EVALUACIÓN Y APLICACIÓN DE LA TECNOLOGÍA IEEE 802.15.4 EN EL TRANSPORTE DEL RITMO CARDÍACO COMO ENTRADA PARA UN SISTEMA DE COMUNICACIÓN AUTOMÁTICA

JOSÉ DARÍO ALEGRÍA JIMÉNEZ
OSCAR GILDARDO MUÑOZ MORALES

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2006

EVALUACIÓN Y APLICACIÓN DE LA TECNOLOGÍA IEEE 802.15.4 EN EL TRANSPORTE DEL RITMO CARDÍACO COMO ENTRADA PARA UN SISTEMA DE COMUNICACIÓN AUTOMÁTICA

JOSÉ DARÍO ALEGRÍA JIMÉNEZ
OSCAR GILDARDO MUÑOZ MORALES

Monografía para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director
Ing. Esp. GUEFRY LEIDER AGREDO MENDEZ

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2006

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ACRÓNIMOS

AES	Advanced encryption standard
AF	Application framework APDU Application support sub-layer protocol data unit
AIB	Application support layer information base
APL	Application layer APS Application support sub-layer
APSDE	Application support sub-layer data entity
APSDE-SAP	Application support sub-layer data entity – service access point
APSME	Application support sub-layer management entity - service access point
APSME-SAP	Application support sub-layer management entity – service access point
BPSK	Binary phase-shift keying
CAP	Contention access period
CBC-MAC	Cipher block chaining message authentication code
CCA	Clear channel assessment
CCM	CTR + CBC-MAC
CCM*	Enhanced counter with CBC-MAC mode of operation
CFP	Contention-free period
CRC	Cyclic redundancy check
CSMA-CA	Carrier sense multiple access with collision avoidance
CTR	Counter mode
DSSS	Direct sequence spread spectrum
ED	Energy detection
FCS	Frame check sequence
FFD	Full-function device
GTS	Guaranteed time slot
ISM	Industrial, scientific, and medical
KVP	Key-value pair
LQI	Link quality indicator
LR-WPAN	Low rate wireless personal area network
MAC	Medium access control
MCPS	MAC common part sublayer
MCPS-SAP	MAC common part sublayer-service access point
MFR	MAC footer
MHR	MAC header
MIC	Message integrity code
MLME MAC	Sublayer management entity
MLME-SAP	MAC sublayer management entity-service access point
MPDU MAC	Protocol data unit
MSB	Most significant bit
MSDU	Medium access control sub-layer service data unit
MSDU MAC	Service data unit
MSG	Message service type
NIB	Network layer information base
NLDE	Network layer data entity
NLDE-SAP	Network layer data entity – service access point
NLME	Network layer management entity
NLME-SAP	Network layer management entity – service access point
NPDU	Network layer protocol data unit
NSDU	Network service data unit NWK Network OSI Open systems interconnection
O-QPSK	Offset quadrature phase-shift keying

OSI	Open systems interconnection
PAN	Personal area network
PD-SAP	Physical layer data – service access point
PD-SAP PHY	Data service access point
PDU	Protocol data unit
PHR	PHY header
PHY	Physical layer
PIB	PAN information base
PLME	Physical layer management entity
PLME-SAP	Physical layer management entity-service access point
POS	Personal operating space
PPDU	PHY protocol data unit
PSDU	PHY service data unit
RFD	Reduced function device
RSSI	Received signal strength indication
SAP	Service access point
SFD	Start-of-frame delimiter
SHR	Synchronization header
SSP	Security services provider
WPAN	Wireless personal area network
WSN	Wireless Sensor Network
ZDO	ZigBee device object

INTRODUCCIÓN

En los últimos años se ha presentado el desarrollo de nuevas tecnologías que han permitido que se disminuyan los costos de producción en los chips, y al mismo tiempo que éstos sean cada vez más pequeños y eficientes en el uso de la potencia y sumado a la gran acogida de las redes Inalámbricas dan como resultado las Redes de Sensores Inalámbricas (WSN -*Wireless Sensor Network*), cuyas aplicaciones están enfocadas en entornos donde las tecnologías actuales no son tan viables principalmente por el tamaño de los dispositivos y consumo de potencia.

Las WSN son capaces de procesar información, recolectar datos del medio y transmitirla de manera inalámbrica, además de presentar unas tasas de transferencia menores, mayor duración de las baterías y la capacidad de formar redes de mayor tamaño.

Con el auge de estas redes, también han surgido nuevos estándares, en el momento el más conocido de ellos es el estándar ZigBee aprobado a finales del año 2004, el cual se basa en sus capas inferiores en el estándar IEEE 802.15.4 con lo cual es conocido con esté nombre.

ZigBee, tiene por objetivo cubrir nuevas áreas, específicamente las que comprende las comunicaciones en redes de área personal (PAN - *Personal Area Network*) pero pensado en el bajo consumo de potencia como principal objetivo. De acuerdo a las características que presenta ZigBee, un entorno de aplicación es el hospitalario, en el cual permite incorporar beneficios en el monitoreo constante para un mejoramiento de la calidad de vida y además contribuyendo con sus pequeños dispositivos a una mayor movilidad. Además ZigBee, esta proyectado como una tecnología de bajo costo con lo cual también ayudará a reducir costos dentro del entorno hospitalario.

La presente monografía desarrolla un piloto que consiste en simular con software el ritmo cardíaco mediante un ECG y en el momento que se presenten trastornos en él realizar una comunicación inalámbrica mediante tarjetas que soporten el estándar ZigBee a un sistema de conmutación automática implementado con software libre (con el propósito de reducir costos para aumentar la viabilidad de la introducción en el uso), que genera una comunicación para enrutar (localizar y dar aviso) a quien corresponda.

Esta comunicación consiste en dar aviso mediante mensajes audibles pregrabados sobre cual paciente necesita atención (ubicación) y de que clase, automatizando el proceso y volviéndolo mas ágil, alcanzando de está manera una atención efectiva y una disminución de fatalidades en momentos en que está en

juego la vida, de esta manera, contribuyendo al desarrollo y mejoramiento en la asistencia integral de los pacientes.

Con el fin de abordar los temas necesarios para el desarrollo de esta Monografía, el contenido consta de 5 capítulos que se distribuyen de la siguiente manera:

Capitulo 1. Redes de Sensores Inalámbricas. Se realiza una clasificación de las redes de sensores; se describen las características y protocolos empleados. También se describen aplicaciones y estándares que se pueden incluir dentro de estas redes.

Capitulo 2. Estándar ZigBee. Se detalla las capas que conforman el estándar: física, MAC, red y aplicación, sus primitivas y principales características.

Capitulo 3. Criterios dentro de un Entorno Hospitalario. Se realiza unos criterios para realizar una red con Zigbee, los dispositivos que se puedan utilizar, y el análisis capa por capa del estándar.

Capitulo 4. Descripción de la aplicación y pruebas realizadas. Se realiza la descripción de la aplicación tanto el módulo transmisor y para el módulo receptor, además se hacen pruebas de algunos parámetros del estándar IEEE 802.15.4.

Capitulo 5. Conclusiones y recomendaciones. Se realiza el análisis de los resultados obtenidos, y posibles trabajos futuros .

1. REDES DE SENSORES INALÁMBRICAS

En la actualidad existen campos emergentes dentro de las redes inalámbricas que ofrecen una gran oportunidad de ampliar el panorama en nuevas aplicaciones, unos de estos campos son las WSN, que gracias a la rápida convergencia de tres tecnologías : microprocesadores, comunicaciones inalámbricas y sistemas electro-mecánicos (MENS - *Micro Electro-Mechanical Systems*), permite que esté tipo de tecnología ser viable en aplicaciones militares, médicas, domóticas, e industriales entre otras [1].

Una WSN esta formada principalmente por pequeños nodos sensores que poseen características de bajo consumo de potencia y tienen como objetivo monitorizar y recolectar datos en un ambiente sin intervención humana, realizar un procesamiento local y transmitirlos hacia su destino final.

Este tipo de redes ofrecen muchísimas ventajas en comparación con las redes tradicionales, como una arquitectura flexible en grande escala, datos detectados de alta calidad, y mecanismos para que las aplicaciones sean adaptables de acuerdo al ambiente, y desventajas como recursos limitados en memoria, limitado en ancho de banda y tamaño de paquetes entre otras.

En este capitulo se da un pequeño análisis sobre las WSN, sus componentes, protocolos, características y aplicaciones, especialmente lo relacionada en aplicaciones médicos.

1.1 COMPONENTES DE WSN [2] [3] [4]

Una red de sensores es una herramienta para transmitir constante o periódicamente datos sobre un determinado fenómeno en un ambiente a un observador para poder tomar determinaciones dentro de los límites de desempeño deseado y con el mejor costo/beneficio posible. Para realizar esta tarea una red de sensores esta compuesta principalmente por: nodos sensores, observador y fenómeno. Además pueden existir componentes secundarios que recolectan la información generada por la red para ser enviada a través de Internet a una base de datos y al observador, como lo muestra la figura 1.1

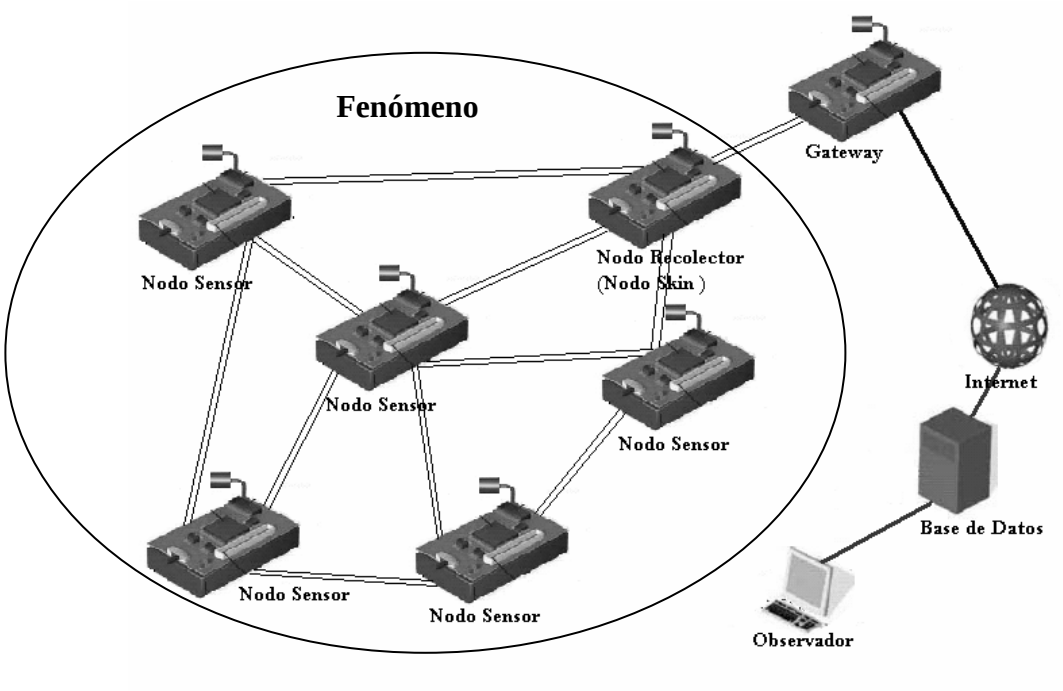

Figura 1.1 Componentes de una Red de Sensores

1.1.1 Nodo Sensor

Es el dispositivo encargado de monitorear, capturar y transmitir los cambios presentados en el fenómeno de acuerdo a parámetros establecidos. Existen diferentes clases de nodos sensores[1], los cuales se pueden usar de acuerdo a la necesidad y la aplicación a implementar. Un nodo sensor, consiste típicamente en cinco componentes: Transmisor/Receptor (transceptor), Memoria, Unidad de Potencia, Microcontrolador y el Sens*or* como lo muestra la figura 1.2. Además de monitorizar los cambios presentados, los nodos sensores también sirven de puente para recibir información de otro nodo y trasmitirla a su destino.

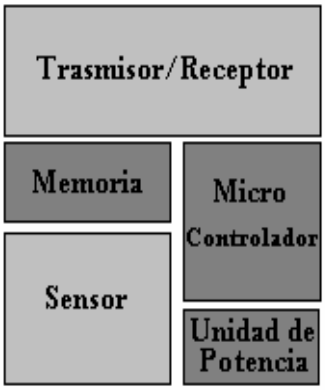

Figura 1.2 Nodo Sensor [2]

[1] En el transcurso del documento también es llamado dispositivo o simplemente nodo.

La unidad de comunicación (transceptor) es la responsable de realizar el enlace entre los nodos sensores, este puede ser de forma infrarroja, óptica o RF. La mayoría de los fabricantes de nodos sensores utilizan la comunicación en radiofrecuencia en las banda Industrial, Científica y Médica (ISM *Industrial, Scientific and Medical*) por ser gratuitas en la mayoría de los países.

La unidad de procesamiento (microcontrolador) es la encargada de ejecutar los algoritmos, los protocolos de comunicación y todo el procedimiento que permite el control de los nodos sensores, además deben economizar el máximo de energía posible en virtud de la limitación de está . El microcontrolador no interfiere directamente en el funcionamiento del sistema operativo, sólo su arquitectura debe ser compatible con las características del nodo sensor.

La memoria es la encargada de dar soporté al microcontrolador para almacenar algoritmos y aplicaciones, es decir, almacena el propio núcleo del sistema operativo, los programas de usuario y sus datos. Las tecnologías de memoria más usadas son a Flash y la Memoria de solo lectura estática (SRAM - Static Random Access Memory).

La unidad de sensores generalmente está compuesta por los sensores y el conversor de señales analógica/ digital (ADC – Conversor Digital Análogo). Todas las señales captadas por los sensores son análogicas y convertidas en señales digitales mediante el ADC para ser procesadas por el microcontrolador. Existen diversos tipos de sensores, entre ellos, de luz, temperatura, presión, humedad etc. En la tabla 1.1 presenta una lista de algunos nodos sensores comerciales.

Tabla 1.1 Nodos de sensores comerciales [3]

Nodo Sensor	Radio	Procesador	S.O	Memoria
BTNode	Ericsson ROK (101 007) ATMega128L TinyOS 64KB	Ericsson ROK (101 007)	ATMega128L	64kB
µAMPS	LMX3162	StrongARM (SA-1100)	Red Hat and eCOS	512KB (Flash)
WINS	Connexant RDSSS9M	StrongARM (SA-1100)	µC/OS-II	4MB (Flash)
PicoNode	Propietario	DW8051	N/A	N/A
PushPin	IrDA Transceiver 83F8851	Cygnal C8051F016	Bertha	N/A
GNOMES	Bluetooth o 900MHz	MSP430F149	N/A	32KB
Eyes	TR1001	MSP430F149	PeerOS	8Mbit
WeC Mote	TR1000	AT90LS8535	N/A	32KB
Mica Mote TR1000	ATMEGA	103L	TinyOS	512KB (Flash)

Mica2 Mote	CC1000	ATMEGA 128L	TinyOS	4Mbit (Flash)
Telos b	CC2420	MSP430F149	TinyOS	4Mbit (Flash)
Nymphs	CC1000	ATMega128L	Mant isOS	64KB (EEPROM)
ESB	TR1001	MSP430F149	N/A	8KB (EEPROM)
Medusa MK-2	TR1000	ATMega128L ARM THUMB	N/A	1MB (Flash)
IBage	TR1000 Bluetooth	ATMega103L	N/A	N/A

La unidad de potencia es la encargada de suministrar la energía necesaria para que el nodo funcione correctamente, por lo general son dos pilas (baterías) doble AA. Las baterías son clasificadas generalmente en miliamperios por hora. En la práctica esto no es así, puesto que el voltaje y los niveles de corriente varían de acuerdo con las necesidades de consumo por lo tanto no es simple calcular su duración. Son construidas comúnmente de Litio, Níquel o metales alcalinos.

1.1.2 Observador

Es el usuario final interesado en conseguir la información suministrada por la red de sensores en relación a un fenómeno. Puede realizar consultas a la red y recibir respuestas de estas. Además, pueden existir, simultáneamente observadores múltiples en la red de sensores.

1.1.3 Fenómeno

Es la entidad de interés para el observador, que esta siendo monitorizada y cuya información será analizada/filtrada por la red de sensores. Se pueden observar múltiples fenómenos simultáneamente. El observador está interesado en monitorizar el comportamiento del fenómeno bajo algún requisito de desempeño específico.

1.1.4 Nodo Recolector de Datos

Es un nodo responsable de ir recibiendo, almacenando y procesando los datos desde los nodos sensores. Esté nodo también es conocido como estación base[2] . La mayoría de veces es usado como coordinador de la red para los diferentes protocolos empleados y aplicaciones desarrolladas.

[2] La estación base también es conocida como sink

1.1.5 Gateway

Nodo utilizado para la interconexión entre la red de sensores y una red con el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP *Transmission Control Protocol/ Internet Protocol*), en muchas ocasiones este nodo también es el nodo recolector.

1.2 CLASIFICACIÓN

La clasificación de una WSN depende principalmente de la aplicación y con ello del objetivo a tratar. La aplicación influye directamente en las funciones ejercidas por los nodos sensores, en la cantidad y distribución; además, en el tipo de servicio que proveerá la red, el tipo de datos a tratar y características ambientales donde se desarrollara. Las WSN pueden ser clasificadas según su configuración, recolección de datos por medio de los sensores y el tipo de comunicación empleada, como lo muestra la tabla 1.2.

Tabla 1.2 Clasificación de las redes de sensores [5]

Configuración.		
Composición.	**Homogénea**	Cuando todos los nodos presentan una misma capacidad de hardware, pero pueden ejecutar diferente software
	Heterogénea	Cuando todos los nodos no presentan la misma capacidad de hardware.
Organización	**Jerárquica**	Cuando los nodos están divididos en grupos y cada grupo tiene una líder.
	Planas	Cuando los nodos no están divididos en grupos
Movilidad	**Estática**	Todos los nodos permanecen en el mismo sitio.
	Dinámica	Los nodos son cambiados periódicamente.
Densidad	**Balanceada**	Los nodos presentan una concentración distribuida de acuerdo a la aplicación en el área determinada.
	Densa	La concentración de nodos es alta de acuerdo a la aplicación en el área determinada.
	Esparza	Los nodos presentan una concentración no homogénea de acuerdo a la aplicación en el área determinada.
Recolección de Datos por los Sensores		
Periódico	Los nodos recogen los datos en intervalos regulares de tiempo.	
Continuo	Los nodos recogen datos continuamente.	
Relativo	Los nodos recogen datos cuando ocurren eventos de interés o solicitados por el observador.	
Tiempo real	Los nodos recogen la mayor cantidad de datos en el menor intervalo de tiempo.	
Comunicación Empleada.		
Tipo de conexión	**Simétrica**	Todas las conexiones existentes entre los nodos, tienen el mismo alcance.
	Asimétrica	Las conexiones no tienen el mismo alcance.
Transmisión	**Simplex**	Los nodos sensores tienen un transceptor que permite transmisión de información en un solo sentido.
	Half-duplex	Los nodos sensores tienen un transceptor que permite transmisión de información en dos sentidos pero no al mismo tiempo.
	Full-duplex	Los nodos sensores tienen un transceptor que permite transmisión de información en ambos sentidos al mismo tiempo.

Ubicación del canal	**Estática**	El ancho de banda que maneja cada nodo esta dividida en partes iguales de frecuencia (FDMA), tiempo (TDMA), espacio (SDMA), en código (CDMA), ortogonal (OFDM), para evitar interferencia.
	Dinámica.	Cada nodo sensor disputa el canal de comunicación para la transmisión de los datos.
Flujo de información.	**Flooding**	El nodo sensor realiza broadcast a sus vecinos, para que ellos a su vez lo realicen hasta alcanzar el destino.
	Multicast	En este tipo de red se forman grupos y usan el multicast para la comunicación entre los miembros del grupo.
	Unicast	En este tipo de red, los sensores pueden comunicarse directamente con el punto de acceso usando protocolos de multi-saltos.
	Gossiping	En este tipo de red, los sensores seleccionan los nodos a cuales envían los datos.
	Bargaining	Solo envían los datos si el destino los quiere recibir.

1.3 ARQUITECTURA

Las WSN tienen características especiales, por lo cual los protocolos empleados en su arquitectura deben ser desarrollados de acuerdo a sus necesidades y limitaciones. El estudio de estos protocolos es realizado en capas TCP/IP como lo muestra la tabla 1.3

Tabla.1.3 Protocolos en WSN

Protocolos de WSN		
CAPAS	**Física**	Tx en RF, óptico o infrarrojo
	Enlace	S-MAC, T-MAC, B-MAC,DE-MAC, TRAMA
	Red	DD, SPIN, SAR, MULTI, STORM, PROC, TinyBeaconing, LEACH,TEEN, PEGASIS, ICA, GEOMOTE, GEAR, GPSR
	Transporte	PFSQ, ESRT, RMST

1.3.1 Capa Física

En una WSN pueden existen tres posibilidades para la comunicación inalámbrica: óptica, infrarrojo y radiofrecuencia (RF) [1] [6].

La comunicación óptica consume menor cantidad de energía por bit transmitido y no requiere área física para instalación de antena, pero necesita de línea de vista (LOS *Line of Sight*) para la comunicación y esta es direccional y sensible a las condiciones atmosféricas.

La comunicación a través de infrarrojo usualmente también es direccional y tiene un alcance máximo de un metro. La ventaja de esta comunicación, también radica en que no se necesita área física para la antena. En la actualidad, aún no existen en el mercado dispositivos que utilicen este tipo de comunicación. En la actualidad nodos con comunicación óptica e infrarroja no se han existen el mercado.

La comunicación en RF basada en ondas electromagnéticas es uno de los mayores desafíos en este tipo de comunicaciones, debido al uso de antena y al

alto consumo de potencia que representa. Las ventajas de la comunicación en RF son la facilidad de uso, la aceptación comercial, penetran en edificios sin problema, de modo que se utilizan mucho en la comunicación tanto en interiores como en exteriores, son omnidireccionales, lo que significa que viajan en todas las direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse físicamente etc. Todas estas características hacen de este tipo de comunicación viable para la plataforma de los sensores. El alto consumo de potencia se puede controlar con los modos de operación del nodo sensor: escucha (*listen*) y dormido (*sleep*), de aquí en adelante cuando se hable de estos modos serán en escucha y dormido respectivamente.

