finales conserven su energía y éstos puedan funcionar durante un largo tiempo. La estrategia para lograr este propósito es lograr que los dispositivos permanezcan "dormidos" la mayoría del tiempo, de tal manera que sólo se "despiertan" durante una fracción de segundo para comunicarse con otro dispositivo. Esta transición dura aproximadamente 15 milisegundos.

CON BALIZAS.

Este es un mecanismo que permite controlar el consumo de potencia de los dispositivos de la red. En este modelo, el camino de transmisión y recepción está permanentemente controlado por un distribuidor que se encarga de controlar el canal y dirigir las transmisiones. El distribuidor permite a todos los dispositivos saber cuándo pueden transmitir.

Las balizas se usan para sincronizar a todos los dispositivos que forman la red. Los intervalos de las balizas son asignados por el coordinador de la red y pueden variar desde 15 milisegundos hasta 4 minutos.

Los dispositivos que conforman la red "escuchan" a dicho coordinador durante el balizamiento, es decir, el envío de mensajes a todos los dispositivos. Cuando un dispositivo quiere intervenir primero tendrá que registrarse con el coordinador y ver si hay mensajes para él. En caso de que no los haya, el dispositivo vuelve a su estado de espera y se vuelve a despertar de acuerdo a un horario previamente establecido por el coordinador.

SIN BALIZAS.

Este mecanismo es autónomo porque se puede iniciar un intercambio de información y cualquier dispositivo puede intervenir en cualquier momento. Con este tipo de mecanismo puede ocurrir que cuando un dispositivo intenta comunicarse con el coordinador, el canal esté ocupado, produciéndose colisiones. Es por esto que se usa un mecanismo de control de acceso al medio, en este caso el estándar define que se haga mediante CSMA-CA.

Este mecanismo se usa típicamente en sistemas de seguridad, en los cuales los dispositivos "duermen" prácticamente todo el tiempo, sólo se despiertan para informar de un evento y en intervalos de tiempo predeterminados para informar al coordinador que siguen dentro de la red.

De acuerdo al estándar, existen tres tipos de transferencias de información:

- la primera es cuando un dispositivo envía información al coordinador
- la segunda es cuando un coordinador envía información a un dispositivo
- la tercera es cuando se presenta comunicación entre cualesquiera dispositivos.

Los mecanismos para cada tipo de transmisión dependen de si la red soporta la transmisión de balizas. Una red con balizas habilitadas se usa cuando se requiera ya sea sincronización o soportar dispositivos de baja latencia como periféricos de una PC. Si la red no necesita sincronización o soporte para dispositivos de baja latencia, se puede usar el mecanismo sin balizas.

Cuando un dispositivo desea enviar información a un coordinador en una red con balizas habilitadas, primero escucha la baliza de la red. Cuando encuentra dicha baliza, el dispositivo se sincroniza con la estructura de supertrama. En el momento apropiado, el dispositivo transmite su trama al coordinador usando CSMA-CA con slots. El coordinador puede enviar una respuesta de reconocimiento para avisar de una transmisión exitosa, si así se le requiere. Véase la figura 3.11.

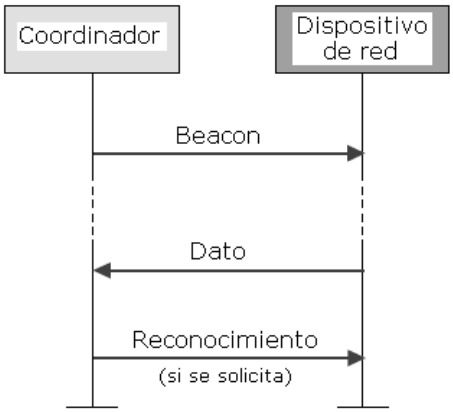

Fig 3.11 Comunicación con coordinador en una red con baliza.
Como se muestra en IEEE 802.15.4-2006

Cuando un dispositivo quiere comunicarse con un coordinador en una red sin baliza, simplemente transmite la trama de datos usando CSMA-CA con slots. El coordinador puede enviar, si así se le solicita, una trama de reconocimiento para avisar que la información llegó satisfactoriamente. Véase la figura 3.12.