1.3.2 Capa de Enlace de Datos

Los requisitos de la capa de enlace de datos difieren de acuerdo a la clasificación de las WSN. Por ejemplo, existen redes donde los nodos pueden permanecer con los transceptores inactivos por largos perıodos de tiempo y repentinamente se activan cuando algún cambio del fenómeno observado es detectado, también pueden haber varios nodos en el área determinada del evento que están monitorizando el medio al mismo tiempo para transmitir los datos, esto sumado a las características particulares de las WSN, causan que el Control de Acceso al Medio (MAC - *Medium Access Control*) sea diferente del tradicional [4].

En una red de sensores inalámbricos el protocolo MAC debe alcanzar dos objetivos: el primero es la creación de la infraestructura de red, como son gran cantidad de nodos sensores los que van a formar la red y estos están densamente posicionados en el campo de aplicación el protocolo MAC debe establecer enlaces de comunicación para la transferencia de los datos; el segundo es compartir de forma eficiente y justa los recursos de comunicación entre los nodos sensores para un uso moderado de la potencia y así lograr conservarla al máximo. Para el acceso al medio los protocolos se pueden dividir en [7]:

- Contienda: son los protocolos basados en la ubicación dinámica del canal, utiliza el modelo CSMA (Carrier Sense Multiple Access) y sus derivaciones (CSMA/CD, CDMA/CA),
- Arbitraje: son los protocolos que se basan en ubicación estática del canal TDMA y FDMA, transmiten sus datos en momentos determinados, evitando colisiones.
- Híbridos: son los protocolos basados en contienda, pero que utilizan los de arbitraje para saber cuando su vecino está por recibir datos. Algunos protocolos son S-MAC y T-MAC.

1.3.2.1 Protocolos

A continuación se detallan brevemente los protocolos más comunes para el acceso al medio en redes WSN [1] [6] [7] [8].

- **S-MAC**

.

El protocolo Sensor-MAC (S-MAC *Sensor-MAC*) está destinado a redes con aplicaciones dirigidas a eventos, con toma periódica de datos, baja latencia y baja tasa de envió de mensajes. La comunicación entre los nodos sigue un flujo broadcast o un flujo unicast para el intercambio de mensajes. Este protocolo obtiene considerable reducción en el consumo de potencia, prolongando el tiempo de vida de la red.

Para que el consumo de potencia por parte de los nodos sea bajo en el protocolo S-MAC, la red debe ser homogénea y evitar los principales eventos responsables del consumo innecesario de potencia como las colisiones, el número de paquetes de control (overhead), que los nodos escuchan transmisiones de paquetes destinados a otros nodos (overhearing),y que escuchan el medio cuando no existe tráfico (Idle listening).

Para las colisiones, S-MAC utiliza la misma técnica de lEEE 802.11, la Función de Coordinación Distribuida (DCF *Distributed Coordination Function*) que emplea un dialogo de comunicación RTS-CTS-DATA-ACK. Este dialogo de comunicación evita colisiones, problemas de terminal escondido y problema de estación expuesta. En caso que la colisión ocurra utiliza un algoritmo para aguardar un tiempo aleatorio el Backoff Exponencial Binario (BEB *Binary Exponential Backoff*) para volver a participar por el canal.

S-MAC reduce el número de paquetes de control para disminuir el tráfico en la red y utiliza un ciclo de operación reducido con tiempos fijos de escucha y de reposo, donde el tiempo de actividad es menor que el tiempo de reposo (cerca de un 10%) para evitar que los nodos escuchan el medio sin trafico en la red.

Para evitar que los nodos escuchan transmisiones de paquetes destinados a otros, el protocolo S-MAC coloca el radio en modo dormido cuando verifica que el paquete no esta destinado para él y se pone rápidamente en modo escucha cuando detectan cierto fenómeno.

La señalización para los paquetes de control y de sincronización es realizada dentro del canal, enviando un paquete de sincronización (SYNC) en broadcast para todos sus vecinos. S-MAC emplea la técnica de mensaje momentáneo (*message passing*) para reducir la latencia durante aplicaciones que requieren almacenamiento de información para procesamiento en la red (in-network). Esta

técnica permite la transmisión de mensajes largos, que son divididos en pequeños fragmentos y enviadas en intervalos**.**

- **B-MAC**

El protocolo Berkeley-MAC (B-MAC- *Berkeley Medium Access Control*) se encuentra disponible desde la version 1.13 de TinyOS y busca obtener:

- Bajo consumo de operación.
- Efectiva evasión de colisiones.
- Implementación simple, por consiguiente bajo uso de memoria física.
- Utilización efectiva de canal tanto para tasas de transmisión pequeñas y altas.
- Que sea reconfigurable por protocolos de red.
- Tolerancia a cambios en las condiciones de la red como del medio.
- Escalable a un gran número de nodos.

Para evitar colisiones B-MAC utiliza el método Valoración del Canal Libre (CCA *Clear Channel Assessment*), que identifica si en el canal existen transmisiones en el momento por medio del indicador de intensidad de la señal recibida (RSSI *Received Signal Strenght Indicator*). Este indicador muestra periódicamente la señal recibida cuando no existe tráfico en la red, para determinar el ruıdo base. Si la señal recibida es superior al ruıdo base, el protocolo detecta una transmisión en marcha.

- **TRAMA**

El protocolo de Acceso Múltiple Adaptativo de Trafico (TRAMA *Traffic adaptive Multiple Access*) es basado en Acceso al Medio por División de Tiempo (TDMA *Time Division Multiple Access*) y proyectado para aplicaciones dirigidas a eventos con transmisión continua o periódica de datos. El objetivo principal de esté es ser eficiente en el consumo de potencia y el método de acceso al canal garantiza que no existen colisiones en comunicaciones unicast, broadcast o multicast. TRAMA se adapta al tipo de tráfico y emplea un algoritmo distribuıdo de elección, él cual determina cual nodo puede transmitir en determinado intervalo de tiempo y no hace reserva para los nodos que no tienen datos para enviar. El algoritmo de elección está basado en informaciones de tráfico de cada nodo y selecciona receptores basados en tablas anunciadas por los transmisores. Las tablas son obtenidas por el intercambio de informaciones locales de los vecinos de dos saltos y son transmitidas para especificar cuáles nodos seran los respectivos receptores de su tráfico en orden cronológico. TRAMA alterna entre accesos aleatorios y escalonados para adaptar cambios de topologías, permitiendo adicionar nodos en la red y tolerar fallos. El protocolo consiste de tres componentes:

- Protocolo de Vecino (NP *Neighbor Protocol*): responsable por la propagación y actualización de informaciones sobre sus vecinos de un salto. Las actualizaciones son incrementales y permiten determinar el conjunto de vecinos que serán añadidos o removidos.
- Protocolo de intercambio secuencial (*SEP Schedule Exchange Protocol*): permite que los nodos intercambien información y tablas de los vecinos de dos saltos
- Algoritmo de elección adaptativo (AEA *Adaptive Election Algorithm*): utiliza las informaciones de la vecindad y de las tablas para seleccionar los transmisores y receptores para el intervalo de tiempo actual, mientras en los otros nodos seleccionan el modo de reposo.

- **T-MAC**

El protocolo Time out - MAC (T-MAC *Time-Out-MAC*) fue desarrollado para aplicaciones dirigidas a eventos que poseen una baja tasa de entrega de mensajes, baja latencia, con transmisión continua o periódica de datos y está basado en protocolos de contienda. El objetivo de T-MAC es contribuir al bajo consumo de energía, considerando las limitaciones del hardware del nodo y los patrones de comunicación en el cambio de mensajes entre vecinos y el nodo y la estación base . El ciclo de operación es reducido y posee dos tiempos de actividad en escucha y reposo, que se adaptan a la carga de la red, los cuales son obtenidos por la implementación de un temporizador que desconecta la radio al verificar que no existen transmisiones durante un intervalo de tiempo, como lo muestra la figura 1.3.

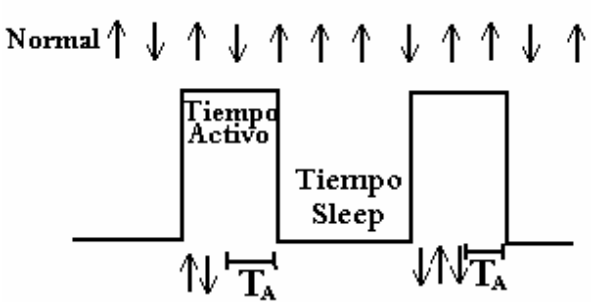

Figura 1.3 Protocolo T-MAC [1]

La idea principal de T-MAC es reducir el tiempo de idle listening para disminuir el consumo de energía del nodo. Los mensajes recibidos durante el tiempo de reposo son almacenados y transferidos en intervalos en el inıcio del tiempo activo.

El nodo escucha la red, transmite y recibe datos durante su tiempo activo. El temporizador determina el final del tiempo activo cuando no ocurren eventos durante un tiempo determinado (T_A). La activación por eventos ocurre por: inıcio periódico del modo activo (como lo muestra la figura 1.5); recepción de datos en la

radio; final de la transmisión de sus vecinos; final de la transmisión de su propio paquete de datos o recepción de un ACK; o por detección de la señal de radio RSSI. Los nodos se comunican por medio de los comandos RTS-CTS-DATA-ACK para evitar colisiones y obtener transmisiones confiables. Un problema encontrado en la T-MAC se presenta cuando un nodo esta inactivo y otro tiene mensajes para él. Este es conocido como el problema de dormir pronto. Este problema puede ser resuelto de dos maneras:

- Un nodo escucha un paquete CTS destinado a otro, é inmediatamente envía a sus vecinos un paquete de FRTS (Futuro RTS) para que no pase a modo dormido;
- Usar un esquema para priorizar el vaciado del buffer cuando este estuviera cerca de su capacidad límite. Un nodo al recibir un RTS no trasmite un CTS, sino, transmite los mensajes almacenados en su buffer para el destino.

- **DE-MAC**

El Energía Distribuida - MAC (DE-MAC *Distributed Energy aware MAC*) es un protocolo empleado para gestionar y balancear la energía en redes WSN. Este protocolo emplea Acceso al Medio por División de Tiempo (TDMA *Time Division Multiple Access*), y por lo tanto esta libre de colisiones y de overhead . Utiliza dos tipos de operación: en escucha y reposo para evitar el consumo de potencia en el overhearing y el idle listening.

DE-MAC establece que los nodos con baja energía deben ser usados con menor frecuencia en el enrutamiento y para eso realiza un procedimiento local de elección de nodos con baja energía para que se queden más tiempo en reposo que sus vecinos.

1.3.3 Capa de Red [1] [6] [8] [9]

En WSN como en las otras redes, está capa tiene la tarea de realizar el enrutamiento de los datos, pero con la diferencia que en las redes tradicionales sus protocolos tienen interés en reducir el retardo de transmisión entre origen - destino y aumentar el flujo de los datos, mientras que en las redes WSN los protocolos deben establecer rutas que aumenten el tiempo de vida de la red racionalizando el consumo de potencia por encima de otras métricas de desempeño, por lo tanto se piensa en protocolos eficientes en potencia, además como el direccionamiento para redes WSN no se puede hacer como en la redes tradicionales donde cada nodo posee una dirección única global que a su vez le sirve como su identificador, porque el costo de una dirección única global en redes con poco consumo de potencia puede ser elevado si la dirección en sí representa la mayoría de los bits trasmitidos, también se piensa en protocolos centrado en los

datos donde el direccionamiento tradicional es remplazado por el direccionamiento basado en atributos.
En el primer protocolo las rutas son definidas de acuerdo a criterios como mayor potencia disponible, menor consumo de potencia, menor número de saltos o una combinación de las alternativas anteriores; en el segundo las rutas se definen con base en los datos que envía un nodo para saber determinada información y los datos que poseen los nodos de la información solicitada.

El direccionamiento basado en atributos se basa en los externos a la topología y relevantes para la aplicación, es decir los usuarios están más interesados en preguntar un atributo del fenómeno antes que preguntar a un nodo determinado. En este esquema, son utilizados para describir o nombrar un dato e identificados por descripciones únicas que son distribuidas por la estación base.

Existen otros direccionamientos que atienden las restricciones de las WSN considerando sus particularidades como el direccionamiento espacial donde las consultas son realizadas con el objetivo de extraer datos de una región o de cualquier nodo capaz de detectar un determinado evento que puede responder a esa consulta, este direccionamiento se hace basado en la posición o localización geográfica, sin embargo, el tamaño de la dirección (codificación de las coordenadas geográficas) depende de factores como la granularidad (precisión) de la localización, del tamaño de la región monitorizada y de la cantidad de nodos a direccionar, factores que dificultar la escalabilidad de este esquema haciendo la dirección muy grande en relación a los datos que están siendo transmitidos.

1.3.3.1 Enrutamiento

El enrutamiento puede ser dividido en tres categorías: plano, jerárquico y geográfico. En el enrutamiento jerárquico los nodos forman grupos (clusters) y algunos nodos son designados líderes (clusterhead). Dentro de cada grupo la comunicación sólo es entre el nodo líder y los demás nodos. Pueden existir agrupaciones de líderes, formando un nivel más alto en la jerarquía y por lo tanto existirá otro líder para este nivel. En cada nivel, el líder recibe las informaciones enviadas por los otros nodos; al reunir todos los datos, el nodo líder transmitirá esas informaciones a otros líderes. De esta forma la información alcanza el usuario final, generalmente una estación base. Los desafíos presentes en este tipo de topología son la elección del líder en un ambiente distribuido y la configuración de la jerarquía para evitar el consumo de potencia excesivo en algunos nodos de la red.

En el enrutamiento plano, cada nodo está conectado a otros nodos, que se comunican entre sí. No existen nodos líderes por donde la comunicación debe siempre pasar. Los nodos son responsables por reunir y enrutar los mensajes. En esa topología puede haber un excesivo número de transmisiones debido al gran

número de interconexiones en la red. Para evitar eso, los protocolos de enrutamiento deben descubrir caminos que minimicen el consumo de potencia.

El enrutamiento Geográfico utiliza información geográfica para enrutar sus datos, estas informaciones suelen incluir la localización de los nodos vecinos. Los datos de localización pueden ser definidos a partir de un Sistema de Posicionamiento Global (GPS *Global Position System*) o aún de un sistema local válido solamente para los nodos de la red o válidos solamente para subconjuntos de nodos vecinos.

1.3.3.2 Protocolos de Enrutamiento Jerárquico

- **LEACH**

El protocolo de Jerarquía de Agrupamiento Adaptativo de Baja Energía (LEACH Low-Energy Adaptive Clustering Hierarchy) tiene como objetivo reducir el consumo de potencia, este protocolo fue desarrollado para redes homogéneas y utiliza ciclos durante los cuales se forman agrupaciones de nodos, donde un nodo se escoge como líder en un determinado tiempo para distribuir la carga de potencia. En el LEACH todos los nodos de la red inician un ciclo al mismo tiempo, pero no especifica como obtener un grado de sincronización lo cual hace que cuando una red esté en actividad durante un largo periodo, algunos nodos comiencen un nuevo ciclo en momentos inoportunos. El líder del grupo es responsable de trasmitir los datos de su grupo a un nodo recolector, esto lo hace a través de un salto lo cual limita el tamaño de la red en función del alcance del radio de los nodos; los miembros del grupo usan emplean TDMA.

- **ICA**

El algoritmo de Enrutamiento de Inter-Agrupación (ICA *Inter Cluster Routing Algorithm*) está basado en el protocolo LEACH, pero con la característica principal del aumento del tiempo de vida y el número de paquetes enviados por la red. Esté protocolo envía por medio de la estación base un broadcast para todos los nodos informando su posición geográfica, por, con lo cual cada nodo sabe su posición y la de su estación base. En el ICA los nodos se agrupan con las mismas reglas de formación del LEACH, por lo tanto van a estar conectados siempre al líder más próximo. Cuando se forman los grupos estos notifican su formación a la red por medio de los grupos vecinos. En el ICA,,contrario al LEACH, los nodos líderes no envían los mensajes directamente a la estación base.

El objetivo es preservar potencia enviando los mensajes punto a punto para los nodos que estén a una distancia corta de la estación base. De esta forma la cantidad de potencia consumida por cada nodo de la red disminuye y la de la red aumenta. Para evitar el problema que a los nodos cercanos a la estación base se les agote la potencia, los nodos lideres deben rechazar la retransmisión de

mensajes de otros grupos a la estación base cuando se esten quedando sin potencia, para evitar que no pueda enviar los mensajes de su propio cluster. Cuando ocurre un rechazo en retransmitir datos, el nodo líder que esta enviando los datos envía el mensaje directamente al nodo recolector, de la misma forma como ocurre en el LEACH.

- **TEEN**

El protocolo Red de Sensores Susceptible al Umbral de Energía (TEEN *Threshold sensitive Energy Efficient sensor Network)* es desarrollado para responder a los cambios repentinos en los atributos o variables monitorizados dando una respuesta rápida, importante para aplicaciones de tiempo real. Este protocolo propone clasificar las redes en proactivas y reactivas. Una red proactiva monitoriza el fenómeno continuamente y posee datos que son enviados a una tasa constante. En una red reactiva los nodos solamente envían datos cuando la variable que está siendo monitorizada se incrementa por encima de un cierto límite. En TEEN los nodos próximos forman grupos, y este proceso sigue hasta que la estación base es alcanzada y utiliza la estrategia de formación de líderes como LEACH.

Cuando se forman los grupos, el líder envía un broadcast con dos umbrales: el umbral fuerte (HT *Hard Threshold*) y el umbral suave(ST Soft Threshold) para determinar la necesidad de transmisión del dato recolectado.

El umbral HT es el valor mínimo posible de un variable para accionar el transceptor de un nodo sensor para poder transmitir al líder del grupo. Esté umbral permite que los nodos transmitan sólo cuando el valor del atributo o variable esté dentro del rango permitido, reduciendo el número de transmisiones considerablemente. Cuando un nodo sensor captura un valor por encima del umbral HT, él sólo transmite el dato cuando ese valor varia en una cantidad igual o mayor que el umbral ST, él cual reducirá aún más el número de transmisiones.

- **PEGASIS**

En el protocolo Reunión Eficiente de la Potencia en Sistemas de Información del Sensor (PEGASIS *Power- Efficient Gathering in Sensor Information Systems*) se forman cadenas de nodos sensores de tal forma que cada nodo transmite y recibe datos de un vecino y los pasa a otro formando una cadena y sólo uno de la cadena formada es escogido para transmitir para a la estación base.

La potencia empleada es menor porque la comunicación será entre nodos vecinos, comparada a otros protocolos que requieren muchos cambios de mensajes para elegir lideres y formar grupos, y protocolos en que los nodos constantemente intercambian mensajes con el nodo recolector de forma directa (generalmente se encuentra distante de los nodos). Esto implica un tiempo de vida

mayor para cada nodo y un consumo menor del ancho banda de la red. El PEGASIS tiene las siguientes características:

- Estación Base que se sitúan a una distancia fija;
- Los nodos son capaces de transmitir datos directamente para la estación base y para cualquier otro nodo;
- Cada nodo posee información de localización de los otros nodos;
- Los nodos son homogéneos y con el nivel de energía uniforme;
- Los nodos no son móviles. Cada tiempo un nodo es escogido para transmitir información al nodo recolector.

1.3.3.3 Protocolos de Enrutamiento Plano

Los Principales protocolos de enrutamiento plano son los que se describen a continuación:

- **De Difusión Directa**

La idea de este protocolo radica en la difusión de datos por los nodos sensores usando un esquema de denominación de datos para acabar las operaciones innecesarias de enrutamiento en la capa de red, economizando energía. El protocolo de Difusión Directa propone el uso de una variable par atributo-valor para los datos y consultas en los sensores bajo demanda.

Para crear una consulta, se define el interés usando una lista de atributo-valor como por ejemplo nombres de objetos, intervalos, área geográfica, etc., esté es introducido en la red por la estación base que envía mensajes en broadcast periódicamente para cada uno de los nodos.

Primero se envía un interés exploratorio para verificar si existe algún nodo capaz de atender la petición mediante los eventos (son los datos que atienden a los intereses), y para que se vayan estableciendo gradientes que son los caminos establecidos por los intereses cuando pasan de la estación base a los nodos. Cuando algún nodo establece que puede atender la petición existen varios caminos para llegar a la estación base, de estos sólo uno es seleccionado por el mecanismo de refuerzo en la cual la estación base re-enviá el gradiente original con una tasa de datos mayor obligando al nodo a aumentar por este camino su tasa de envío de datos.

- **SPIN**

El protocolo Negociación de Información de Protocolos de Sensor (SPIN *Sensor Protocols Information Negotiation*) se basa en la información sobre la cantidad de potencia disponible en cada nodo para realizar el enrutamiento y propagar la

información de un nodo a los demás nodos de la red. Este protocolo cuando se da cuenta que un nodo esta cerca de un límite preestablecido de potencia, lo adapta para participar menos en la propagación de los datos.

El SPIN funciona en tres estados: ADVertise, REQuest, DATA. El protocolo se inicia cuando un nodo obtiene nuevos datos que desea trasmitir, esté hecho lo advierte transmitiendo un mensaje ADV el cual contiene información sobre los datos a transmitir (estado ADV) para sus vecinos. Al recibir un ADV, los vecinos verifican si poseen o no los datos, si no lo poseen envían al nodo que trasmitió un mensaje de petición de datos (estado REQ). El nodo que transmitió los datos al recibir la petición envía los datos (estado DATA). Después de recibir el dato, el nodo vecino envía un mensaje ADV a todos sus vecinos, informando que posee un dato nuevo y que quiere trasmitirlo. Así, el ciclo se reinicia.

- **PROC**

El protocolo Coordinación con Enrutamiento Proactivo (PROC *Proactive Routing with Coordination*) es un protocolo de enrutamiento desarrollado para redes de sensores homogéneas y estacionarias, donde los nodos envían datos periódicamente a la estación base (nodo recolector). El protocolo considera que los nodos poseen capacidad para el procesamiento y comunicación para una implementación compacta. El PROC utiliza el concepto de coordinadores para construir un backbone de enrutamiento, que tiene como raíz el nodo recolector. Los nodos que no pertenecen al backbone se conectan directamente a un nodo coordinador. El backbone es reconstruido periódicamente, para que el consumo de los nodos sea balanceado. El proceso de elección de los nodos que formaran el backbone se divide en dos partes: en la primera parte, los nodos determinan cuales deben ser coordinadores de acuerdo sus características; en la segunda parte, completar el backbone en caso de que este no haya sido completamente formado.

- **TinyOS Beaconing**

Es un protocolo de enrutamiento utilizado en los nodos sensores de la plataforma Mica Motes de la Universidad de Berkeley, y tiene como requisito el funcionamiento en redes con este tipo de dispositivos.

En él, la estación base envía un paquete de broadcast denominado beacon a través de la red, los nodos sensores utilizan este paquete para determinar su distancia en relación a la estación base; aquellos que lo reciben directamente son identificados como a un salto de distancia; y los que no envían sus datos a la estación base a través de estos nodos, construyendo rutas periódicas basadas en el menor camino.

1.3.3.4 Protocolos de Enrutamiento Geográfico

El protocolo de Enrutamiento de Energía y Geográfico (GEAR *Geographical and Energy Routing*) divide las regiones a monitorizar en forma rectangulares para realizar el enrutamiento, de las regiones escoge un nodo que va ser el encargado de transmitir los mensajes a las otras regiones, él cual se selecciona de acuerdo al menor costo de envío hasta la región deseada.

El costo del envío es calculado a través del análisis de la distancia y de la potencia que posee los nodos que componen la menor ruta hasta la región especificada. La función costo es recalculada para cada paquete que es enviado para una determinada región para perfeccionar el camino de transmisión de los datos. Al encontrar la región de destino, el protocolo difunde los paquetes a través de una partición formada por cuatro secciones. El paquete es enviado para un nodo de cada una de las secciones el cual se encargará de transmitirlo al destino de su región aplicando el algoritmo recursivamente. En regiones donde la densidad de los nodos es pequeña, la difusión de los datos es hecha vía broadcast.

El protocolo GEAR se destaca de los demás algoritmos geográficos por utilizar informaciones de toda la ruta. El uso de informaciones de nodos distantes permite una ruta más eficiente, al costo de un tiempo mayor de convergencia.

1.3.4 Capa de Transporte

En la actualidad existen pocos estudios realizados en esta capa para las WSN, estos toman mayor importancia cuando la aplicación realizará acceso a redes externas como Internet, pero por las características de las redes WSN se hace necesario pensar en protocolos especiales para esta capa.

1.3.4.1 Protocolos

Algunos estudios han definido algunos protocolos que se enuncian a continuación [10] [11] [12]:

- **PSFQ**

El protocolo lograr rápidamente, bombear lentamente PSFQ (*Pump Slowly, Fetch Quickly*) es un protocolo de transporte diseñado para adaptarse a las diferentes condiciones de la red. El protocolo trabaja con corrección local de errores, utilizando para esto confirmación punto a punto que se hace más escalable y robusta en ambientes con altas tasas de errores, como las WSN. El PSFQ es adaptativo, o sea, si la red presenta un porcentaje de fallos bajo, el envío de datos será el tradicional. En casos de fallos frecuentes, el protocolo tiene un comportamiento store and forward. Con el objetivo de identificar pérdidas de

datos, el emisor transmite el mensaje en fragmentos numerados. Cada fragmento es recibido y almacenado en la cache de cada nodo intermedio de la comunicación. Esta cache se utiliza para identificar cuáles fragmentos o secuencias de fragmentos (ventanas) fueron perdidos.

El PSFQ trabaja con 3 tipos de operación: push, fetch y report. Las operaciones de push se utilizan para enviar fragmentos de un mensaje al próximo salto en el camino del destinatario; la operación fetch cuando un nodo intermedio identifica que fragmentos no fueron recibidos, y pide la retransmisión de los fragmentos perdidos y operación report en los nodos receptores del mensaje para notificar al emisor que la transmisión fue completada.

En la operación push se realiza una transmisión periódica de fragmentos de un mensaje, en intervalos regulares. Si un nodo recibe un fragmento con número de secuencia mayor que el esperado, el protocolo identifica que existe un fragmento perdido, y éste realiza la operación de fetch reactivo, para recuperar los fragmentos perdidos. Al escuchar un mensaje de fetch reactivo, los nodos verifican si poseen uno de los fragmentos requeridos en su cache, si está trasmiten el dato al nodo correspodiente. El fetch también puede ser proactivo, esté se presenta cuando un fragmento no llegue en el tiempo esperado.

- **RMST**

El Transporte Seguro Multi-Segmento (RMST *Reliable Multi-Segment Transport*) es un protocolo desarrollado para operar en conjunto con difusión directa, el propósito es garantizar la entrega de todos los datos solicitados por la estación base, que sean transmitidos desde un nodo. El RMST realiza la fragmentación y la reagrupación de los mensajes mediante una confirmación punto a punto añadiendo atributos específicos a los datos mediante un pequeño overhead.

La detección de los fragmentos perdidos se hace por medio de temporizadores. Si un fragmento no se recibe en el tiempo especificado, se envía un NACK para los nodos que están en el sentido inverso del gradiente, para encontrar los fragmentos perdidos. Los nodos que poseen uno de los fragmentos en el cache lo trasmiten al nodo. Si el fragmento no está en el cache, el NACK es trasmitido en sentido contrario al gradiente hasta que el fragmento sea encontrado.

- **ESRT**

Transferencia Confiable Estación Base - Evento (ESRT *Event-to-Sink Reliable Transfer*) es un protocolo que tiene como objetivo reconocer un evento de forma confiable por medio de la estación base a través de la recepción de varios mensajes de los sensores. Si el número de mensajes recibidos es inferior al límite establecido, el evento no es reconocido de forma confiable. De esta forma, el

objetivo del ESRT es ajustar la tasa de envío de datos de cada nodo para que la tasa de paquetes recibidos sea próxima al valor necesario para el reconocimiento confiable.

El protocolo utiliza conceptos de estados de operación, cada estado es definido por el comportamiento de la red en términos de la confiabilidad de los datos recolectados y congestionamiento. Para medir el congestionamiento de los nodos, se verifica el tamaño de la fila de paquetes enviados. Si pasa un tamaño predeterminado, el nodo comunica el hecho a la estación base a través de la cabecera del protocolo. Se pueden identificar comportamientos posibles de la red y se han definido 5 estados de funcionamiento.

- Intervalo sin congestionamiento y baja confiabilidad.
- Intervalo sin congestionamiento y alta confiabilidad.
- Intervalo con alto congestionamiento y alta confiabilidad.
- Intervalo sin congestionamiento y pequeña confiabilidad.
- Intervalo de operación óptimo.

La estación base calcula en que estado de operación se encuentra la red en intervalos regulares de tiempo. Al calcular el estado de la red, el protocolo evita el consumo de energía y procesamiento en los sensores, lo que podría imposibilitar la operación. Si la red se encuentre fuera del estado de operación óptimo, la tasa de envío de datos de los nodos se ajusta para llegar a su punto de operación óptimo.

1.4 CARACTERÍSTICAS

Las redes de sensores están influenciadas por diversos factores (topología, consumo de potencia, costo, hardware, software etc.) que están directamente relacionados con cualquier solución propuesta, por lo tanto las WSN presentan diferentes características particulares de acuerdo a las áreas de aplicación. A continuación se enuncian algunas características de acuerdo a los factores mencionados anteriormente [1] [2] [13]:

- **Topología Dinámica:** en una red de sensores, la topología siempre es variable y los nodos tienen que adaptarse para poder comunicar nuevos datos adquiridos y aceptar nuevos nodos.

- **No se utiliza infraestructura de red:** una red de sensores no tiene necesidad alguna de infraestructura para poder operar, ya que sus nodos pueden actuar de emisores, receptores o enrutadores de información.

- **Tolerancia a fallos**: algunos nodos sensores pueden bloquearse debido a falta de potencia, daños físicos o interferencia del medio, su fallo no puede afectar la tarea de la red de sensores. El nivel de tolerancia a fallos está relacionado con la

aplicación a ser soportada por la red y el número de nodos dentro del área de cubrimiento.

- **Consumo de potencia:** es uno de los factores más sensibles debido a que tienen que conjugar autonomía con capacidad de proceso, ya que cuenta con una unidad de energía limitada. Un nodo sensor tiene que contar con un procesador de consumo ultra bajo así como de un transceptor radio con la misma característica, a esto se agrega un software que también conjugue esta característica haciendo el consumo aún más restrictivo.

- **Limitaciones hardware:** para poder conseguir un consumo ajustado, se hace indispensable que el hardware sea lo más sencillo con lo cual la deja una capacidad de proceso limitada.

- **Costos de producción:** como la mayoría de las aplicaciones son proyectadas para áreas extensas será necesario una gran cantidad de nodos sensores para poder obtener datos confiables. Para que estas aplicaciones sean factibles económicamente deben tener un bajo costo de producción. El costo de un nodo sensor debería ser mucho menor a 1 dólar para permitir que la red de sensores fuera viable.

- **Direccionamiento de los sensores**: dependiendo de la aplicación, cada sensor que transmita un dato puede ser direccionado (ubicación exacta) o no. Por ejemplo, los sensores colocados en el cuerpo humano deben ser direccionados porque se necesita saber exactamente de donde viene el evento. Por otro lado, sensores que están monitorizando el ambiente en una región posiblemente no necesitan ser identificados individualmente porque lo importante es saber que ha ocurrido un evento en esa región.

También existen otras características como la agregación de datos, capacidad de responder a consultas, tareas colaborativas que están ligadas a la aplicación, por lo tanto son características propias de ellas.

1.5 APLICACIONES

Las WSN, han crecido en popularidad y las aplicaciones que se pueden desarrollar para esté campo son muy amplias, van desde el monitoreo en diversos ambientes hasta el monitoreo de personas, siempre con el objetivo de mejorar la eficiencia y productividad. Entre las principales aplicaciones se encuentran [4] [5] [6] [13]:

- **Entornos de alta seguridad**: En algunos entornos existen elementos que pueden llegar a ser peligrosos: escapes de gas, instalaciones eléctricas en mal estado, contaminación de agua o aire, etc., que requieren altos niveles de

seguridad, que pueden ser percibidos por una WSN de una manera sencilla y a bajo costo.

- **Sensores ambientales**: el control ambiental en áreas extensas como océanos o bosque, sería imposible sin las redes de sensores para controlar variables como temperatura, humedad, fuego, actividad sísmica así como otras. También ayudan a expertos a diagnosticar o prevenir un problema o urgencia y además minimiza el impacto ambiental de la presencia humana.

- **Sensores industriales**: dentro de fábricas existen complejos sistemas de control de calidad, el tamaño de estos sensores les permite estar donde se requiera.

- **Automoción**: las redes de sensores son el complemento ideal a las cámaras de tráfico, ya que pueden informar de la situación del tráfico en ángulos muertos que no cubren las cámaras y también pueden informar a conductores de la situación, en caso de atasco o accidente, con lo que estos tienen capacidad de reacción para tomar rutas alternas.

- **Medicina:** es otro campo bastante prometedor. Con la reducción de tamaño que están sufriendo los nodos sensores, la calidad de vida de pacientes que deban que tener controlada sus constantes vitales (pulsaciones, presión, nivel de azúcar en sangre, etc), podrá mejorar substancialmente. Es en esté escenario donde el presente trabajo realiza un piloto de aplicación.

- **Domótica**: su tamaño, economía y velocidad de despliegue, lo hacen una tecnología ideal para domotizar el hogar a un precio asequible.

1.6 ESTÁNDARES

El desarrollo y la gran acogida de aplicaciones orientadas a sensores han establecido redes que brindan soluciones económicas y atractivas para una amplia gama de aplicaciones conocidas y nuevas.

Sin embargo, con la multiplicidad de las especificaciones incompatibles se ha creado un cierto grado de confusión, la cual ha impuesto una carga económica innecesaria ha consumidores y fabricantes que utilizan las WSN. En vista de esta situación la IEEE ha patrocinado una serie de proyectos conocidos como IEEE P1451, dentro del cual esta el IEEE 1451.5 que especifica información que permite usar sensores y dispositivos para comunicarse inalambricamente, eliminando costos y de tiempo de instalación. Esté proyecto actualmente está trabajando en varios estándares entre ellos Bluetooth y Zigbee, los cuales se clasifican bajo el grupo de las Redes inalámbricas de Área Personal (WPAN Wireless Personal Área Networks) y sus dispositivos son de pequeñas dimensiones [2].

1.6.1 Bluetooth

Bluetooth [34] o IEEE 802.15.1 aparece en 1998, es una norma desarrollada por un consorcio de empresas con el objetivo de reemplazar a IrDA y permitir una comunicación inalámbrica mediante radiofrecuencia entre dispositivos generalmente pequeños, PDAs, teléfonos móviles, periféricos etc. Esta tecnología soporta hasta 8 dispositivos en una Piconet o WPAN .

Bluetooth opera en la banda de 2,56 GHz y ofrece hasta 1Mbps, que se reduce a 434 Kbps al descontar la sobrecarga de los protocolos. El alcance máximo es de entre 10 y 100 metros, no obstante los resultados obtenidos en la práctica por la mayoría de los equipos disponibles comercialmente son muy inferiores al venir provistos de antenas de mala calidad. En 2004 se definió la norma Bluetooth v2.0, con una velocidad de transmisión de 3Mbps (1307 Kbps para datos).

1.6.2 ZigBee

ZigBee, ES un estándar reciente para la normalización de redes de sensores, promovido por un consorcio de empresas llamado “ZigBee Alliance” [36]. Define un sistema completo de redes inalámbricas con baja velocidad de transferencia de datos para dispositivos muy sencillos, muy baratos y de un consumo tan bajo como para ser capaces de funcionar meses o años sin recargar sus baterías. Para el nivel físico y de enlace, ZigBee se basa en el estándar IEEE 802.15.4 [15]. Las aplicaciones finales son desarrolladas por los usuarios, pero el estándar da las pautas para realizarlas en su capa de aplicación. Este estándar será ampliado en el siguiente capitulo y es el principal enfoque de esté trabajo.

1.7 SISTEMAS OPERATIVOS [3] [14]

Debido a las limitaciones que poseen los nodos sensores, se han creado diversos sistemas operativos para poderlas solventar y dar un mejor soporte. Entre los sistemas operativos mas utilizados y difundidos se encuentran: TinyOS de la Universidad de Berkeley; Contiki del Instituto de Ciencias de computación de Suecia; el S.O de redes de sensores multinodal (MantisOS *Multimodal Networks of In-situ Sensors*) de la Universidad de Colorado; SOS de la Universidad de California; Yatos de la Universidad de Minas Gerais; el S.O de tiempo real (PeerOS *Preemptive EYES Real Time Operating System*) de la Universidad de Twente en Holanda. Todos estos sistemas operativos tienen como objetivo consumir poca potencia, ocupar poca memoria del nodo, ofrecer multitareas y basarse en componentes.

1.7.1 Principales Características de los Sistemas Operativos

TinyOS es el sistema operativo más conocido y el más utilizado en las investigaciones con redes WSN; desarrollado para las plataformas Motes es usado en muchas aplicaciones. Cuando se carga una aplicación en los sensores, ésta se compila junto al sistema operativo y se carga en el sensor, por los que no es necesaria una instalación previa del TinyOS en los motes. TinyOS utiliza un modelo de programación basado en el concepto de "*wiring*" que enlaza componentes para producir un programa final.

El sistema SOS es un sistema operativo para el Mote-class Embedded Sensor Networks, usa un kernel común, que implementa la ejecución dinámica de módulos para crear sistemas que soporten adición, modificación y renovación de servicios de red mediante la reprogramación para modificar el software y las aplicaciones de los nodos después que estos ya estén distribuidos en el espacio del fenómeno.

MantisOS, es un sistema operativo que se puede ejecutar en nodos MANTIS Nymph, MICA2 MICA2DOT, MICAZ y Telos. Está basado en hilos que permite que los nodos de la red puedan intercalar nativamente tareas complejas y de esta forma permite que hilos con altas prioridades se ejecuten antes de hilos con bajas prioridades, además soporta multihilos en forma preventiva y fue proyectado para multicapas, permitiendo que el sistema pueda ser migrado para un nuevo hardware sin mayores complicaciones.

Contiki, fue desarrollado para ambientes confinados, provee de una ejecución dinámica de programas y servicios. El kernel está dirigido por eventos, pero el sistema soporta multithrading preventivo, que puede ser aplicado en cada proceso básico solamente por las aplicaciones que las requirieran.

El sistema operativo PeerOS basa su funcionamiento en los siguientes principios: operación orientada a eventos, división en la ejecución en tareas, separación de funcionalidades en unidades distintas y comunicación entre los componentes del S.O y entre los nodos. Actualmente, el PeerOS ha sido usado como una plataforma para desarrollar, implementar y probar varios algoritmos distribuidos, además de ser utilizado para realizar demostraciones

El YATOS es un sistema operativo para el sensor BEAN desarrollado por la misma universidad, tiene un sistema de programación basado en tareas. Cuando se presentan muchas tareas a ser ejecutadas, es necesario que haya una prioridad para decidir el orden de ejecución, esta prioridad depende si ocurre un evento para dar por concluida.

2. ESTÁNDAR ZIGBEE

Como se mencionó en el capitulo anterior, el desarrollo de protocolos y arquitecturas para el diseño de redes de sensores inalámbricos se ha convertido en un campo de investigación muy importante en los últimos años. El desarrollo de esta tecnología ha venido de la mano con nuevos estándares inalámbricos de comunicación que ha permitido la aparición de aplicaciones nuevas en medicina, agricultura, sistemas de control industrial, y nuevos escenarios como domótica, inmótico, control inteligente de edificios etc. Dentro de los nuevos estándares inalámbricos apareció ZigBee, mencionado brevemente como estándar dentro de las WSN, orientado a la interconexión de dispositivos autónomos, implementando en su diseño un bajo consumo de potencia y la capacidad de formar redes de mayor tamaño que Bluetooth y Wi- Fi, a cambio, de soportar tasas de trasferencias menores.

El estándar ZigBee surge de un consorcio de compañías llamado “ZigBee Alliance” [36] cuyo objetivo es encaminar y promover el desarrollo de redes inalámbricas de área personal con baja velocidad, bajo costo y bajo consumo de potencia.

Bajo el lema de “Control inalámbrico que simplemente funciona”[3], se han desarrollado diferentes escenarios para el uso de ZigBee, desde hogares completamente interconectados, controles de acceso ambientales, periféricos, mecanismo para controlar el uso de la potencia, etc. Hasta escenarios en el ámbito hospitalario donde puede ser usada como herramienta para asistencias médicas.

En un entorno doméstico, una red ZigBee puede controlar e interconectar todos los electrodomésticos, desde televisores con sus respectivos controles remotos, dvds, computadores y hasta lavadoras. También puede ser utilizado para controlar aspectos de seguridad y mantenimiento doméstico como el control de acceso, control de luces, temperatura, el estado de ciertos alimentos, hasta prestar un servicio tan específico que puede notificar si un estante de libros en la biblioteca de la casa esta más pesado de lo normal e inclusive para controlar la irrigación de los jardines.

En el ámbito empresarial ZigBee cumplen el mismo propósito de interconexión y control, solo que en estas aplicaciones de red, están destinadas a incrementar la productividad, eficiencia y seguridad. Otro factor a considerar dentro de las aplicaciones de control industrial, es el manejo de carga, control de procesos, control de inventarios, control ambiental y el control de energía.

[3] ZIGBEE ALLIACE, ZigBee tecnology: Wíreles Control that simply works [Presentación en Power Point]. http://www.zigbee.org

Un sector donde ZigBee esta teniendo gran aceptación y usos bastante prácticos es el sector salud, donde sus aplicaciones en hospitales e instituciones dedicadas a la atención de enfermos pueden contribuir a mejorar la atención y realizar un seguimiento del estado de salud de los pacientes, por medio de dispositivos de monitoreo interconectados a la red. En este escenario las redes son empleadas para que doctores y enfermeras supervisen continuamente el estado de los pacientes, capturen en tiempo real muestras de los signos vitales de pacientes mediante sensores (del tamaño de una moneda) colocados en sus cuerpos y almacenar datos de pacientes tales como identificación, historia, y tratamientos, supliendo el uso de los sistemas de almacenaje tradicional en los centros hospitalarios.

El propósito de esté capitulo es profundizar sobre el estándar ZigBee basándose principalmente en el estándar IEEE 802.15.4 del 1 de octubre de 2003 [15] y la especificación Zigbee versión 1.0 de abril 14 de 2005 [16], por lo tanto también sus tablas y figuras.

2.1 GENERALIDADES

ZigBee es un estándar diseñado para presentar un bajo costo y poder ser competitivo; soportar una gran variedad de aplicaciones en control industrial, automatización de casa, sistemas de seguridad, agricultura y medicina, mercados en los cuales no se requiere una tasa de transmisión de datos muy alta, donde el bajo consumo de potencia y la batería de larga vida son importantes.

ZigBee se basa en el estándar 802.15.4 de la IEEE que normaliza las capas bajas (Física y MAC) de las Redes de Área Personal inalámbricas – Baja Tasa (LR-WPAN - *Wireless Personal Area Network – Low Rate*) como lo muestra la figura 2.1, y estandariza las capas altas para las LR-WPAN para que se presente una solución unificada en este tipo de redes y de esta manera los diferentes fabricantes puedan ínteroperar [23].

Las LR-WPANs se utilizan para transmitir información a través de distancias relativamente cortas, diferente a las redes de Área Local Inalámbrica (WLAN - Wireless Local Area Network). Conexiones realizadas vía LR-WPANs involucran una pequeña o ninguna infraestructura, esta pequeña característica permite, redes de comunicación simple y económica con conectividad en aplicaciones con requerimientos de bajo consumo de energía, facilidad de instalación, confiabilidad en la transferencia de datos, y una vida de la batería razonable, mediante un protocolo simple y flexible.

<table>
<tr><th>Modelo OSI/ISO</th><th>Modelo IEEE 802</th><th colspan="2">Modelo ZigBee</th></tr>
<tr><td>Aplicación</td><td rowspan="5">Capas Altas</td><td colspan="2">Usuario</td></tr>
<tr><td>Presentación</td><td rowspan="3">Capa de Aplicación.</td><td rowspan="3">ZigBee</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td></tr>
<tr><td>Red</td><td>Red</td></tr>
<tr><td rowspan="2">Enlace de Datos</td><td>Control de Enlace de Datos</td><td rowspan="2">Control de Acceso al Medio</td><td rowspan="3">IEEE 802.15.4</td></tr>
<tr><td>Control de Acceso al Medio</td></tr>
<tr><td>Física</td><td>Física</td><td>Física</td></tr>
</table>

Figura 2.1 Modelo OSI comparado con ZigBee y IEEE 802 [17]

ZigBee es impulsado por empresas importantes como Chipcon, Microchip, Motorola, Philips, Samsung, etc. que conforman la "ZigBee Alliance", encargada de promover y fomentar su uso a nivel mundial y de definir los perfiles de las aplicaciones.