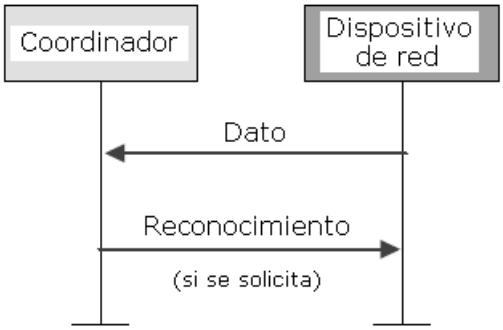

Fig 3.12 Comunicación con coordinador en una red sin baliza.
Como se muestra en IEEE 802.15.4-2006

Cuando el coordinador desea enviar información a una red con baliza, indica en la baliza de red que hay un mensaje pendiente. Como el dispositivo “escucha” al

beacon de la red, se da cuenta de que hay un mensaje pendiente, entonces transmite un comando MAC para solicitar la información usando CSMA-CA con s*lots*. El coordinador envía una trama de reconocimiento para avisar que ya le llegó la solicitud de información. La trama de datos se envía usando CSMA-CA con slots o, de ser posible, inmediatamente después de la trama de reconocimiento. El dispositivo puede enviar una trama de reconocimiento para avisar que la transmisión del dato fue exitosa. En este momento queda completada la transmisión de manera exitosa y entonces se borra el mensaje de la lista de mensajes pendientes. Véase figura 3.13.

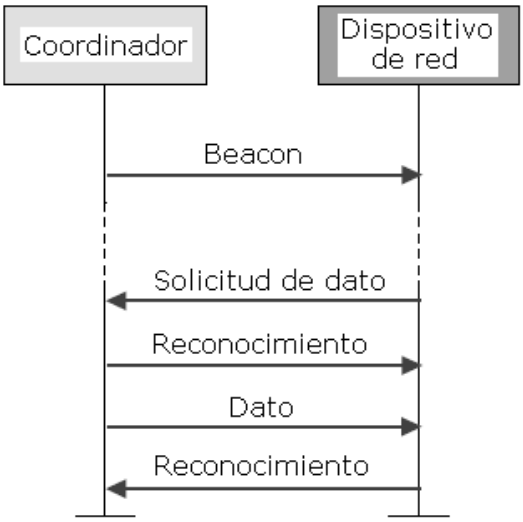

Fig 3.13 Comunicación del coordinador a un dispositivo en una red con baliza.
Como se muestra en IEEE 802.15.4-2006

Cuando el coordinador quiere enviar información a un dispositivo en una red sin baliza, almacena la información hasta que el dispositivo destino hace contacto con el coordinador y solicita la información. El dispositivo puede hacer contacto transmitiendo un comando MAC para solicitar la información, usando CSMA-CA sin s*lots*, a una tasa de aplicación definida. El coordinador reconoce la recepción de la trama solicitando el dato enviando una trama de reconocimiento. Si la trama del dato está pendiente, el coordinador transmite dicha trama al dispositivo usando CSMA-CA sin *slots*. Si no hay trama de datos pendiente, el coordinador informa de esto ya sea con una trama de reconocimiento inmediatamente después de la trama de solicitud de dato o con una trama de datos con un *payload* de longitud cero. Si se le solicita, el dispositivo envía una trama de reconocimiento para avisar de la recepción exitosa. Véase la figura 3.14.

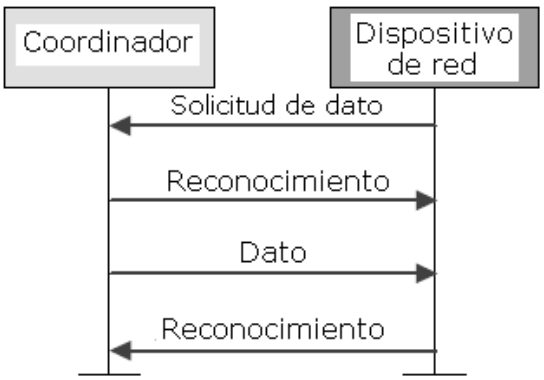

Fig 3.14 Comunicación del coordinador a un dispositivo en una red sin baliza.
Como se muestra en IEEE 802.15.4-2006

SEGURIDAD

El tema de la seguridad siempre es un tema delicado en cualquier sistema, en el caso de las comunicaciones inalámbricas se vuelve un punto importante porque al darse las comunicaciones en espacio abierto, siempre existe la posibilidad de que se presenten interferencias intencionales o interferencias inherentes a un sistema de comunicación de este tipo.