Para obtener un bajo consumo de potencia, la solución está en reducir el ciclo de trabajo y pasar la mayor parte del tiempo con el transceptor desactivado, permitiendo que en algunas aplicaciones los transmisores estén activos menos del 1 % del tiempo. Para hacer posible este ciclo de trabajo, el estándar IEEE 802.15.4 dispone de un modo que usa tramas beacon o tramas de señalización, denominado modo en estructura de supertrama, concepto que se ampliará más adelante [17].

2.2 CARACTERÍSTICAS

Zigbee tiene como objetivo principal ofrecer un estándar abierto y eficiente, con características de bajo consumo de potencia, bajo costo en sus productos, una tasa de transferencia menor a 250kbps, facilidad de instalación y transferencia de datos manteniendo un protocolo simple y flexible; para brindarles a los usuarios flexibilidad y escalabilidad, diseño y reducción del tiempo de instalación, e interoperabilidad. Las principales características son:

- Velocidad de datos de 250 kbps, 40 kbps y 20 kbps.
- Operación en estrella, igual-a-igual, árbol, malla y grupos de árbol[4].
- Asignación de direcciones IEEE cortas de 16 bits o extendidas de 64 bits.
- Asignación garantizadas de ranuras de tiempo (GTS *Guaranteed Time Slot*).
- Acceso al canal a través de acceso múltiple con detección de portadora – evitando colisión (CSMA-CA *Carrier Sense Multiple Access with Collision Avoidance - Channel Access*)
- Distancia de transmisión de hasta 200 mts dependiente de las aplicaciones y de la línea de visión.

[4] Esta topología es conocida como Cluster Tree

- Detección de Energía (ED *Energy Detection*).
- Indicador de calidad del enlace (LQI *Link Quality Indication*).
- 16 canales en la banda 2450 Mhz, 10 canales en la banda de 915 Mhz, y un canal en al banda de 868 Mhz.
- Presenta otra forma de direccionamiento mediante los puntos finales (endpoint).
- Utiliza perfiles, clusters, descriptores para las aplicaciones.
- Proporciona servicios de seguridad para las capa de red, subcapas MAC y APS.

2.2.1 Dispositivos

Para formar una red ZigBee se necesitan dos o más dispositivos dentro de un espacio de operación, los cuales se comunican dentro de un canal físico para constituir una LR-WPAN.

El estándar IEEE 802.15.4 define dos dispositivos: el Dispositivo de Función Completa (FFD *Complete Function Device*) y el Dispositivo de Función Reducida (RFD *Reduced Function Device*). El FFD se usa en cualquier tipo de red, su función principal es coordinar la red, por tal razón se comunica con cualquier dispositivo sea RFD o FFD, mientras que el dispositivo RFD no podrá ser coordinador, solo se comunicara con un FFD y su uso se limita solamente a transmitir y recibir.

De estas definiciones, ZigBee especifica tres tipos de dispositivos: ZigBee coordinador, ZigBee Router y ZigBee dispositivo final.

- ZigBee Coordinador (FFD): es el responsable de la creación y el mantenimiento de la red permitiendo la asociación de nuevos dispositivos con la asignación de direcciones, disociación de estos, almacena toda la información sobre la red, con lo cual requiere de mayor capacidad de memoria y de procesamiento.

- ZigBee Router (FFD): puede operar como coordinador de la red, pero su función principal es el enrutamiento para encaminar los mensajes hacia el destino correcto y permitir la expansión de la red.

- ZigBee Dispositivo Final (RFD o FFD): generalmente son los dispositivos de frontera, y están inactivos en determinados periodos de tiempo para reducir el consumo de energía.

2.2.2 Topologías

Zigbee soporta varias topologías de red, las definidas por la subcapa MAC en el estándar IEEE 802.15.4 (estrella e igual a igual[5]) ver figura 2.2; y las definidos por la capa de red (malla y árbol) ver figura 2.3.

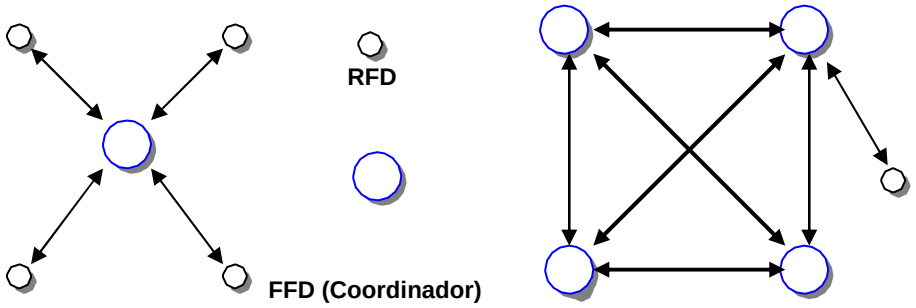

Figura 2.2 Topologías en estrella e igual–igual

En la topología en estrella interviene un coordinador ZigBee y varios dispositivos finales. Toda comunicación establecida entre los dispositivos finales es controlada por el coordinador ZigBee. Los dispositivos finales solamente se enteran cuando se inician y terminan las comunicaciones de la red. El coordinador es el que comienza, mantiene y termina la red, además de admitir nuevos dispositivos finales.

En una topología igual-a-igual intervienen dispositivos FFD y RFD. Los FFD se comunican entre si dentro de su área de cobertura sin pasar por un nodo central, pero solamente uno será el coordinador de la red ZigBee. Los RFD son sólo periféricos, ya que carecen de capacidad para poder repetir paquetes, estarán enlazados a los FFD y solo se comunicaran con ellos directamente.

En las topologías en malla y árbol, intervienen los tres tipos de dispositivos ZigBee, pero existe un único coordinador de red que será el responsable de empezar la red con ciertos parámetros de funcionamiento, los otros FFD tomaran funciones de enrutamiento para dirigir la información hacia los dispositivos finales y extender la red, como lo muestra la figura 2.3. Los RFD están organizados en una topología en estrella, en este caso el dispositivo central (FFD) va ser un enrutador que controla el flujo de datos.

Las redes en topología en malla, permiten el enrutamiento desde cualquier dispositivo origen a cualquier dispositivo destino, logrando múltiples rutas para las comunicaciones de los dispositivos, mientras que en la de árbol el enrutamiento se

[5] Está topología es conocida como peer to peer.

realiza por un solo camino utilizando la estrategia de enrutamiento jerárquico, como se observa en la figura 2.3

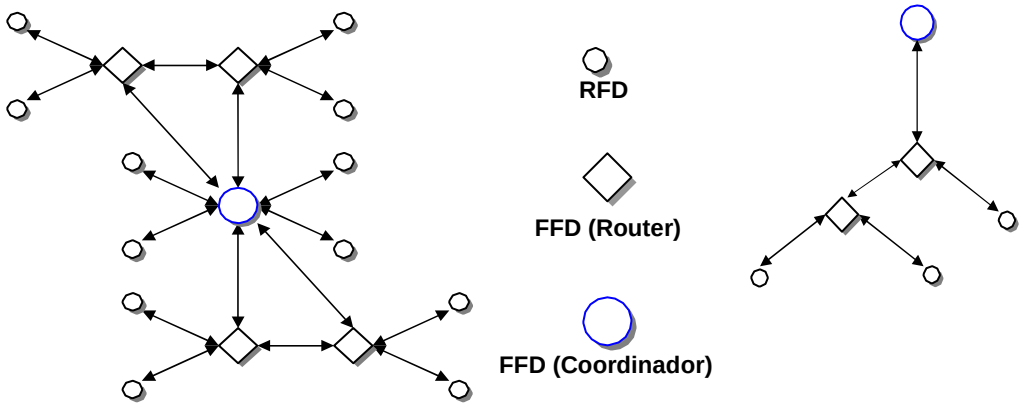

Figura 2.3 Topologías en malla y árbol

Las topologías en malla permiten altos niveles de confiabilidad, escalabilidad, nivel de redundancia, de tal forma que en caso de que un dispositivo salga de la red exista siempre una ruta secundaria para la comunicación de datos.

Las topologías grupos de árbol utilizan una topología híbrida árbol/malla que combina los beneficios de ambas para altos niveles de confiabilidad y soporte para este tipo de dispositivos. En estas topologías existen varios coordinadores de red, uno por cada grupo, los cuales son llamados cabeza de grupo y un coordinador central de toda la red.

Para identificar los dispositivos finales dos tipos de direcciones se utilizan: la dirección de 64 bits o extendida y la de 16 bits o corta. La dirección extendida la tienen todos los dispositivos y la corta se asigna por parte del coordinador cuando un dispositivo se une a la red para reducir el tamaño del paquete.

2.2.3 Supertrama

Dentro de la subcapa MAC, el estándar IEEE 802.15.4 define 4 tipos de tramas: datos, ACK, comandos y beacon; está última es la que permite el uso opcional de las supertramas, están definidas por el coordinador y son las que permiten la sincronización sin necesidad que los dispositivos estén permanentemente en modo de escucha, con el importantísimo ahorro de energía que esto representa.

La supertrama consiste en 16 ranuras de tiempos (slots) temporales reservados para que ciertos nodos transmitan en forma coordinada lo que deseen (tramas de datos, tramas de comandos) y tantas tramas como lo permita el tiempo que tiene asignado. Las supertramas son enviadas por el coordinador entre periodos que oscilan entre 15.38 mseg y 252 mseg. En la primer ranura de tiempo se envía la

trama beacon donde va información sobre el identificador de red, periodo de beacon, la estructura de la supertrama, y evita que los nodos que trasmiten se traslapen entre si.

Para que la comunicación entre un dispositivo y el coordinador tenga éxito el dispositivo deberá intentar comunicarse entre dos tramas de beacon sucesivas (ver figura 2.4). A este periodo de tiempo (15 ranuras de tiempo) se le denomina periodo de contención de acceso (CAP *Contention Access Period*). En esté periodo de tiempo todos los dispositivos pueden acceder al medio utilizando CSMA/CA ranurado en donde las ranuras están alineadas con el comienzo de un beacon. Cualquier dispositivo, que desee transmitir durante el periodo de acceso de contención, espera a que empiece la siguiente ranura de tiempo y después determina si algún otro dispositivo se encuentra transmitiendo en la misma ranura de tiempo. Si algún otro dispositivo se encuentra transmitiendo en dicha ranura, el dispositivo se repliega a un número aleatorio de ranuras o indica un fallo en la conexión después de varios intentos.

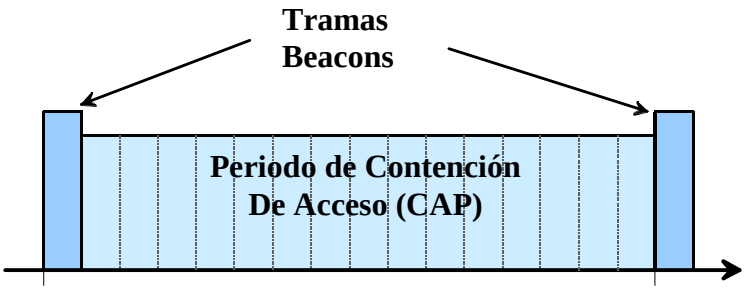

Figura 2.4 Estructura básica de Supertrama

El coordinador puede asignar 7 ranuras de la supertrama a dispositivos de la red, A estas se le llama ranura de tiempo garantizada (GTS - *Guaranteed time slots*) ver figura 2.5. Esto se emplea en aplicaciones que requieran determinados anchos de banda y latencia. El grupo GTS definen un nuevo periodo de tiempo, llamado Periodo de Libre Contención (CFP - *Contention Free Period*). Cuando el GTS se utiliza, todos los dispositivos deben completar sus transmisiones antes de que el CFP comience, a si mismo cuando los dispositivos transmiten en CFP deber terminar sus transmisiones antes del final del mismo.

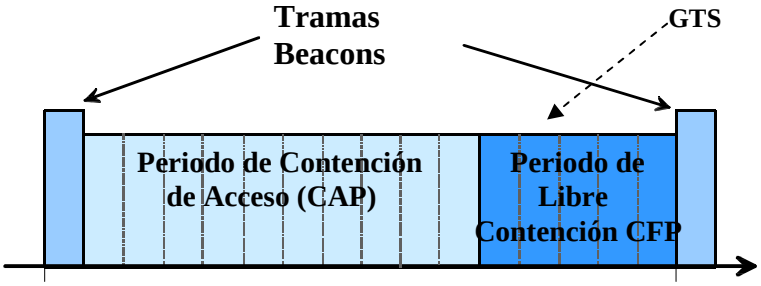

Figura 2.5 Estructura de Supertrama con GTS

Si el coordinador no desea usar la estructura de supertrama puede desactivar las transmisiones en el campo “estructura de la supertrama” en la trama beacon. Aquí el mecanismo de acceso al medio es CSMA/CA no ranurado, esto implica que los dispositivos transmiten en el momento que es necesario sin esperar la pauta (beacons) de un coordinador. Cuando algún dispositivo desea transmitir en una red que no permite señales de sincronización (beacon), la red primero revisa si otro dispositivo se encuentra transmitiendo sobre el mismo canal; si es el caso, el intento de acceso al canal se tiene que hacer en ocasiones posteriores, o indica una falla de conexión después de varios intentos fallidos.

2.2.4 Transferencia de Datos

El modelo de transferencia de datos depende de la topología de red que se esté usando. En el caso de la topología estrella existen dos formas para enviar información, la cual depende si está habilitado el envió de beacon (acceso al medio el CSMA-CA ranurado) o no (acceso al medio el CSMA/CA no ranurado). Los dos escenarios para la transferencia de datos son:

- Desde un dispositivo al coordinador.
- Desde un coordinador a un dispositivo.

En la transferencia de datos desde un dispositivo a un coordinador, ver figura 2.6, en entornos Beacon, los dispositivos siempre esperan una trama guía para utilizar las supertramas y poder enviar los datos. Si no tiene un GTS asignado debe transmitir en el CAP. En caso de ya tener asignado el GTS simplemente habrá que esperar el momento preciso después de escuchar la trama de señalización para transmitir. En entornos no beacon, no existe una trama guía, los dispositivos no están sincronizados y el envío de una trama de datos se da en cualquier momento.

Tanto en entornos beacon y no beacon, las tramas ACK se utilizan como opcionales para confirmar si las recepciones fueron exitosas o no.

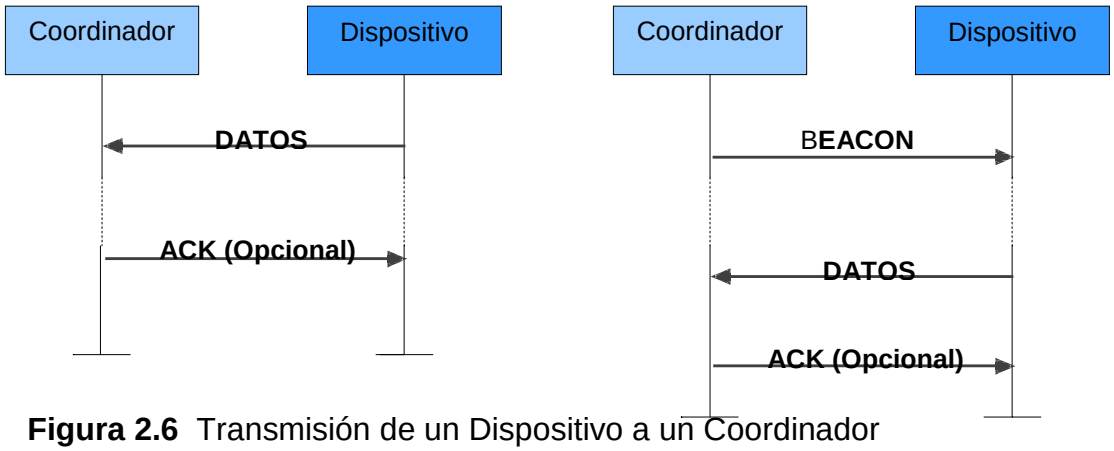

Figura 2.6 Transmisión de un Dispositivo a un Coordinador

Para la transferencia de datos desde un coordinador a un dispositivo ver figura 2.7 en entornos “Beacon” el coordinador transmitirá en la trama beacon la información necesaria para decirle al dispositivo que tiene datos para el. Los dispositivos esperan la trama guía para ver si tienen datos pendientes, si los hay, el dispositivo pide los datos enviando una trama para indicar que está preparado para recibir la información (trama de petición de datos). El coordinador envía un ACK (si es necesario) y después procederá a enviar los datos directamente. Por último el dispositivo envía un ACK par confirmar la llegada de los datos.

En entornos no beacon, el terminal envía una trama de petición de datos, el coordinador responderá con una trama ACK, e inmediatamente transmitirá la trama de datos. Finalmente el terminal responderá con una trama ACK

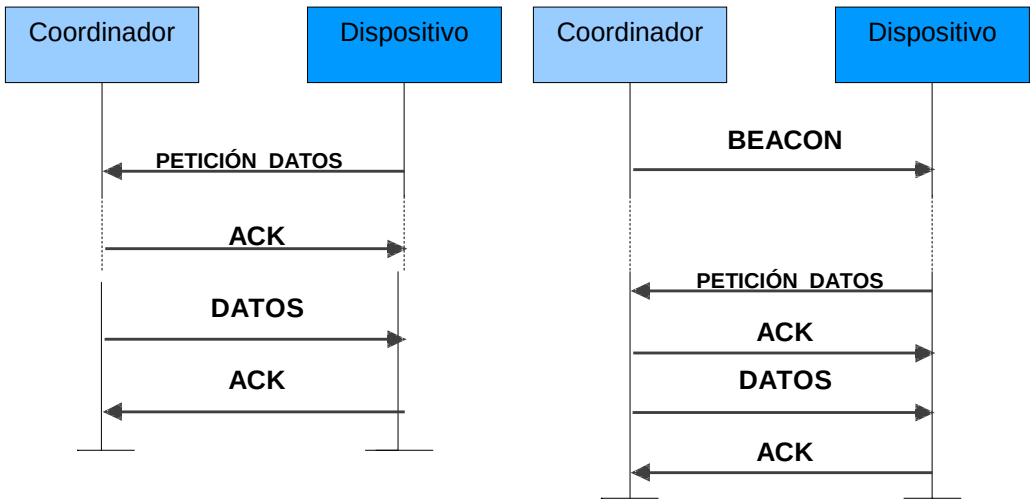

Figura 2.7 Transmisión de un Coordinador a un Dispositivo

Para la transferencia de datos en topologías malla, igual-a-igual y grupos de árbol, donde los dispositivos se pueden comunicar entre ellos, se realiza uniendo las transferencias vistas anteriormente.

2.3 ARQUITECTURA

La arquitectura ZigBee, como se mencionó anteriormente, se basa en el modelo de las siete-capas del Sistema Abierto de Interconexión (OSI *Open Systems Interconnection*), el estándar IEEE 802.15.4 define las capas más bajas: la capa física y la subcapa del Control de Acceso al Medio. La alianza de ZigBee específica la Capa de la Red y la Capa de Aplicación que incluye las aplicaciones de soporte de subcapas (APS *Application Support Sub-layer*), los dispositivos objetos ZigBee (ZDO *ZigBee Device Objects*) y los objetos de aplicación definidos por el fabricante mediante las aplicaciones framework, como lo muestra la figura 2.8

Para la correcta operación, funcionalidad e interoperabilidad, las capas conceptualmente contienen dos servicios (conjunto de primitivas necesarias que coloca a la capa inferior a disposición de la capa superior): de datos y de gestión cuyas funcionalidades son accedidas mediante puntos de acceso de servicio (SAP *Service Access Point*). El primer servicio es el encargado de la transmisión y recepción de las unidades de datos de los protocolos (PDU *Protocol Data Unit*) y el segundo permite el transporte de los comandos de gestión para una mejor interoperabilidad, los dos mediante el intercambio de primitivas.

Es necesario diferenciar entre las primitivas y los paquetes. Las primitivas son el conjunto de funcionalidades mínimas que debe colocar cada capa a disposición de las capas superiores y por lo tanto se originan internamente dentro de cada dispositivo. Por otra parte los paquetes hacen referencia a las transmisiones externas, es decir, entre dispositivos. Aun cuando las primitivas pueden hacer que se transmita un paquete, y un paquete recibido coloca en marcha una serie de primitivas, no son el mismo. En total hay cuatro tipos de funciones que puede desarrollar una primitiva:

- Petición (Request): esta función va desde las capas superiores a las inferiores y pide la iniciación del servicio.

- Indicación (Indication): va desde las capas inferiores hasta las superiores y se destina a indicar eventos sucedidos de cierta importancia. Estas indicaciones se pueden originar ya sea por la recepción de una trama proveniente de otro dispositivo o simplemente por algún evento interno.

- Respuesta (Response): esta función se origina en las capas superiores y va dirigida a las infeeriores; se envía para responder alguna primitiva request que se hubiera originado.

- Confirmación (Confirm): Se pasa de las capas inferiores a las superiores o para confirmar alguna primitiva de petición anterior.

Cada capa posee en su entidad de gestión una “Base de Información” que contiene los atributos requeridos para manejar cada capa. La base de información en la capa física y subcapa MAC es conocida como PIB, en la capa de red como NIB y en la APS como AIB. Los atributos pueden ser manipulados por medio de comandos GET/SET.

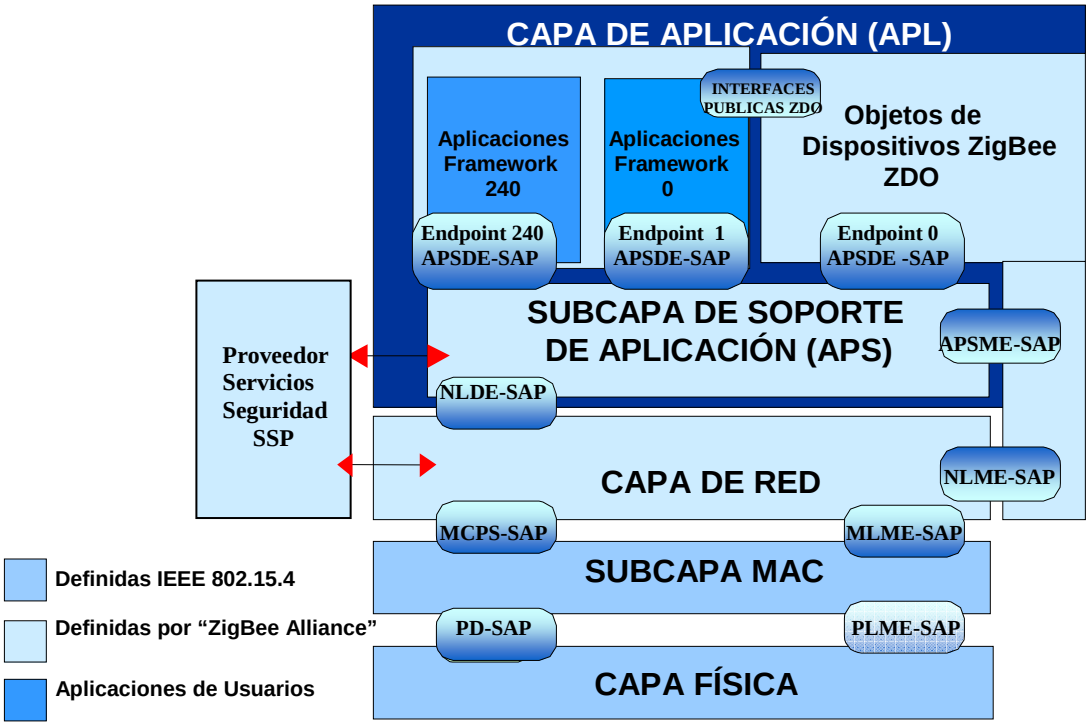

Figura 2.8 Arquitectura ZigBee

2.3.1 Capa Física

La capa física es responsable de las siguientes tareas principalmente [17]:

- La activación y desactivación del transceptor radio del dispositivo,
- selección de frecuencia del canal y
- la transmisión de los datos y recepción.
- Incluye sistemas ED, LQI y Valoración de Canal Libre(CCA *Clear Channel Assessment*)

La recepción del ED es usada por la capa de red como parte de la selección del canal cuando se quiera formar una red. Esto es una estimación de la potencia de la señal recibida dentro del canal presente de acuerdo a los parámetros de sensibilidad establecidos para cada frecuencia.

El LQI es una característica de la fuerza o calidad de un paquete recibido. Esta medida puede ser implementada usando ED o SNR (relación señal a ruido) o por la combinación de estos métodos.

El CCA es usado para mirar si el canal esta ocupado o libre de acuerdo al ED y a las características de modulación y propagación. Se utilizan los siguientes modos para esto:

- Modo 1: energía arriba del umbral. El CCA reportará un medio ocupado al detectar cualquier energía por encima del umbral ED.
- Modo 2: portadora detectada únicamente. El CCA reportará un medio ocupado sólo en la detección de una señal con la modulación y las características de propagación IEEE 802.15.4. Esta señal puede estar arriba o debajo del umbral ED.
- Modo 2: portadora detectada con energía arriba del umbral. El CCA reportará un medio ocupado sólo en la detección de una señal con la modulación y las características de propagación IEEE 802.15.4 con energía por encima del umbral ED.

2.3.1.1 Parámetros

- **Frecuencias de operación**

IEEE 802.15.4 proporciona dos capas físicas de operación en frecuencias separadas 868/915 MHz y 2.4 GHz. La capa física a 2.4 Ghz especifica la operación en la banda Industrial, Médica y Científica (ISM) disponible prácticamente en todo el mundo. La capa física a 868/915 MHz, en su frecuencia más baja especifica la operación en Europa y la más alta en la banda ISM de los Estados Unidos. Algunos parámetros establecidos en función de la banda utilizada se muestran en la tabla 2.1. La decisión de elegir una banda u otra depende obviamente de la localización geográfica y del mercado al que se destine la aplicación.

Tabla 2.1 Parámetros de la capa física

Capa Física	Banda	Parámetros de los Datos			Parámetros de Propagación	
		Velocidad de Bits (Kb/s)	Velocidad de Símbolos (kbaud)	Modulación	Velocidad de Chip (Chips/s)	Modulación
868/915MHz	868.0-868.6MHz	20	20	BPSK	300	BPSK
	902.0-928 MHz	40	40	BPSK	600	BPSK
2.4 GHz	2.4-4.4835 GHz.	250	62.5	O-QPSK	2000	O-QPSK

Las modulaciones que se utilizan en las bandas de operación (868/915 MHz y 2.4 GHz) cumplen los requisitos de simplicidad y facilitan la implementación en relación a modulaciones más complejas usadas en sistemas de comunicaciones modernos; se basa en métodos de Secuencia Directa de Espectro Extendido (DSSS *Direct Sequence Spread Spectrum*) que mejora considerable la calidad de la transmisión al recibir correctamente la señal. También permite funcionar en bandas no licenciadas ya pobladas coexistiendo con otras tecnologías, aumenta el ancho de banda mejorando la fiabilidad de la comunicación y no exige una

sincronización tan grande como CDMA lo que permite tener redes escalables hasta cantidades muy elevadas de dispositivos sin problemas.

Se definen 27 canales (0 hasta 26) de frecuencia entre las tres bandas, como se muestra en la tabla 2.2. La capa física a 868/915 MHz soporta un solo canal entre los 868 y los 868.6 MHz a una tasa de transmisión de 20 kbps; diez canales entre los 902.0 y 928.0 MHz a una tasa de transmisión de 40 kbps. Las dos bandas se consideran lo suficientemente cercanas en frecuencia, por lo tanto, es posible utilizar el mismo hardware para ambos y así reducir costos. La capa física a 2.4 GHz soporta 16 canales entre los 2.4 y los 2.4835 GHz con un amplio espacio entre canales (5 MHz), con el objetivo de facilitar los requerimientos de filtrado en la transmisión y en la recepción, a una tasa de transferencia de 250 kbps como lo muestra la figura 2.9.

Tabla 2.2 Bandas de frecuencia con el número de canales soportados

Banda de Frecuencia (MHz)	Tasa de Bits (Kb/s)	Número de canales
868 - 868.6	20	1
902 – 928	40	10
2400 – 2483.5	250	16

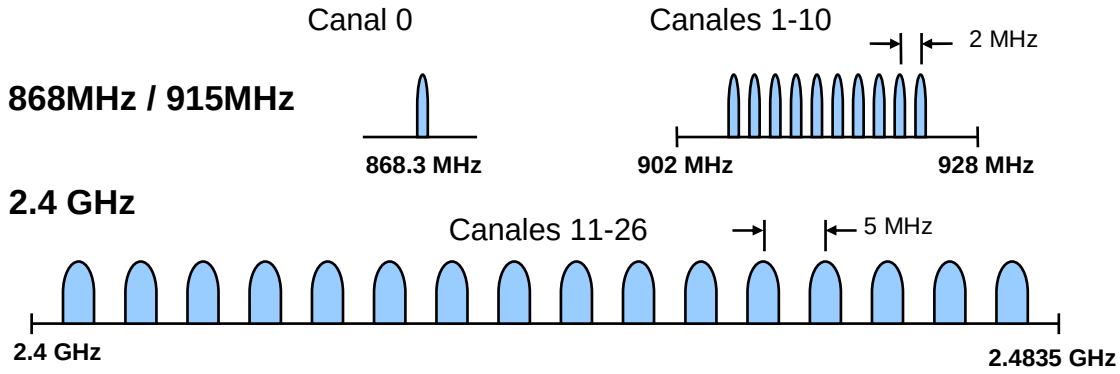

Figura 2.9 División del espectro y canales en la capa Física

La frecuencia central de los canales esta definida de la siguiente forma:
Fc = 868.3 en MHz, para k = 0
Fc = 906 + 2 (k–1) en MHz, para k = 1, 2,..., 10
Fc = 2405 + 5 (k–11) en MHz, para k = 11, 12,..., 26
Donde k es el número del canal.

- **Sensibilidad del receptor y Potencia del transmisor**

El estándar IEEE 802.15.4 no establece ninguna potencia de transmisión máxima, por lo tanto se puede usar cualquiera y como potencia mínima -3dBm para conseguir unas distancias de transmisión aceptables.

La sensibilidad mínima requerida por el receptor variará según la banda en la que se trabaje, si bien, ambas bandas tienen una limitación relativamente pequeña,

debido a que necesitan poca potencia de señal de entrada para funcionar correctamente, el estándar especifica - 85 dBm para la capa física a 2.4 GHz y de -92 dBm para la capa de 868/915 MHz, garantizando que el receptor no debe ser demasiado complicado, reduciendo el costo de fabricación.

- **Selectividad del receptor**

Como se utiliza un sistema DSSS no se requiere una selectividad demasiada alta. Además, los canales del estándar IEEE 802.15.4 están muy espaciados entre si (5 Mhz a la banda de 2,4Ghz) en relación a su ancho de banda.

- **Selectividad del canal y bloqueo del canal adyacente**

El estándar IEEE 802.15.4 establece como mínimo un rechazo de canal adyacente para un correcto funcionamiento del sistema. En la banda de 868 Mhz no define rechazo porque sólo se dispone de un canal. Para las bandas de 915 Mhz y 2,4 Ghz establece que el sistema receptor debe ser capaz de rechazar un canal adyacente del mismo nivel de potencia que el canal útil. Por otra parte también establece que el sistema debe rechazar los canales secundarios interferentes (los que están separados 2 canales del canal útil) de hasta 30 dB de más potencia que la potencia útil.

- **Modulación**

La banda de 2,4 Ghz usa una modulación DSSS con un tipo de señalización ortogonal multinivel (técnica de modulación “16-ary cuasi-ortogonal”), que usa secuencia PN (pseudo ruido) de 32-chip (co….c31) para representar 1 símbolo y a la misma vez conseguir el espectro ensanchado, asegurando una velocidad de transmisión bastante elevada (devolviendo así más rápido al modo de bajo consumo) y al mismo tiempo usa una tasa de símbolos relativamente baja (minimizando así la potencia transmitida).

Por otra parte la secuencia de 32-chip a transmitir se divide en dos: par e impar; la primera se usa para la transmisión de la fase y la segunda para la transmisión de la cuadratura. Además, a la segunda se le añade un retardo de tiempo chip (Tc) para crear el offset de la modulación. Por lo tanto, se usan 16 chips para la fase y 16 chips para la cuadratura, de aquí su nombre.

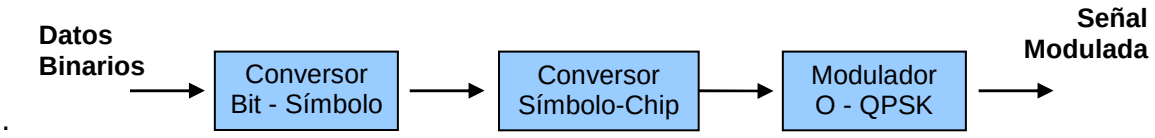

Figura 2.10 Diagrama en bloques del trasmisor de 2.4 GHz

El proceso para transmitir consiste en convertir los bits de datos (datos PPDU) a símbolos (2 bits por símbolo), separar la información de fase y de cuadratura, y asociarle una secuencia de 16 chips a cada una y a su vez, representar cada

símbolo por una secuencia PN de 32-chip (c0..c31) como lo muestra la tabla 2.3. El hecho de modular y transmitir la fase y la cuadratura por separado provoca el equivalente a usar 4 bits por símbolo. Por lo tanto cada bit de fase o de cuadratura utiliza 8 chips. En esta banda el estándar establece una tasa de símbolos de 62,5 símbolos/s, y como se trasmiten 4 bits por símbolo se tiene una tasa total de 250 kbps. Finalmente la velocidad de chip total es de 2 Mchips/s puesto que se transmiten 32 chips en 1 tiempo de símbolo (16 µs). Por lo tanto la velocidad de chip de uno de los canales (fase o cuadratura) es de 1 Mchips/s.

Las secuencias PN son concadenadas para que sean datos de símbolos exitosos, y la secuencia del chip es modulada en la portadora utilizando modulación O-QPSK con half-sine shaping, también conocida como MSK como la muestra la figura 2.10.

Cada byte del PPDU comenzando con el preámbulo y terminando con el último de la carga útil, se agrupan secuencialmente, es decir, los 4 LSBs (b0, b1, b2, b3) se procesan primero dentro de un símbolo, y los 4 MSBs (b4, b5, b6, b7) son mapeados después en el siguiente símbolo. Para la transmisión de los chips a través de la modulación O-QPSK, el menos significativo C_0 es transmitido primero y el chip más significativo C_{31} es transmitido de último.

Tabla 2.3 Mapeo de Símbolo a Chip

Decimal	Binario (b_0,b_1,b_2,b_3)	Valores del Chip (c_0...c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

La banda de 868/915 Mhz a diferencia de la banda de los 2,4 Ghz no implementa ningún sistema complejo de codificación ni de offset. Esta banda asigna a cada símbolo un número de bits (1 bit por símbolo porque la modulación es BPSK) y a cada símbolo asignarle un chip-15 de máxima longitud de secuencia (secuencia m) tal y como se representa en la figura 2.1.1.

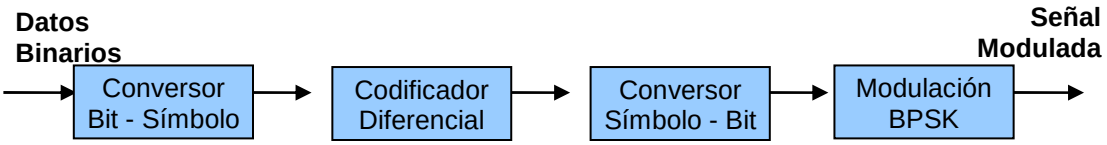

Figura 2.11 Diagrama en bloques del trasmisor de 868/915 Mhz

En la etapa de codificación diferencial, si el bit a la entrada es “0” se transmite a la salida del canal RF, el bit con la misma fase que el bit anterior, y si el bit de entrada es “1”, a la salida del modulador BPSK se transmite el bit actual en contrafase respeto al anterior. Por otra parte la conversión de símbolo a chips se hace por inversión del código. Es decir, se transmite el código de 15 chips cuando se debe transmitir un “1” y se transmito el código inverso cuando se quiera representar un “0”.

En términos de eficiencia (energía requerida por bit), la señalización ortogonal mejora el funcionamiento en 2 dB que BPSK diferencial. Sin embargo, en términos de sensibilidad de recepción, la capa física 868/915 MHz tiene una ventaja de 6-8 dB debido a que tiene velocidades de transmisión más bajas. Por supuesto, que en ambos casos las pérdidas de implementación debido a la sincronización, forma del pulso, simplificaciones en el detector y demás cosas, resultan en desviaciones en sus curvas óptimas de detección.

- **Acceso al Canal**

El acceso al canal se gestiona desde la capa MAC, pero es importante en la capa física porque esta tiene que implementar muchas funcionalidades para que la capa MAC pueda gestionarlo.

El acceso al medio en ZigBee es independiente del tipo de red y topologías usadas, y sólo depende si transmite en el modo con supertramas o no. En el caso que no se trasmitan supertramas se accede al medio usando el acceso CSMA/CA ranurado. En el caso contrario se usará el CSMA/CA no ranurado.

- **Formato de Trama**

La capa física dispone de una trama conocida como la Unidad de Datos del Protocolo de la Capa Física (PPDU *PHY Protocol Data Unit*). Las tramas de capas superiores se van encapsulando dentro las tramas de niveles inferiores y, por lo tanto, el PPDU es el último encapsulado antes de acceder al canal y transmitir.

Las dos bandas de frecuencia en las que se trabaja comparten una estructura simple de trama (figura 2.12). Cada PPDU contiene un encabezado de sincronización (SHR *Synchronization Header*), un encabezado de la capa física (PHR *PHY Header*) y la unidad de datos de la capa física (PSDU *PHY Service Data Unit*).

La cabecera de sincronización es independiente de la banda en que se trabaje y consiste en 2 campos básicos: un preámbulo de 32 bits fijados todos a cero, que permite al receptor sincronizarse correctamente con el emisor (estos ceros se agrupan en símbolos y se codifican en la secuencia de chips por lo tanto no serán ceros reales a la hora de transmitir) y un campo que delimita el inicio de la trama (SFD *Start-of-Frame Delimiter*), que consiste en una secuencia determinada de 8 bits ("11100101") que permite al receptor establecer el inicio del paquete.

La cabecera de la capa física es de 8 bits dónde el bit más significativo está reservado y los otros 7 bits están destinados a informar la longitud del paquete (por lo tanto la longitud máxima es de 128 bytes). Los paquetes de longitud entre 0 y 4 bytes y entre 6 y 7 bytes están reservados, los paquetes de 5 bytes son paquetes de ACK que contienen una trama MAC de ACK y los paquetes de 9 o más bytes son paquetes con datos útiles para las capas superiores a la física.

La carga útil es un único campo compuesto por el PSDU. Este campo Puede variar de entre 0 y 128 bytes y lleva todos los datos útiles del PPDU, es decir aquí se encapsulan los datos de las capas superiores.

<table>
<tr><th>Bytes : 4</th><th>Bytes :1</th><th colspan="2">Bytes: 1</th><th>Bytes: Variables</th></tr>
<tr><td>Preámbulo</td><td>Delimitador de Inicio de Trama (SFD)</td><td>Longitud de la trama (7 bits)</td><td>Reservado (1 bit)</td><td>PSDU</td></tr>
<tr><td colspan="2">SHR</td><td colspan="2">PHR</td><td>Carga Útil</td></tr>
</table>

Figura 2.12 Estructura de Trama Capa Física

2.3.1.1 Servicios de la Capa Física

La capa física ofrece dos servicios accedidos a través de dos puntos de acceso: el servicio de datos de la capa física (PD *PHY Data*) accedido por medio del PD - SAP y el servicio gestión conocido como la entidad de gestión de la capa física (PLME *Physical Layer Management Entity*) accedido por el PLME-SAP. El PLME provee las interfaces a través de las cuales las funciones de gestión pueden ser invocadas.

- **Servicio de Datos**

El servicio de datos de la capa física PD-SAP se encarga de gestionar todas las peticiones de datos que lleguen a la capa física ya sea de la capa MAC o mediante la transmisión de otro dispositivo. El servicio de datos ofrece a la capa MAC una única primitiva con tres funcionalidades como lo muestra la tabla 2.4.

Tabla 2.4 Primitivas PD-SAP

Primitiva	Petición.	Confirmación.	Indicación.
PD-DATA	Solicita la transferencia de un MPDU.	Confirma la transmisión de un MPDU	Indica la transferencia de un MPDU

- **Servicio de Gestión**

El servicio de administración (gestión) PLME-SAP de la capa física controla y gestiona las propiedades de la comunicación y el control de la radio mediante el transporte de comandos de administración entre la entidad de gestión de la subcapa MAC (MLME MAC *sublayer management entity*) y el PLME. El PLME también es responsable de mantener la base de información PAN (PIB) de la capa física. La tabla 2.5 muestra las diferentes primitivas que se manejan en el servicio de gestión.

Tabla 2.5 Primitivas PLME-SAP

Primitiva	Categoría	Petición.	Confirmación.
PLME-GET	Propiedades de la comunicación	Solicita la obtención de un atributo de PIB de la capa física.(Propiedades básicas de la configuración de la capa física como la potencia de transmisión, la última trama que se ha recibido , etc)	Reporta si el atributo solicitado estaba en el PIB.
PLME-SET		Solicita fijar el atributo indicado del PIB al valor dado.	Reporta si fue escrito al atributo indicado.
PLME-CCA	Mesura de energía RF	Solicita la realización de un CCA.(Hacer una medida del canal y mirar si está ocupado o libre)	Reporta los resultados del CCA.
PLME-ED		Solicita la realización de un ED (Detecta la energía del canal para la selección)	Reporta los resultados del ED.
PLME-SET-TRX-STATE	Control de radio	Solicita el cambio del estado del sistema de radio (Activar o desactivar la radio).	Reporta si se produjo el cambio de estado en el sistema de radio.

En todas estas primitivas, existes únicamente 2 tipos de funcionalidades (petición y confirmación), es decir, se recibe la petición y se enviará una confirmación si el cambio ha sido realizado. En la figura 2.13 se muestra el esquema de funcionamiento por las primitivas PLME-GET y PLME-CCA.

Las primitivas PLME-SET y PLME-SET-TRX-STATE seguirían el esquema de la primitiva PLME-GET mientras que la primitiva PLME–ED seguiría el esquema de la primitiva PLME-CCA.

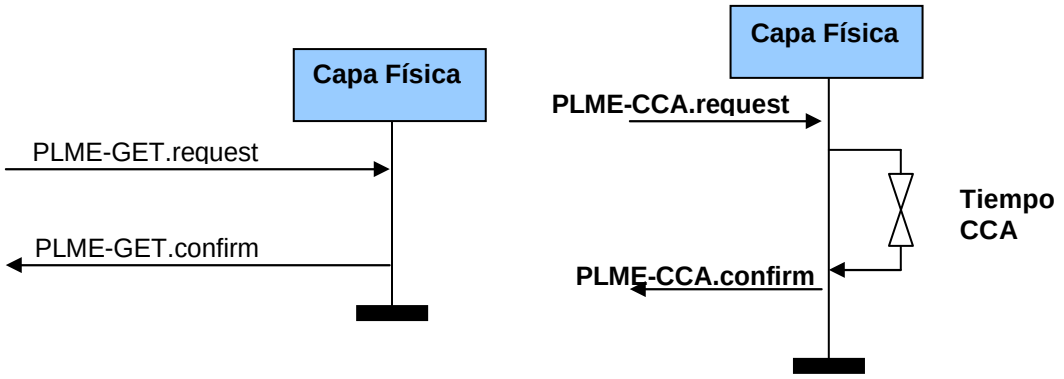

Figura 2.13 Funcionamiento de primitivas PLME-GET y PLME-CCA

2.3.2 Subcapa MAC

Los estándares 802 definidos por la IEEE han dividido la Capa de Enlace de Datos en dos subcapas: la subapa de Control al Medio y del Control Lógico del Enlace, con el propósito de mantener compatibilidad con las especificaciones del Modelo OSI.

La subcapa del Control Lógico del Enlace esta definida de igual forma para todos los estándares, mientras la subcapa MAC depende de la parte física y suministra una interfaz entre la Capa Física y los Servicios Específicos de Convergencia de Capas que proporcionan la interfaz con la subcapa Control Lógico del Enlace

La subcapa MAC define las siguientes tareas en el estándar IEEE 802.15.4 [17]:
- generación y sincronización de redes *beacon* (guías),
- soporta asociación y disociación,
- reconocimientos de entrega de trama (ACK),
- control de garantía de ranuras de tiempo (Slot Time) y
- emplea el mecanismo CSMA- CA para acceso al canal.
- encriptación AES (128 bits) para seguridad.