Los beneficios en cuestión de seguridad proporcionados por la subcapa MAC del estándar son:

- Control de acceso, hay una lista de dispositivos confiables de la red.
- Encriptación de los datos con un código simétrico avanzado de 128 bits.
- Integridad de la trama para evitar que algún dispositivo externo modifique los datos.
- Refrescamiento secuencial para registrar valores nuevos actualizados y rechazar las tramas que ya han sido transmitidas.

Sumado a esto, ZigBee proporciona una lista de control de acceso y paquetes de refresco así como paquetes *toolbox* que sirven para generar y distribuir claves para el acceso y comunicación entre dispositivos.

Las aplicaciones de seguridad permiten garantizar la integridad del mensaje protegiéndolo de ser modificado mientras viaja en el aire, permite tener un método de autentificación para asegurarse de que quien origina el mensaje es una fuente segura, refresco para evitar ataques por envíos dobles, proporciona privacidad contra receptores ajenos al sistema y guarda una base de datos de los dispositivos de la red que serán los únicos que puedan estar en comunicación.

La seguridad proporcionada por ZigBee define y da mantenimiento a las claves que pueden ser de red, de enlace y claves maestras. La primera de estas claves se encarga de proteger la infraestructura y los datos de los ataques de algún interferente externo; la segunda y la tercera proporcionan las bases para

proporcionar seguridad entre dispositivos. También define un modo de operación unificado/simple CCM. Usa un algoritmo AES de 128 bits.

SYSTEM ON CHIP

Como se ha mencionado, una de las grandes ventajas de los elementos que trabajan con ZigBee es la capacidad de tener elementos de bajo costo y poca complejidad. Los dispositivos de silicón SoC (*system on chip*) permiten satisfacer los criterios mencionados. En la figura 3.15 se ve uno de estos dispositivos y la figura 3.16 muestra el diagrama interno de uno de ellos.

La posibilidad de integrar un transreceptor de radio, una unidad de procesamiento de datos, una memoria y la aplicación definida por el usuario en un solo chip permite:

- alcanzar un bajo costo de manufactura
- corto tiempo de penetración en el mercado
- ocupar un espacio pequeño con pocos componentes
- facilidad de ensamblaje y pruebas
- diseños sencillos y confiables
- gran desempeño con bajo consumo de potencia debido a la interacción íntima de las funciones dentro del mismo chip minimizando de esta manera los gastos de energía.