2.3.2.1 Formato de Trama

La trama general MAC o unidad de datos MAC (MPDU *MAC protocol data unit)* es muy sencilla, por tal razón contiene tres componentes básicos como lo muestra la figura 2.14**:**

a) Una cabecera MAC (MHR *MAC header*), que comprende la trama de control, número de secuencia, y la información de la dirección que no se incluyen en todas las tramas.
b) Carga útil MAC, de longitud variable, contiene información específica del tipo de trama. Las tramas de reconocimiento (ASK) no contienen una carga útil.

c) Una secuencia de chequeo de trama (FCS *Frame Check Sequence*)

Estas tramas MAC se incluyen para ser transmitidas dentro de un paquete de la capa física.

<table>
<tr><td>Octetos: 2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Control de Trama</td><td rowspan="2">Número de Secuencia</td><td>Identificador PAN Destino</td><td>Dirección Destino</td><td>Identificador PAN Fuente</td><td>Dirección Fuente</td><td rowspan="2">Carga Útil</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Campos de Direccionamiento</td></tr>
<tr><td colspan="6">MHR</td><td>Carga Útil MAC</td><td>MFR</td></tr>
</table>

Figura 2.14 Trama general MAC

- **Cabecera MAC (MHR)**

- **Campo de control de trama**

Es una trama que contiene 9 subcampos en los cuales se define principalmente el tipo de de trama (ver tabla 2.6) y banderas de control como un identificador que indica si el emisor de la trama espera una confirmación de recepción (trama ACK), es decir, especifica como es el resto de la trama de datos y que es lo que contiene, además si la seguridad esta habilitada o si existen tramas pendientes.

Tabla 2.6 Tipo de Tramas Subcapa MAC

Valor del Tipo de Trama	Descripción
000	Beacon
001	Datos
010	ACK
011	Comandos
100-111	Reservado

- **Campo número de secuencia.**

El campo número de secuencia es el identificador de la trama para que el emisor y el receptor no confundan la trama con otra enviada previa o posteriormente, este campo está en función del paquete de origen y se incrementa para cada clase de trama que sea enviada.

- **Campo de direccionamiento**

Este campo depende de las diferentes tipos de tramas que se envían (tramas de datos, beacon, ACK y comandos MAC). Contiene las direcciones de la red necesarias para la transmisión, dependiendo de la topología de la red y de otros factores (como el tipo de trama, etc.) que se incluyan en este campo, sólo la dirección de origen, la de destino, o las dos. Las direcciones pueden ser de 16 bits o de 64 bits de acuerdo a la configuración de la red; esta flexibilidad en la estructura ayuda a incrementar la eficiencia del protocolo al mantener los paquetes lo más reducidos posibles.

- **Identificador PAN destino.**

Tiene la dirección de la red PAN del receptor donde va dirigida la trama. Este campo está incluido en la trama MAC únicamente si el subcampo del modo de direccionamiento destino del campo de control es distinto a cero.

- **Dirección destino**

Especifica la dirección del receptor deseado de la trama. Su longitud depende del subcampo del modo de direccionamiento destino del campo del control y esta incluida en la trama MAC si este subcampo es distinto de cero.

- **Identificador PAN fuente.**

Tiene la dirección de la red PAN de donde sale la trama hacia su destino. Este campo está incluido en la trama MAC solamente si el modo de direccionamiento fuente y los subcampos intra-PAN del campo de control de trama son distintos a cero o iguales a cero, respectivamente.

- **Dirección fuente.**

Este campo especifica la dirección del dispositivo origen de donde sale la trama. Este campo está incluido en la trama MAC solamente si el subcampo del modo de direccionamiento fuente del campo de control de trama es distinto a cero.

- **Campo carga útil**

Es de longitud variable; sin embargo, la trama completa de MAC no debe de exceder los 127 bytes de información y se destinan al transporte de los datos de cada tipo de trama (trama beacon, trama de datos, trama ACK y tramas de comandos MAC), por lo tanto, puede estar dividido en múltiples campos según la funcionalidad de la trama y dependerá de cada una de ellas. Solo las tramas de datos y beacon contienen información que proviene de capas superiores; las tramas de mensajes “ACK” y la de comandos MAC originados en el MAC son usados para las comunicaciones MAC igual – igual..

- **Campo FCS**

Este campo es utilizado para el chequeo mediante 16 bits de redundancia cíclica (CRC *Cyclic Redundancy Chech*). Esta verificación se realiza con el polinomio de grado 16.

2.3.2.2 Tipos de Tramas

La subcapa MAC define cuatro tipos de tramas para que se ajusten a las necesidades de las diferentes aplicaciones con diversas topologías de red y al mismo tiempo mantener un protocolo simple y económico en el consumo de potencia.

- **Trama Beacon**

Este tipo de trama es un mecanismo para controlar el consumo de potencia y sincronizar todos los nodos de la red, añadiendo de esta manera un nuevo nivel de funcionalidad. Los dispositivos pueden activarse solamente cuando es transmitida una señal beacon para saber si ésta es para ella, o anunciar su presencia en al red, el resto de tiempo permanecen inactivos logrando de esta manera un ahorro de energía.

Los campos MHR de la trama beacon son los mismos que la trama básica, los componentes de la carga útil se divide en 4 campos como lo muestra la figura 2.16.

Octetos: 2	1	4/10	2	variable	variable	variable	2
Control de Trama	Número de Secuencia	Campos de Direccionamiento	Especificación Supertrama	GTS	Dirección Pendiente	Carga Útil Beacon	FCS
MHR			Carga Útil MAC				MFR

Figura 2.15 Formato Trama Beacon

Esta trama beacon especifica todo lo relacionado con las características de la supertrama, es decir los parámetros de GTS,CAP,CFP, sea el caso, además el campo Direccionamiento Pendiente, informa desde que direcciones se va a transmitir o recibir tramas. La carga útil, se utiliza para llevar información de capas superiores o información encriptada en caso de usar el algoritmo de encriptación AES establecido en el estándar.

- **Trama de datos**

Esta trama trasmite los datos (carga útil) provenientes de capas superiores. Los campos MHR de la trama de datos son los mismos que la trama básica como lo muestra la figura 2.17.

Octetos: 2	1		Variable	2
Trama de Control	Número de Secuencia	Campo de Direccionamiento	Carga Útil Datos	FCS
MHR			Carga Útil MAC	MFR

Figura 2.16 Formato Trama de Datos

- **Trama de Reconocimiento**

Se envía para confirmar la correcta recepción de la trama que se recibió, y solamente si la recibida lo indica.

Como las tramas tienen que ser lo más cortas posibles para minimizar el tráfico en la red, ésta no tiene campos de dirección ni carga útil como lo muestra la figura

2.18. Cuando un dispositivo recibe una trama ACK, para identificar si es para él, como no existe campo de dirección, mira si esperaba recibir una trama ACK y si el número de secuencia es el correcto.

Octetos : 2	1	2
Control de Trama	Número de Secuencia	FCS
MHR		MFR

Figura 2.17 Formato Trama ACK

- **Trama de comandos MAC**

La trama de comandos MAC (ver figura 2.18) tiene como objetivo trasmitir todos los comandos definidos en el estándar 802.15.4 tales como asociación, desasociación, sincronización con coordinadores, etc., de la capa MAC de un dispositivo a otro.

Octetos: 2	1		1	Variable	2
Trama de Control	Número de Secuencia	Campo de Direccionamiento	Identificador de Comando	Carga Útil Comando	FCS
MHR			Carga Útil MAC		MFR

Figura 2.18 Formato Trama de Comandos

Los campos MHR de la trama son los mismos que la trama básica como lo muestra la figura. La carga útil se divide en dos campos: el tipo de comando (ver tabla 2.7) que identifica el comando y la carga útil: que esta función del comando utilizado para trasportar los datos del tipo de comando seleccionada.

Tabla 2.7 Tipos de comandos MAC

ID del Comando	Tipos del Comando
1	Petición de de asociación
2	Petición a la respuesta de asociación
3	Notificación de desasociación
4	Petición de datos
5	Notificación de conflictos en el identificador del Coordinador
6	notificación de huérfano
7	Petición de Trama de Señalización (Beacon)
8	Realimentación del Coordinador
9	Petición de GTS
10-255	Reservados

2.3.2.3 Servicios de la Subcapa MAC

Los servicios que provee la subcapa MAC son accedidos a través de dos puntos de acceso: el servicio de datos de la capa MAC accedido por medio de MCPS (MAC *common part sublayer*)-SAP y el servicio de gestión accedido por medio de MLME-SAP. El MLME es la entidad de gestión que conceptualmente incluye la subcapa MAC y proveen las interfaces a través de las cuales las funciones de gestión pueden ser invocadas

- **Servicio de datos MAC**

El MCPS-SAP dispone de dos tipos básicos de primitivas, las destinadas a la transmisión (MCPS-DATA) y las destinadas a eliminar los datos que proviene de las capas superiores que no son necesarios (MCPS-PURGE). La tabla 2.8 enumera las primitivas utilizadas por la MCPS-SAP.

Tabla 2.8 Primitivas MCPS-SAP

Primitiva	Petición	Confirmación	Indicación
MCPS-DATA	Solicita la transferencia de una trama de datos MAC a un dispositivo remoto.	Reporta los resultados de la solicitud de transferencia de una trama de datos MAC	Indica que trama de datos MAC fue recibida desde el dispositivo remoto.
MCPS-PURGE	Permite que la capa superior borre datos de la cola de transmisión.	Permite que la subcapa MAC notifique a la capa superior sobre la petición de borrar un datos de la cola de transmisión	

- **Servicio de gestión MAC**

El servicio de gestión MLME-SAP controla y gestiona las propiedades de la comunicación, el control de la radio y propiedades de red mediante el transporte de comandos de administración entre el MLME y la entidad de gestión de la capa de red. El MLME es responsable de mantener la base de información PAN (PIB) de la subcapa MAC. La tabla 2.9 muestra las diferentes primitivas que se manejan en el servicio de gestión.

Tabla. 2.9 Primitivas MLME-SAP

Primitiva	Categoría	Petición	Confirmación	Respuesta	Indicación
MLME-GET	Propiedades de la comunicación	Solicita información sobre un determinado atributo del PIB	Reporta los resultados de una solicitud de información desde el MAC PIB.		
MLME-SET		Intenta escribir un determinado valor a un atributo indicado del MAC PIB.	Reporta los resultados de intentar escribir un determinado valor a un atributo indicado del MAC PIB		
MLME-RESET		Permite a la capa superior solicitarle a la subcapa MAC ejecutar un reset e operación.	Reporta el resulta del reset de operación.		
MLME-RX-ENABLE	Control de radio	Permite a la capa superior solicitar que el receptor este habilitado por un determinado tiempo.	Reporta el resultado de habilitar el receptor		
MLME-SCAN		Comienza la exploración de un canal sobre una determinada lista de canales. El canal explorado puede ser usado para medir la	Reporta el resultado de la solicitud de la exploración del canal.		

		energía del canal, buscar el coordinador con el cual esta asociado, o buscar todos los coordinadores que están transmitiendo tramas beacon con el POS del dispositivo de exploración			
MLME-ASSOCIATE	Gestión De la red.	Permite a un dispositivo realizar la petición para la asociarse a un coordinador.	Es usada para informar a la capa superior si la petición del dispositivo para asociarse fue satisfactoria o no.	Usado para iniciar una respuesta a la primitiva MLME-ASSOCIATE.indication	Indica la recepción de un comando de petición de asociación.
MLME-DISASSOCIATE		Es usada para informarle a un coordinador que un dispositivo asociado quiere desasociarse.	Reporta el resultado del comando de petición de disociación.		Empleada para indicar la recepción de un comando de petición disociación.
MLME-GTS		Permite a un dispositivo enviar una solicitud a un coordinador para asignar espacio a un nuevo GTS o cancelar el espacio de un GTS existente.	Reporta los resultados de la solicitud para asignar espacio a un nuevo GTS o cancelar el espacio de un GTS existente.		Indica que ha sido asignado un nuevo espacio al GTS o que el espacio que estaba asignado ha sido cancelado.
MLME-ORPHAN				Permite a la capa superior responderle al coordinador de la notificación acerca que existe un dispositivo solo.	Permite notificar a la capa superior la presencia de un dispositivo (coordinador o no)
MLME-SYNC		Solicita la sincronización con el coordinador.			
MLME-SYNC-LOSS					Indica la perdida de sincronización con el coordinador
MLME-START		Realiza una solicitud para que el dispositivo comience a usar una nueva configuración de supertrama.	Reporta los resultados de intentar realizar una solicitud para que el dispositivo comience a usar una nueva configuración de supertrama		
MLME-BEACON NOTIFY					Es empleada para enviar parámetros en una trama beacon desde la capa MAC hacia la capa superior.
MLME-POLL		Pregunta el coordinador remoto si hay un dato pendiente del	Reporta el resultado de solicitud de si existe un dato pendiente.		

		dispositivo local.			
MLME-COMM STATUS					Permite a la subcapa MAC indicar el estado de la conexión.

2.3.2.4 Seguridad

El estándar IEEE 802.15.4 proporciona tres modos de seguridad:

- Sin seguridad.
- Listas de control de acceso a la red: proporcionan servicios de seguridad para la comunicación entre dispositivos conocidos, pero limitada porque no provee seguridad criptográfica (algoritmos de cifrado complejos).
- Modo seguro: cuando se trasmite en el modo seguro se puede emplear cualquier de servicio de seguridad que emplea llaves simétricas proporcionadas por procesos de la capa superior: los servicios de seguridad son los siguientes:

    - Lista de control de acceso: un dispositivo tiene una lista de control de acceso para determinar de cuales dispositivos planea recibir tramas.
    - Encriptación de datos: Usando el estándar de encriptación avanzado (AES *Advanced Encryption Standard*)
    - Integridad de trama: usa un Código Integrado de Mensaje (MIC *Message Integrity Code*) para proteger datos que están siendo modificados por terceros sin la llave criptográfica. La integridad de los datos se realiza en las tramas beacon, comandos y datos
    - Secuencia freshness: Utiliza un orden de secuencia de entrada para rechazar tramas que han sido enviadas. Cuando una trama es recibida, el valor de freshness es comparado con el de último valor, si este es más reciente que el último, entonces la comprobación ha pasado, y el valor de freshness ha sido actualizado con el valor reciente. Si el valor de freshness no es más reciente entonces el chequeo ha fallado.

Todos estos servicios son proporcionados por un grupo de operaciones de seguridad llamados suites de seguridad,que se basan en tres modalidades de operación: el modo de conteo (CTR *Counter Mode*) para la encriptación, el modo autenticación de mensajes asociando bloques de codificación (CBC-MAC Cipher Block Chaining Message Authentication Code) para la integridad y una combinación de encriptación e integridad llamado el modo CCM (CTR + CBC-MAC), empleando AES como lo muestra la tabla 2.10.

Tabla 2.10 Seguridad Subcapa MAC

Suite de Seguridad	Control de Acceso	Encriptación de datos	Integridad de Tramas	Freshness (Opcional)
AES-CTR	X	X		
AES-CCM-128	X	X	X	X
AES-CCM-64	X	X	X	X
AES-CCM-32	X	X	X	X
AES-CBM-MAC-128	X		X	X
AES-CBM-MAC-64	X		X	
AES-CBM-MAC-32	X		X	

2.3.3 Capa de Red

La capa de red suministra la funcionalidad para garantizar una correcta operación de la subcapa MAC y para proveer una adecuada interfaz de servicio para la capa de aplicación. Esta capa incluye mecanismos usados para formar y mantener una red, asociarse y desasociarse de ella, capacidades de enrutamiento y direccionamiento, asignación de direcciones a dispositivos entre otros [18] [25].

2.3.3.1 Formato de Trama

El formato general de la trama de la capa de red o unidad de datos de protocolo de la capa de red (NPDU *Network Layer Protocol Data Unit*), esta compuesta por una cabecera y una carga útil (ver figura 2.20).

<table>
<tr><th>Octetos : 2</th><th>2</th><th>2</th><th>0/1</th><th>0/1</th><th>Variable</th></tr>
<tr><td rowspan="2">Control de Trama</td><td>Dirección de Destino</td><td>Dirección Fuente</td><td>Radio Broadcast</td><td>Número de secuencia Broadcast.</td><td>Trama Carga Útil</td></tr>
<tr><td colspan="4">Campos de Enrutamiento</td><td></td></tr>
<tr><td colspan="5">Cabecera</td><td>Carga Útil</td></tr>
</table>

Figura 2.19 Trama general Capa de Red

- **Cabecera capa de red**

Los campos de control de trama, dirección destino y dirección fuente siempre estan presente, mientras que los campos de broadcast no pueden ser incluidos en todas las tramas.

- **Campo de control de trama**

El campo de control de trama contiene información sobre el tipo de trama (puede ser de datos o comandos NWK) como lo muestra la tabla 2.11, direccionamiento, campos de secuencia y otras banderas de control. Además permite descubrir la ruta del nodo y si se está usando seguridad en la red. El campo de control de trama se divide en 6 subcampos como lo ilustra la figura 2.21.

Bits: 0-1	2-5	6	7-8	9	10-15
Tipo de Trama	Versión del Protocolo	Descubrimiento de ruta	Reservado	Seguridad	Reservado

Figura 2.20 Campo de Control de Trama

Tabla 2.11 Valores del Tipo de Trama

Valores Tipo de Trama (b1,b2)	Nombre de Tipo de Trama
00	Datos
01	Comandos de Red
10-11	Reservado

- **Campo de dirección destino**

Esté campo contendrá la dirección de la red del dispositivo destino o la de broadcast.

- **Campo de dirección fuente**

Esté campo contendrá la dirección de red del dispositivo fuente.

- **Campo de radio broadcast**

El campo de radio broadcast está presente si la dirección destino de la trama es broadcast. y especifica el radio-limite (cobertura) de la transmisión broadcast.

- **Campo número de secuencia broadcast**

Está presente si la dirección destino de la trama es broadcast.y especifica la secuencia numérica de la trama broadcast. Esta secuencia se incrementa en uno cada vez que una nueva trama broadcast se trasmita.

- **Campo carga útil**

La carga útil tiene longitud variable y contiene la información del tipo de tramas.

2.3.3.2 Tipos de Tramas

- **Trama de datos**

La cabecera de la trama de datos es la misma de la básica, la carga útil llevará información indicada por las capas superiores (vea figura 2.22)

Octetos: 2		Variable
Trama de Control	Campo de Enrutamiento	Carga Útil de Datos
Cabecera		Carga útil de la Capa de Red

Figura 2.21 Trama de Datos

- **Trama de comandos**

La cabecera de la trama de datos es la misma de la básica, el campo de identificador de comando indica el comando de la capa de red que se está usando y la carga útil contiene el comando usado (vea figura 2.23).

Octetos: 2		1	Variable
Trama de Control	Campo de Enrutamiento	Identificador de Comandos de Red	Carga Útil
Cabecera		Carga Útil de la Capa de Red	

Figura 2.22 Trama de Comando de la Capa de Red

Los comandos de la capa NWK estas definidos en la tabla 2.12.

Tabla 2.12 Comandos de la trama de Red

Valores Tipo de Trama (b1,b2)	Nombre del Comando
1	Petición de Enrutamiento
2	Respuesta de Enrutamiento
3	Error de Enrutamiento
4-255	Reservado

Petición de enrutamiento (Route request): permite que un dispositivo le pida a otro dispositivo que están en la misma cobertura de la radio (alcance), que busquen un dispositivo (destino) en particular y establecer condiciones dentro de la red que permitan encaminar mensajes a ese destino.

Respuesta de enrutamiento (Route reply): permite que el dispositivo destino de un comando route request informe al origen que la petición ha sido recibida.

Error de enrutamiento (Route error): se usa cuando no se puede enviar la trama de datos y notifica al dispositivo fuente que la trama de datos no se pudo enviar.

2.3.3.3 Entidades de Servicio de la Capa de Red

Para interactuar con la capa de aplicación, el nivel de red conceptualmente incluye dos entidades de servicios,estas son: entidad de servicio de datos conocida como (NLDE -*NWK layer data entity*) y entidad de servicio de gestión (NLME - *NWK layer management entity*).

La entidad de datos de la capa de red provee el servicio de transporte de datos y la entidad de gestión provee el servicio de gestión. El NLME mantiene una base de datos de objetos de gestión conocida como base de información de red (NIB).

- **Entidad de datos**

El NLDE proveerá un servicio de datos para permitir el transporte de unidades de datos de protocolo de aplicación (APDU *Aplication Layer Protocol Data Unit*) entre dispositivos de la misma red.

La entidad NLDE proporciona dos servicios: generar un NPDU desde un APDU a través de la adición de un encabezado apropiado y trasmitirlo para un dispositivo, ya este sea el destino final de la comunicación o el siguiente paso hacia el destino final.

- **Entidad de gestión**

La entidad MLDE proporciona los siguientes servicios:

- Configurar un nuevo dispositivo como coordinador, enrutador o un dispositivo final.
- Establecer una nueva red.
- Asociación y disociación de un dispositivo cualquiera a la red.
- Generar direcciones por medio de coordinadores o routers para dispositivos que se asocian a la red.
- Descubrir, registrar y reportar información relacionado con los vecinos que se encuentre a un salto.
- Descubrir y registrar caminos a través de la red por medio de los cuales los mensajes puede ser eficazmente encaminados.

2.3.3.4 Servicios de la Capa de Red

La capa de NWK provee dos servicios, accedidos a través de dos SAP. Estos son: el servicio de datos de NWK, accedido a través del NLDE - SAP y el servicio de gestión de NWK accedido por medio de NLME - SAP.

- **Servicios de datos**

El NLDE-SAP permite el trasporte de APDU entre entidades iguales de aplicación. La tabla 2.13 resume los primitivas utilizadas por el NLDE-SAP.

Tabla 2.13 Primitivas NLDU-SAP

Primitiva	Petición	Confirmación	Indicación
NLDE-DATA	Solicita la transferencia de un NSDU desde una entidad APS para uno o más entidades APS.	Confirma el resultado de una solicitud para la transferencia de un NSDU.	Indica la transferencia de un NSDU desde la capa de red a una entidad de la APS.

- **Servicios de gestión**

El NLME-SAP permite el transporte de comandos de gestión entre la capa superior y la entidad NLME. La tabla 2.14 resume las primitivas utilizadas por el NLME-SAP.

Tabla 2.14 Primitivas NLME-SAP

Primitiva.	Petición.	Indicación.	Confirmación
NLME-NETWIORK-DISCOVERY	Solicita el descubrimiento de redes.		Confirma el resultado del descubrimiento de redes.
NLME-NETWIORK-FORMATION	Solicita que un dispositivo comience una nueva red y el como coordinador.		Confirma la inicialización de un coordinador ZigBee en una red ZigBee.

NLME-PERMIT-JOINING	Solicita que un coordinador o router ZigBee coloque la bandera de unión de la subcapa MAC en un periodo fijo, durante el cual se pueden aceptar dispositivos en la red.		Confirma el resultado de la petición para permitir nuevos dispositivos en la red.
NLME-START-ROUTER	Solicita que un coordinador y router ZigBee cambien la configuración de la supertrama, y que el router la inicialice.		Confirma el resultado de la petición de cambiar o inicializar la supertrama por un coordinador o router ZigBee.
NLME-JOIN	Solicita que un dispositivo ingrese a la red, por unión directamente o porque esta sin red.	Indica cuando un nuevo dispositivo ha sido unido a la red.	Confirma el resultado de la petición para unión una red.
NLME-DIRECT-JOIN	Solicita que un coordinador o router ZigBee unan directamente un dispositivo a la red.		Confirma el resultado de la petición para unir un dispositivo directamente a la red.
NLME-LEAVE	Solicita que un dispositivo deje la red.	Indica cuando un dispositivo a sido desasociado de la red.	Confirma que un dispositivo se ha desasociado de la red.
NLME-RESET	Solicita que se realice un reseteo de operación de red.		Confirma que se ha realizado un reseteo de operación en la red.
NLME-SYNC	Solicita sincronizar o adquirir cualquier dato de un coordinador o router ZigBee.	Indica de la perdida de sincronización en la subcapa MAC.	Confirma que la sincronización o extracción cualquier dato de un coordinador o router ZigBee.
NLME-GET	Solicita leer un valor de un atributo de la NIB.		Confirma el intento de leer un valor de un atributo de la NIB.
NLME-SET	Solicita escribir un valor de un atributo de la NIB		Confirma el intento de escribir un valor de un atributo de la NIB.

2.3.3.5 Funcionalidades de la Capa NWK

Las funcionalidades de la capa de red permiten a cualquier dispositivo ZigBee asociarse y desasociarse a una red; adicionalmente los routers y coordinadores ZigBee pueden crear y mantener una lista de los vecinos, asignación de direcciones y los coordinadores establecer una nueva red. Todas estas funcionalidades están dadas mediante las primitivas del servicio de gestión de la capa de red [19].

- **Establecimiento de una nueva red.**

Sólo los coordinadores pueden realizar la petición de iniciar una red, por lo tanto solo ellos la efectúan, después de la petición se efectúa un ED sobre canales

específicos o canales disponibles y un scan activo para encontrar redes en el espacio de operación. Cuando los datos se procesan se selecciona un identificador para la red, se realiza la selección del canal y se asigna una dirección. Después que todos los parámetros sean aceptados se confirma que el coordinador puede establecer una red.

- **Asociación a una red**.

Para que un dispositivo forme parte de una red, lo realiza mediante unión o asociación y solo los coordinadores y los enrutadores lo pueden hacer. La relación entre el dispositivo que asocia/une y el dispositivo que quiere asociarse/unirse a la red se llama relación padre (coordinador o enrutador)-hijo.

Un padre directamente puede aceptar a un hijo y unirlo a la red con la dirección IEEE de 64 bits, el hijo recibe una dirección lógica única para esa red de 16 bits para trasmisiones futuras.

Cuando un dispositivo quiere conectarse a la red mediante una petición de asociación, primero detecta los canales activos dentro de su rango de comunicaciones, después, se busca un padre adecuado en las tablas de vecinos. Si la asociación tuvo éxito el nuevo dispositivo recibe una dirección de 16 bits corta para la comunicación dentro de la red. Los dispositivos luego actualizan la información en sus tablas de vecino.

Las tablas del vecino contendrán información acerca de los dispositivos que están dentro de un rango especificado de transmisión. La información servirá para propósito diferentes y contiene información básica del dispositivo y de la red. También puede ser incrementada con más información. Una tabla se actualizará cada vez que un dispositivo recibe una trama desde el vecino.

Cada dispositivo tiene asociada una distancia en las tablas. Es decir, los saltos mínimos que una trama de datos tenga que realizar a través del padre para alcanzar al coordinador. El coordinador tiene 0 saltos y sus hijos tienen 1 salto. Los saltos máximos de la red son decididos por el coordinador.

- **Desasociación de una red**

La desasociación de una red se realiza por petición del hijo o del padre para que el dispositivo hijo salga de la red. Cuando es el hijo que se desconecta de la red o del padre, a esté procedimiento se le llama “Huérfano”.

- **Enrutamiento**

Los coordinadores y los enrutadores proveerán estas capacidades básicas de enrutamiento:

- transmitir trama de datos para las capas superiores y otros enrutadores ZigBee

- participar del descubrimiento de la ruta
- participar en la reparación de la ruta
- utilizar algoritmo ZigBee para la reparación y descubrimiento de las rutas.

Mediante el descubrimiento de la ruta los dispositivos cooperan para ello y establecen rutas entre una fuente en particular y los dispositivos destino; las reparaciones se dan cuando un enlace de comunicación experimenta o alcanza ciertos límites de desempeño.

Además coordinadores y enrutadores con cierta información manejan tablas de enrutamiento para mejorar las rutas disponibles. Estas tendrán una estructura como lo muestra la tabla 2.15. Si un dispositivo mantiene una tabla de enrutamiento, también mantendrá una tabla de descubrimiento ruta, para poseer una capacidad enrutamiento alta.

Tabla 2.15 Tabla de Enrutamiento

Nombre	Descripción
Dirección Destino	16 bits Dirección de Red
Status	Valor Predefinido de status
Próximo Dirección de salto (Hop)	16 bits Dirección del Próximo Salto

2.3.4 Capa de Aplicación

A pesar que esta capa está definida dentro del estándar ZigBee, no realiza ninguna aplicación final, solo define características y da las pautas para ínteroperar entre las diferentes soluciones técnicas que desarrollan los proveedores.

La capa de aplicación se divide en: la Subcapa de Soporte de Aplicación *(*APS *Application Support Sublayer*) destinada al correcto procesamiento de todas las tramas tanto de salida como de entrada y proporciona la interfaz con la capa de red; los objetos dispositivos de ZigBee *(ZDO ZigBee Device Object*) que administran los nodos de la red y la información de encaminamiento para transmitir correctamente los datos; y los Objetos de Aplicación definidos por el usuario los cuales se encuentran dentro de las aplicaciones framework.

Una aplicación en ZigBee de cualquier área se puede definir como un grupo de objetos aplicación situados en el mismo y/o diferente nodo. Por ejemplo, un uso del control de la iluminación puede consistir en los siguientes objetos de aplicación los sensores, los interruptores, los reguladores, y las lámparas.

Para especificar los objetos de aplicación primero se tiene que definir un perfil dentro del área específica. Los perfiles son acuerdos y formatos de mensajes para tener un lenguaje común para enviar y recibir datos, tener bien definido las acciones de procesamiento, confiabilidad y sencillez para los usuarios finales entre

otros. Los perfiles son desarrollados por proveedores de ZigBee que posibilitan la interoperabilidad entre dispositivos construidos por diferentes fabricantes y estos a su vez con el estándar ZigBee [20].

Cuando se definen los perfiles también se pueden especificar hasta 2^{16} descriptores, a su vez, cada descriptor puede tener máximo 256 clusters y cada cluster alcanza 2^{16} atributos. Esta flexibilidad permite que un nodo tenga un número muy grande de atributos, es decir dentro de un objeto de aplicación los puntos de entrada y salida. Por ejemplo, un termóstato puede contener un atributo de salida “temperatura” que representa la temperatura actual de un cuarto, un regulador del horno puede tomar este atributo como entrada y controlar el horno según el valor de la temperatura recibido del termóstato.

Una colección de atributos es llamada cluster, cada cluster se identifica con un identificador de cluster (clusterID) de 8 bits y único dentro del alcance de un perfil. Existen cluster de entrada y salida, los de entrada son el conjunto de atributos enviados por otros nodos y cluster de salida que son atributos que suministran datos para otros nodos.

Los descriptores son un conjunto de características que detallan las capacidades del dispositivo dentro de una red y permite a otros dispositivos pedir información acerca de él. La capa APL define tres descriptores obligatorios:

- Nodo Descriptor: describe el tipo y las capacidades del nodo. El tipo de un nodo puede ser coordinador, router o dispositivo final. Las capacidades de un nodo son propiedades como la banda de frecuencia, el tamaño máximo del buffer, tamaño máxima de transferencia, etc.
- Descriptor de potencia: da una indicación dinámica del estado de potencia del nodo.
- Descriptor simple: contiene información específica de cada punto final (endpoint) que contiene el nodo. Esto incluye el perfil del identificador, el número de entrada y de salida de cluster, etc.

Ahora bien, Los nodos ZigBee pueden tener varios dispositivos físicos conocidos como subunidades, ejemplo de ellas son los sensores, leds, interruptores, lámparas etc., las cuales se modelan por los objetos aplicación que son programas que controlan el hardware de cada subunidad; estos objetos se comunican por clusters, cuando dos dispositivos se unen, el cluster de salida de un dispositivo se conecta con el cluster de entrada del otro dispositivo. El número máximo de subunidades por nodo es de 240 y a cada uno se le asigna un endpoint.

Un endpoint son extensiones lógicas añadidas a un nodo que permite soportar múltiples aplicaciones y pueden ser considerados como los números de los puertos usados en TCP/IP, es decir, identifican cada subunidad, pueden haber desde 1 hasta 240 en cada nodo ZigBee y son descritos por medio de los

descriptores. Dos endpoint adicionales están definidos: el endpoint 0 para la interfaz del ZDO y el endpoint 255 es reservado para realizar una función broadcast de datos a todos los objetos de aplicación.

La transmisión de mensajes entre los objetos de aplicación se puede realizar de dos maneras: mediante la dirección que posee cada nodo o por medio de tablas de Binding conocida como indirecta.

Cuando se comunican por medio de tablas se utiliza un proceso conocido como Binding que es la creación de enlaces lógicos entre objetos de aplicación basado en sus servicios y necesidades. Para realizar la transmisión mediante binding el coordinador debe tener una tabla de binding con la siguiente información:

$$(a_s, e_s, c_s) = \{ (a_{d1}, e_{d1}), (a_{d2}, e_{d2}), \ldots, (a_{dn}, e_{dn}) \}$$ donde:

a_s = la dirección del dispositivo como fuente del enlace lógico.
e_s = el identificador endpoint como fuente del enlace lógico.
c_s = el clusterID usado en el enlace lógico.
a_{di} = la dirección e-nésimo del dispositivo como el destino del enlace lógico.
e_{di} = el e-nésimo identificador endpoint del dispositivo como el destino del enlace lógico

La comunicación por medio de las direcciones se divide en unicast y broadcast y es llamada directa. En la primera la comunicación es uno a uno, y la segunda cuando se envía un mensaje a una aplicación objeto ya sea a todos los dispositivos en la red, o las aplicaciones objeto en un dispositivo, o las aplicaciones objeto en todos los dispositivos en la red [21].

2.3.4.1 Subcapa de Soporte Aplicación (APS)

La subcapa de soporte de aplicación suministra la interfaz entre la capa de red y la entidad de la capa más alta (NHLE *next higher layer entity*) a través de dos servicios que son usados por los objetos de dispositivos ZigBee y los objetos de aplicación. Estos servicios son ofrecidos por dos entidades: entidad de servicio de datos (APSDE) y la entidad de servicio de gestión (APSME).

- **Entidad de datos APS**

La entidad de datos APS proporciona un servicio de datos para la capa NWK, los ZDO y los objetos de Aplicación.

El APSDE proporciona el siguiente servicio:
Genera una APDU , a través de la adición de un encabezado apropiado y realizar Binding cuando sea necesario.

- **Entidad de gestión de la APS**

La entidad de gestión APS (APSME) proporciona un servicio de gestión para permitir que una aplicación interactué con la arquitectura el protocolo, también es responsable de mantener una base de datos de objetos de gestión de la subcapa APS, conocida como la AIB (APS sub-layer information base).

El APSME proporciona los siguientes servicios:

- Binding
- Gestión de la AIB (Base de Información de la APS)
- Seguridad.

- **Servicios de la APS**

La subcapa APS proporciona dos servicios accedidos a través de dos SAP: servicios de datos APS accedidos a través de APSDE-SAP y servicios de gestión APS accedidos por medio de APSME-SAP. Estos dos servicios proveen la interfaz entre el NHLE y la capa de NWK.

- **Servicios de datos**

El APSDE-SAP soporta el trasporte de unidad de datos del protocolo de aplicación entre entidades iguales de aplicación. La tabla 2.16 resume los primitivas utilizadas por el APSDE-SAP.

Tabla 2.16 Primitivas APSDE-SAP

Primitiva	Petición	Confirmación	Indicación
APSDE-DATA	Solicita la transferencia de un NHLE PDU (ASDU) desde un NHLE local para una única entidad NHLE.	Confirma el resultado de una solicitud para la transferencia de un ASDU para un NHLE local.	Indica la transferencia de un ASDU desde la subcapa APS para una entidad local de aplicación.

- **Servicios de gestión**

El APSME soporta el trasporte de comandos de aplicación entre la capa superior y el APSEME. La tabla 2.17 resume los primitivas utilizadas por el APSME-SAP.

Tabla 2.17 Primitivas APSME-SAP

Primitiva	Petición	Indicación	Respuesta	Confirmación
APSME-BIND	Permite a la capa superior solicitar la asociación de dos dispositivos por medio de un coordinador o router ZigBee			Permite a la capa superior notificar del resultado de la petición de asociar dos dispositivos directamente o por un proxy.
APSME-GET	Permite a la capa			Reporta los resultados

	superior solicitar leer el valor de un atributo del AIB.			del intento de leer el valor un atributo del AIB
APSME-SET	Permite a la capa superior escribir el valor de un atributo del AIB.			Reporta los resultados del intento de escribir un valor en un atributo del AIB
APSME-UNBIND	Permite a la capa superior solicitar la desasociación de dos dispositivos por medio de un coordinador o router ZigBee			Permite a la capa superior notificar del resultado de la petición de desasociar dos dispositivos directamente o por un proxy

2.3.4.2 Formato de la Trama del APS

El formato de trama APS o APDU consiste en dos componentes como lo muestra la figura 2.23:

- Cabecera APS: contiene la trama de control e información sobre el direccionamiento.
- Carga Útil APS: contiene información específica sobre el tipo de trama.

Octetos: 1	0/1	0/1	0/2	0/2/8	variable
Control de Trama	Destino Endpoints	Identificador de Cluster	Identificador de Perfil	Fuente Endpoints	Carga Útil
	Campos de Direccionamiento				
Cabecera					Carga Útil

Figura 2.23 Trama APS

- **Campo de control de trama**

El campo de control de trama contiene información sobre el tipo de trama (ver tabla 2.18), el modo de entrega (transmisión unicast, dirección indirecta broadcast) y banderas de control para mirar si el endpoint va en la cabecera; si es usada la seguridad; o si es requerido un ACK. El control de trama se divide como lo muestra la figura 2.24

Bits 0-1	2-3	4	5	6	7
Tipo de trama	Modo	Fuente de Endpoints Presente	Seguridad	Petición ACK	Reservado

Figura 2.24 Trama Control de Trama APS

Tipo de Trama	Nombre de Tipo de Trama
00	Datos
01	Comandos
10	ACK
11	Reservado

Tabla 2.18 Tipos de Trama APS

- **Campo Destino endpoints.**

El campo destino endpoints específica el endpoint final del receptor final de la trama. Este campo siempre va incluido a menos que el tipo de trama sea de dirección indirecta.

- **Campo Identificador de cluster**.

El campo identificador de cluster específica el identificador del cluster que debe usarse en la operación binding en el coordinador ZigBee. Este campo va incluido a en la tramas de datos y ACK.

- **Campo identificador del perfil.**

El campo identificador del perfil identifica que endpoints deben recibir el mensaje. Este campo va incluido solamente en la trama broadcast. Mantendrá el identificador del perfil ZigBee para el cual el broadcast es deseado y esta durante el filtrado de mensajes en cada dispositivo que recibe una entrega del broadcast

- **Campo fuente endpoints.**

Especifica el endpoints de la trama inicial. Este campo va incluido en tramas de datos y ACK.

- **Campo carga útil**.

Contiene información específica de acuerdo al tipo de trama.

2.3.4.3 Tipos de Tramas

- **Trama de datos**

La cabecera de la trama de datos APS es la misma de la trama básica como lo muestra la figura 2.25**,** la carga útil para una trama de datos saliente contendrá los octetos que la capa superior ha pedido al servicio de datos APS para transmitir, para una trama entrante contiene los octetos que recibió por el servicio de datos APS Y eso debe reflejarse para los dispositivos destino o entregado para la siguiente capa superior si el coordinador fuera uno de los destinos.

Octetos: 1	0/1	1	0/2	1	2
Trama de Control	Destino Endpoint	Id Cluster	Profield	Fuente Endpoint	Carga Útil Datos
Cabecera					Carga Útil APS

Figura 2.25 Trama de Datos de APS

- **Trama de comandos APS**

La cabecera será la misma que la general (ver figura 2.26), el primer subcampo de la carga útil identifica que comando se va a utilizar en el siguiente subcampo

Octetos: 1	1	Variable
Control de Trama	Identificador de Comandos APS	Carga Útil
Cabecera	Carga Útil APS	

Figura 2.26 Trama de Comandos APS

- **Trama ACK APS**

La trama ACK es la misma cabecera de la trama General APS (APDU) sin el campo Identificador de Perfil como lo muestra la figura 2.27

Octetos : 1	0/1	1	1
Control de Trama	Destino Endpoint	ID Cluster	Fuente Endpoint

Figura 2.27 Trama ACK de APS

2.3.4.4 Framework de Aplicación

La framework de aplicación (AF) es el entorno en el cual los objetos de aplicación se almacenan en las subunidades de los dispositivos de ZigBee. Dentro de la aplicación framework, los objetos de aplicación envían y reciben datos a través del APSDE-SAP. El control y administración de los objetos de aplicación se realiza a través de las interfaces públicas que brinda ZDO.

El servicio de datos proporcionados por APSDE-SAP, incluye las primitivas de petición, confirmación e indicación para la transferencia de datos. Las primitivas de petición soportan transferencia de datos entre entidades iguales de objetos aplicaciones. La primitiva de confirmación reporta los resultados de un llamado a una primitiva de petición. La primitiva de indicación se usa para indicar la transferencia de datos desde la APS para la entidad destino de objetos de aplicación.

Usando los servicios ofrecidos por el APSDE-SAP, la aplicación framework proporciona dos servicios de datos para las aplicaciones objeto: valores pares de llaves (KVP *Key Value Pair*) y el servicio de mensaje genérico (MSG *Generic Message*).

El KVP permite definir y trasmitir datos de atributos mediante los siguientes comandos: eventos, set, get con ACK, set con ACK, event con ACK, get con response, set con response y event con reponse; usando una estructura en XML comprimido, mientras que el MSG utiliza un formato de trama libre.

- **Formato de la trama AF**

La trama AF es usada en la comunicación de las aplicaciones objeto, y puede tener cualquier cantidad de mensajes KVP o MSG conocidos como transacciones.

El formato de la trama se ilustra en la figura 2.28 y específica el tipo de trama (KVP o MSG) usado para cada transacción y el número de ellas [24].

Bits : 4	4	Variable	Variable	Variable
Conteo de Transacciones	Tipo de Trama	transacción 1	…	Transacción n

Figura 2.28 Trama AF

- **Trama KVP**

La trama KVP (ver figura 2.29) permite que una aplicación manipule atributos definidos por el perfil de aplicación. Los atributos tienen un designador (llave) y un valor asociado, los cuales pueden ser cambiados o solicitados usando la trama KVP.

Bits : 4	4	16	0/8	Variable
Identificador del tipo de comando	Tipo de dato del atributo	Identificador de Atributo	Error	Datos de Atributo

Figura 2.29 Trama KVP

El primer campo especifica el tipo de comando (event, set, get con ACK, set con ACK, event con ACK, get con response, set con response y event con reponse) ; el siguiente específica el tipo de datos en el campo datos del atributo los cuales pueden ser: sin o con signo de 8 y 16 bits, semi-precisión, tiempo absoluto, tiempo relativo, cadena de caracteres y 8 bits de cadena de caracteres ; el campo posterior el identifica el atributo del dispositivo dentro del cual el comando es operado. El campo Código de Error específica el estado de la transacción y el último campo contienen información específica para el atributo en el que se estableció referencias en el campo de identificador de atributo.

- **Trama MSG**

La trama MSG habilita un perfil de una aplicación en forma independiente del formato de ésta, permitiendo que las aplicaciones que no están dentro de la estructura KVP la flexibilidad para definir comandos de acuerdo a sus necesidades. La trama esta definida en la figura 2.30.

Bits : 8	Variable
Longitud de Transacción	Datos de Transacción

Figura 2.30 Trama MSG

El campo de longitud de transacción provee el número de octetos contenidos en el siguiente campo y el campo datos de transacción contienen mensajes de información específica definidos en un perfil aplicación en particular.

Cuando las aplicaciones objeto quieren enviar datos estos son anexados en la trama de la capa inferior hasta llegar al medio físico como lo muestra la figura 2.31

2.3.4.5 Perfil de dispositivos ZigBee

Este perfil opera como cualquier perfil ZigBee definiendo descripciones, clusters y atributos. A diferencia de los perfiles específicos de cierta aplicación, las descripciones del dispositivo y los clusters dentro de este perfil definen capacidades que se encuentran en todos los dispositivos ZigBee.

El perfil de dispositivos ZigBee soporta los siguientes dentro del protocolo ZigBee:

- Descubrimiento de dispositivos y servicios (Device and Service Discovery): el descubrimiento permite que por medio de mensajes de direccionamiento broadcast o unicast determinar la identidad de otro dispositivo en la red y los servicios ofrecidos por los dispositivos en la red. En este perfil se encuentran los descriptores obligatorios (simple, potencia y nodo) que ayudan a hallar un servicio determinado en un dispositivo de red. .
- Procesamiento de petición de vinculación en un dispositivo final. (End Device Bind Request Processing): permite realizar un “simple Binding “a través de la intervención del usuario.
- Procesamiento de comandos para la vinculación y desvinculación (Bind and Unbind Command Processing): permite crear o extraer entradas en la tabla de binding.
- Gestión de red (Network Management): permite recuperar información de gestión desde los dispositivos y colocar controles a la información de gestión.

El perfil de dispositivos ZigBee asume una topología cliente/servidor. Un dispositivo que realiza un servicio de descubrimiento, binding o peticiones de gestión de red lo realiza mediante un papel de cliente. Un dispositivo que proporciona estos servicios y responde las peticiones lo hace eso en un papel de servidor.