Fig 3.15 Módulo transreceptor XBee ZNet 2.5
Imagen tomada de www.digi.com

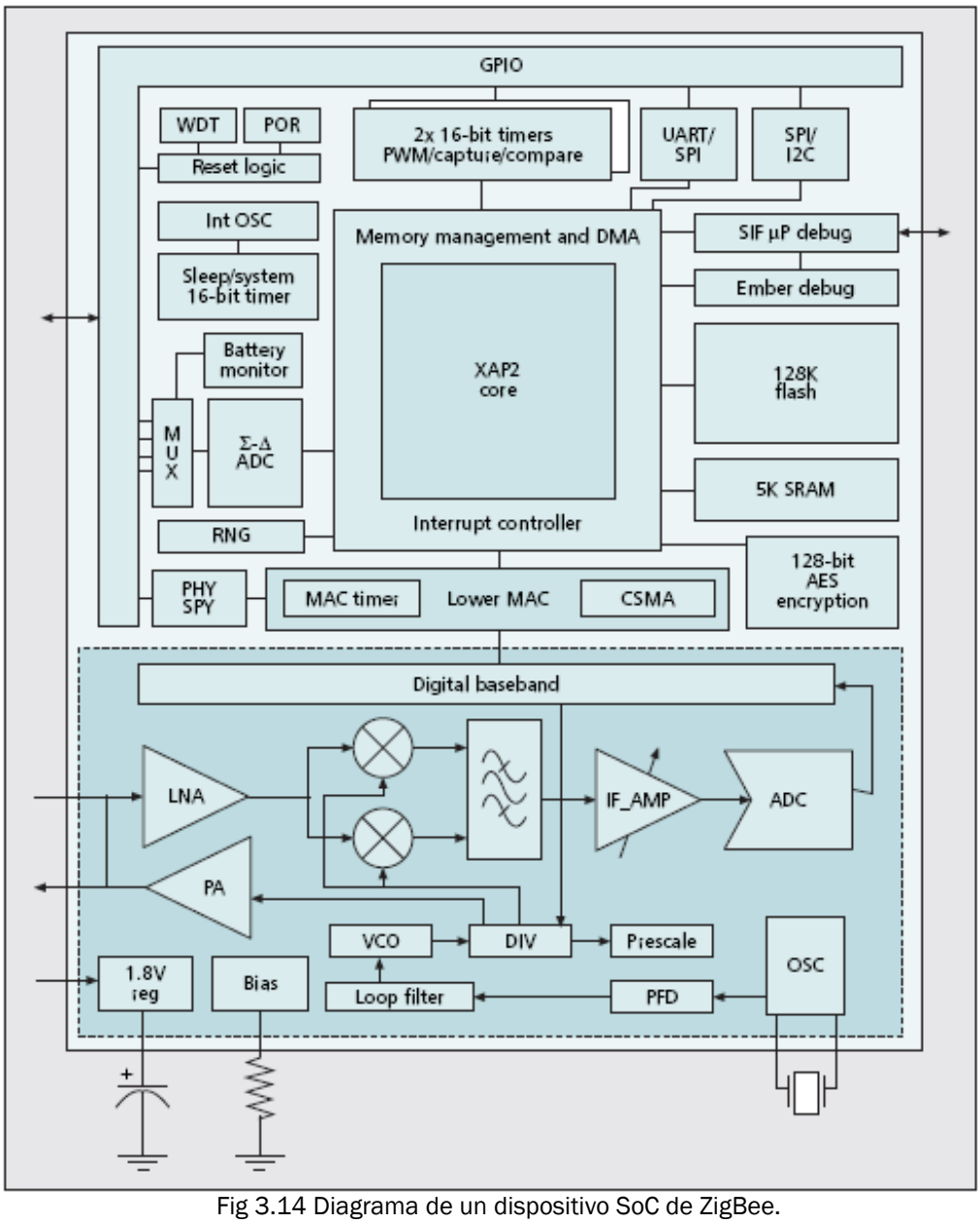

Fig 3.14 Diagrama de un dispositivo SoC de ZigBee.
Imagen tomada de "Commercial applications for wireless sensors networks using ZigBee".

El bajo costo de los materiales y un diseño simplificado para las transmisiones por RF que proporcionan los dispositivos SoC están ayudando a facilitar la adopción de esta tecnología.

VENTAJAS/DESVENTAJAS

A continuación se presentan puntos más específicos que nos ayudarán a ver por qué ZigBee es la tecnología adecuada. Cabe mencionar que todas las tecnologías son muy buenas, sólo hay que identificar el campo de aplicación donde las usaremos e identificar cuál es la más conveniente para ella.

Ventajas.

- un gran número de dispositivos
- cubre un área grande con la configuración adecuada
- larga vida útil de las baterías
- bajo nivel de interferencia derivado de las tasas de transmisión y las técnicas de comunicación
- bajo costo
- facilidad de instalación
- soporta diferentes topologías
- interoperabilidad entre diferentes fabricantes
- facilidad de lectura sin necesidad de línea de vista
- posibilidad de trabajar en cualquier parte del mundo al trabajar en la banda de 2.4 GHz.

Desventajas.

- corto alcance en la comunicación punto a punto
- tecnología nueva, lo que siempre presenta renuencia a su integración dentro de la vida cotidiana por parte del consumidor
- tasas de transmisión no muy elevadas.