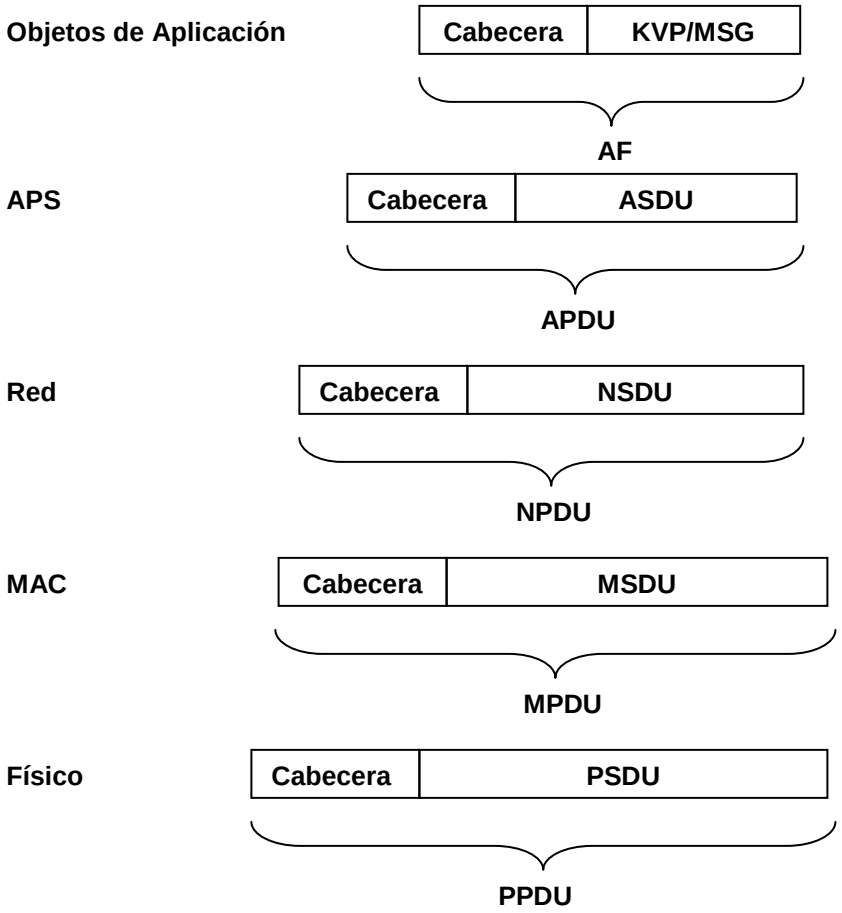

Figura 2.31 Construcción de un Paquete de Datos

2.3.4.6 Objetos de Dispositivos ZigBee

Los ZDO son una aplicación objeto con el endpoint 0 que es responsable de inicializar la APS, la capa de red (NWK), la especificación de los servicios de seguridad (SSP), además ajusta la información de configuración de las aplicaciones finales para determinar e implementar el descubrimiento, gestión de seguridad, gestión de red, gestión de binding y gestión del nodo.

El ZDO presenta interfaces públicas para la interacción con el framework de aplicación y los objetos aplicación para el descubrimiento de otros dispositivos y el servicio que proporciona, además es la parte de la capa de aplicación responsable de definir el rol del dispositivo dentro de la red como coordinador, router o dispositivo final Zigbee, y obtener una relación entre ellos. Las interfaces ZDO se interconectan mediante el endpoints 0, a través de APSDE-SAP usando el perfil de dispositivos ZigBee y a través de los mensajes de control de APSME-SAP con la APS y el NLME-SAP para la capa de NWK.

2.3.5 Seguridad

Zigbee aplica seguridad a la capa de red y APS por medio del SSP (Proveedores de servicio de seguridad) y a la subcapa MAC mediante la descrita en el estándar IEEE 802.15.4.

El SSP protege criptologicamente las interfaces entre los diferentes dispositivos, pero la separación de las interfaces entre las diferentes capas no es encriptada por parte del SSP, es decir, permite seguridad fin a fin entre los dispositivos en lugar de realizarlo entre las capas, este principio se basa en el modelo “open trust”, el cual permite el re-uso de las mismas llaves en medio de diferentes capas en el mismo dispositivo; además permite integridad, autenticación y *freshness* en las tramas que se trasmiten.

Cuando se transmite una trama para asegurar la integridad, a la derecha de la carga útil se anexa el MIC que consiste en 4, 8, o 16 octetos, que es creado mediante cálculos realizados entre la carga útil y la cabecera; y para asegurar la autenticación, a la izquierda se agrega una cabecera auxiliar que contiene un conteo de tramas y la secuencia de llaves, datos usados para encriptar la carga útil (*nonce*).

El estándar ZigBee usa la seguridad descrita en el estándar IEEE 802.15.4 para la subcapa MAC que emplea para la seguridad de sus tramas AES como su algoritmo criptográfico y describe una gran variedad de suites de seguridad. Estas suites pueden proteger la confidencialidad, la integridad y la autenticidad de las tramas MAC.

La Subcapa MAC es la encargada de su propio procesamiento de seguridad, pero las capas superiores determinan el nivel de seguridad a usar. Una capa superior establece los atributos (establecen las claves y determina los niveles de seguridad a usar.) del MAC PIB para la seguridad que se aplica en todas las tramas.

Cuando la capa MAC trasmite o recibe una trama con seguridad habilitada, considera el destino de la trama, recupera la llave asociada con ese destino (la fuente), y luego la usa para procesar la trama según la suite de seguridad designada.Cada llave es asociada con una solo suite de seguridad y el encabezado de la trama MAC tiene un bit que especifica si la seguridad de la trama esta habilitada o deshabilitada.

Cuando se recibe el paquete, si el MIC está presente, es verificado y si la carga útil esta encripta, es descifrada. Los dispositivos remitentes aumentarán el conteo de tramas con cada mensaje enviado y los dispositivos receptores seguirán el último conteo recibido de cada dispositivo remitente. Si un mensaje con un viejo conteo es detectado, entonces se señalará seguridad con error.

La capa de red también hace uso de AES, sin embargo, de manera diferente que en la subcapa MAC, todas las suites de seguridad están basados en el modo de operación CCM*, este CCM*[6] es una modificación del utilizado en la subcapa MAC. Este incluye todas las capacidades del CCM y adicionalmente ofrece capacidades de una sola encriptación e integridad. Estas capacidades extras simplifican la seguridad en la capa de red eliminando la necesidad de los modos CTR y el CBC-MAC. También, el uso de CCM* en todas las suites de seguridad permite una sola llave para ser usada por las diferentes suites. Desde que una llave no está estrictamente ligada a cada suite de seguridad, una aplicación tiene la flexibilidad de especificar la suite de seguridad actual aplicada a cada trama de la capa de red, y permite saber si la seguridad está habilitada o deshabilitada.

Cuando la capa de red transmite una trama usando una suite de seguridad en particular utiliza el SSP para procesarla. El SSP considera el destino de la trama, recupera la llave asociada con ese destino (la fuente), y luego aplica la suite de seguridad para la trama. El SSP provee a la capa de red una primitiva para aplicar seguridad para tramas salientes y una primitiva para verificar y quitar seguridad de las entrantes. La capa de red es responsable del proceso de seguridad, pero las capas superiores controlan el procesamiento estableciendo las llaves y determinando cuál suite de seguridad CCM * se usa para cada trama.

[6] Así esta definido dentro de la especificación ZigBee

3. CRITERIOS EN UN ESCENARIO HOSPITALARIO

El surgimiento de nuevas tecnologías de información y comunicaciones emergentes, como se menciona en capítulos anteriores, abren la posibilidad de nuevas aplicaciones en entornos hospitalarios que permitirán transmitir las señales de origen biomédicas[7] constantemente o alertar en caso de que estas presenten alteraciones a dispositivos de visualización (pantalla, PDA, PC…) o centros de procesado, sin que se vea limitada la movilidad del paciente [27].

Las ventajas que proporcionan estas tecnologías emergentes como las WSN no solo está en la eliminación de los cables de los dispositivos actuales, sino que abre un abanico de nuevos escenarios, como permitir la monitorización remota y constante de los pacientes cambiando el tradicional uso de dispositivos de alto volumen, a los cuales estaban conectados a través de cables. Esto limita en gran medida la movilidad del paciente y por lo tanto su bienestar durante la estancia hospitalaria.

Para lograr una monitorización constante y remota por parte del personal médico las redes WSN son ideales por su bajo consumo de potencia, por sus diminutos dispositivos y la cantidad que se pueden emplear para formar una red.

En este capitulo se analiza como en un entorno hospitalario se puede implementar una red se sensores con la tecnología ZigBee para la transmisión de señales eléctricas producidas por el cuerpo humano y llevarlas a una estación base para que alerte de forma automática y directa a la persona idónea para atender la emergencia.

3.1 ESCENARIO HOSPITALARIO

Los entornos hospitalarios son escenarios grandes, por lo general con varios pisos los cuales están divididos en áreas como neurología, traumatología, problemas cardiovasculares, urgencias, unidad de cuidados intensivos (UCI), hospitalización, pediatría, etc. Cada una de estas áreas posee un puesto de enfermería para la atención de los pacientes y habitaciones numeradas de acuerdo al piso. Cada habitación o área puede tener uno o varios pacientes los cuales se identifican de acuerdo al número de la habitación.

Los puestos de enfermería son los encargados de la atención y cuidado de los pacientes, realizan una monitorización a determinados momentos (cambios de turnos, suministro de medicamentos etc.) o ante cualquier llamado realizado por ellos (mediante timbres, alarmas etc.), pero no detectan de inmediato alteraciones en su estado funcional de manera imprevista, las cuales pueden comprometer su

[7] Señales eléctricas producidas por determinados órganos de cuerpo humano.

vida. Entre las variaciones que se presentan están los cambios en los signos vitales, señales que tienen que ser supervisadas de forma constante porque revelan cambios en los órganos primordiales (corazón, pulmones y cerebro).

Estas variaciones se manifiestan través de actividades eléctricas, el corazón produce una señal llamada electrocardiograma o ECG, la actividad de los músculos produce un electromiograma o EMG, mientras que el cerebro genera una señal conocida como electroencefalograma o EEG. Estas señales tienen la característica que presentan amplitudes muy pequeñas y bajas frecuencias como lo muestra la tabla 3.1, características que con el estándar ZigBee se pueden soportar.

Tabla 3.1 Amplitud y Rango de frecuencias en señales bioeléctricas típicas [27]

Señal	Amplitud (mV)	Rango Frecuencial (Hz)
ECG	0.02 – 5	0.05 – 100
EEG	0.0002 – 0.3	DC – 150
EMG	0.1 – 5	DC – 10000

La instalación de la WSN basada en Zigbee para el entorno hospitalario debe ser automática o semiautomática, con el propósito que se puedan colocar fácilmente varios sensores a los pacientes sin que estos ocasionen problemas en la red y un costo bajo para permitir que se agreguen dependiendo del caso.

Como el estándar ZigBee es una WSN es necesario identificar cada componente para la formación de su red; de acuerdo al capítulo 1:

- Fenómeno: son las señales eléctricas producidas por le cuerpo (ECG, EMG, EEG).
- Nodos sensores: son los que van conectados a cada paciente y los encargados de tomar constantemente las señales eléctricas y enviar alarmas en caso que estas presenten alteraciones.
- Observador: es el personal médico que está atento a los cambios presentados en el paciente.
- Nodo recolector: será el dispositivo conectado a la estación base y actuará como coordinador.
- Gateway: cumplirá sus funciones respectivamente dentro de la red de acuerdo a su formación.

3.2 COMPATIBILIDAD CON APLICACIONES BIOMÉDICAS

Los dispositivos Zigbee de acuerdo a la capa física no especifican una potencia máxima de salida, esto depende de los fabricantes, pero está no es superior a -3dBm (0.5 mW). Según los estándares internacionales [22] un dispositivo de estas características trabajando a una frecuencia máxima de 2,4 GHz será totalmente seguro implantado en el cuerpo humano.

Por otro lado, también se debe tener en cuenta la atenuación introducida por el cuerpo humano dada la baja potencia de transmisión. Según [22] una separación mínima de 10 mm entre la antena y el cuerpo es suficiente para asegurar un funcionamiento correcto o con pérdidas inapreciables.

3.3 DISPOSITIVOS ZIGBEE

Para la implementación de una red ZigBee existen básicamente dos dispositivos comerciales [22]:

- Módulos IEEE 802.15.4/ ZigBee, consisten en tarjetas que tienen integrado para la transmisión y recepción un chip de transceptor que tiene implementado el estándar IEEE 802.15.4. Como inconveniente de este tipo de soluciones es que no se encuentra el resto de capas ZigBee, por lo tanto deber ser implementadas por el diseñador; y como ventaja que se dispone de total libertad en el diseño del dispositivo, ejemplo de ellos son los dispositivos de la empresa Crossbow.

- Módulos stack ZigBee, que consisten en una única tarjeta que incluye todas las capas de la especificación ZigBee y el estándar IEEE 802.15.4. La ventaja principal de este tipo de soluciones es que se reducen considerablemente el tiempo de desarrollo, ejemplo de ellos son los dispositivos de Microchip, Ember, Luxoft Labs, Helicomm entre otros.

El enlace de cualquiera de estos dispositivos se realiza mediante una conexión serie UART, RS-232 o USB.

La elección del dispositivo depende del diseñador, si necesita una aplicación que esté orientada a los perfiles certificados por la “Alliance ZigBee” debe optar por un módulo stack ZigBee, por el contrario, si la aplicación no es ninguno de los perfiles puede elegir módulo IEEE 802.15.4/ Zigbee.

3.4 CAPA FÍSICA

La capa física que proporciona el estándar IEEE 802.15 4 para la tecnología ZigBee define tres bandas de frecuencias como lo menciona el capítulo 2, y cada una de ellas tiene distintas características, tanto de modulación como de canales por los cuales transmitir, como el ancho de banda de una señal ECG está entre (100-125) Hz cualquiera de los tres canales es apto para enviar esta señal.

Para Colombia la banda a utilizar es la de 2.4 Ghz que posee 16 canales, es necesario destacar que esta frecuencia interactúa con la tecnología inalámbrica 802.11, por lo tanto es necesario trabajar en el canal 26 porque es el más alejado como lo muestra la figura 3.1 y con ello él más inmune a interferencias, además el estándar define una separación de 5 Mhz y establece que para la frecuencia de

2.4 Ghz el receptor tiene una selectividad del canal y bloqueo de canal adyacente por lo tanto los problemas de traslape y co-canal van a ser mínimos y además es la banda que trasmite a una mayor velocidad.

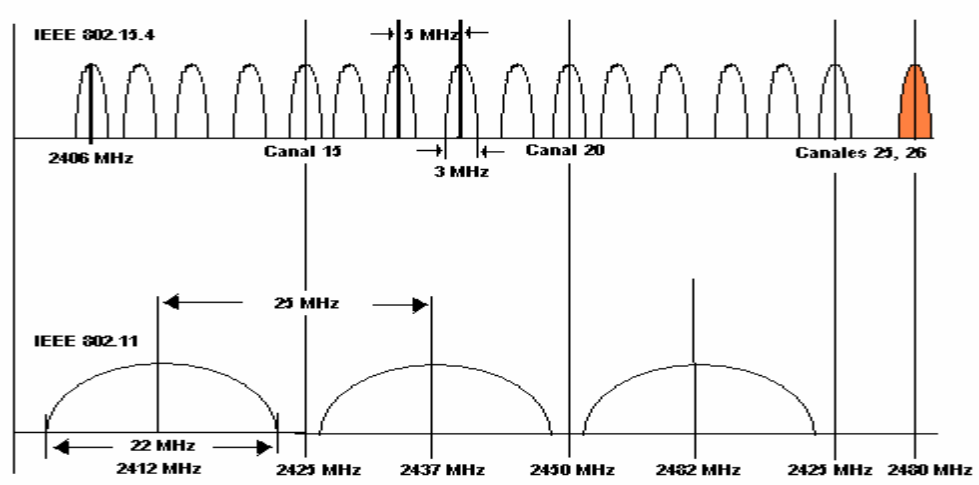

Figura 3.1 Espectro de frecuencia 802.15.4 vs 802.11

Como esta capa viene incorporada en el transceptor, todas las características de ésta se acceden por medio del sistema operativo que maneja el dispositivo, un ejemplo de ellos es el Chip transceptor CC2420 de Chipcon[30] el cual tiene incorporado todas las características del estándar IEEE 802.15.4 y se acceden a ellas mediante componentes que proporciona TinyOS [31], por lo tanto, para interactuar con sus características se deben realizar cambios a los parámetros (ver tabla 3.2) que por defecto trae la librería cc2420const.h [33].

Tabla 3.2. Valores por defecto del CC2420

Parámetro	Valor
CC2420_DEF_RFPOWER	0x01(-25dBm)-0x1F(0dBm)
CC2420_DEF_CHANNEL	26
CC2420_DEF_PRESET	2405
CC2420_ACK_DELAY	75 (microsegundos)

- CC2420_DEF_RFPOWER: permite variar la potencia de emisión de vía radio en niveles distintos que oscilan entre 0dBm y -25dBm.
  CC2420_DEF_CHANNEL: permite definir el canal por el que se transmite. Su valor va entre el canal 11 y el canal 26.
- CC2420_ACK_DELAY: Tiempo en μs que puede tardar en confirmarse un paquete antes de declararlo inválido.

3.5 SUBCAPA MAC

Al igual que la capa física, la subcapa MAC está incorporada en el chip, por lo tanto sus características también se modifican de acuerdo a los parámetros

establecidos por los fabricantes en el sistema operativo que lo maneja. En el CC2420 se modifica por medio de registros los cuales únicamente indican la posición en memoria y la posición del bit que modifica la configuración.

En CC 2420 Los registros mas significativos son el MDMCTRL1 y MDMCTRL0 los cuales dan unas variables de configuración que permiten modificar los campos que se envían dentro de los paquetes a nivel de enlace, tales como el tamaño de preámbulo, tiempos entre paquetes, así como aspectos de compatibilidad y modulación. Un bit del registro MDMCTRL0 permite determinar que nodo actúa como coordinador PAN, es decir si se habilita las tramas con beacon.

La subcapa MAC establece dos posibilidades de acceso al medio:

- Un mecanismo CSMA/CA ranurado (beacons).
- Un mecanismo CSMA/CA no ranurado.

Como en un entorno hospitalario no se pretende enviar gran cantidad de paquetes de datos, sino asegurar la llegada de estos paquetes y que lo hagan con el menor gasto de energía posible, por lo tanto, es necesario implementar el método de supertrama que habilita el uso de beacons con el mecanismo ACK para lograr la protección de transmisión efectiva salto por salto y conseguir una pérdida reducida de paquetes y un ahorro de energía considerable.

3.6 CAPA DE RED

Este nivel ya pertenece a la especificación ZigBee y la incorporación en el dispositivo dependerá si es módulo ZigBee ó IEEE 802.15.4/ZigBee.

Para los dispositivos que son módulos ZigBee, ya vienen definidos protocolos de enrutamiento, su selección depende de la aplicación; y para los que son módulos IEEE 802.15.4/ ZIgBee el protocolo se puede crear por parte de quien genera la aplicación al igual que la topología.

La elección de la topología dependerá de la aplicación que representa la solución, cuando el área de cobertura es muy amplia, se piensa en una topología en malla, mientras que si lo que se requiere es un control constante de los dispositivos (por ejemplo, control de periféricos), se suele optar por un diseño en estrella.

Independiente del dispositivo, como el área de cobertura es muy amplia, la topología a implementar es una topología en malla principalmente porque tiene un cubrimiento muy grande y es autónoma, es decir auto-configurable y realiza auto – reparación de rutas permitiendo que en caso de caída del enlace se busque otro camino para que el paquete llegue a su destino.

Para implementar una red en malla de acuerdo al capítulo 2 se deben tener dispositivos RFD y FFD (con sus dos funciones: Router y Coordinador). Los sensores que llevará cada paciente serán dispositivos RFD los cuales se comunicaran con los FFD y estos a su vez se comunicaran con el coordinador ZigBee.

Los enrutadores FFD serán los encargados de recibir las señales de los RFD conectados a los pacientes y enrutarlas hacia el coordinador ZigBee ya sea directamente o por medio de otro enrutador FFD.

Debido a que el escenario hospitalario es grande por cada pieza se va tener un enrutador FFD y los RFD dependerán del número de pacientes (formando una topología en estrella), el número de enrutadores FFD en el piso son de acuerdo a la distancia y las características indoor del hospital.

El coordinador ZigBee será el responsable de inicializar la red y de elegir los parámetros de funcionamiento, estará conectado a un a estación base que será la entrada al sistema que avisa a quien corresponda de la emergencia que se ha presentado.

El protocolo de enrutamiento que se emplee debe optimizar la trayectoria más corta y más confiable a través de la red siempre teniendo en cuenta el ahorro de energía. Existen varios protocolos con estas características de acuerdo a la sección 1.3.3.1, el que más se adapta a lo expuesto anteriormente son los protocolos de enrutamiento jerárquico, la elección de cualquiera de ellos dependerá si son módulos ZigBee los que el fabricante facilite y si es chipset de quien realice la programación.

3.7 CAPA DE APLICACIÓN

Como se mencionó en el capítulo 2, este nivel da las pautas para realizar una aplicación por parte del usuario final, estas pautas son perfiles que se aprueban y se certifican por parte de la “Alliance ZigBee” previo a un estudio.

En la actualidad existen perfiles para el control de los hogares, monitoreo de plantas industriales entre otros, y no existe un perfil orientado al cuidado clínico, por tal razón no existe un modelo para realizar aplicaciones en este entorno.

De acuerdo a las características del ambiente estudiado y a los perfiles que actualmente están certificados por la “Alliance ZigBee” se puede pensar en un perfil llamado “Monitoreo de Señales Biomédicas en Pacientes (MSBP)” para atender las diferentes alteraciones que un paciente presenta en su estancia hospitalaria. Cabe recordar que al especificar un perfil también se definen los descriptores clusters y atributos.

Como la aplicación es la implementación de una descripción del perfil, estas serán las que se implementen en el objeto de aplicación y estos a su vez en un endpoint del dispositivo ZigBee. La comunicación es realizada entre los endpoint por medio de cluster que contienen los atributos que comparten la información entre los objetos de aplicación, es decir, cuando dos dispositivos se conectan, el cluster de salida es conectado con el cluster de entrada del otro dispositivo.

Los cluster de salida y entrada para un descriptor de Monitoreo de Señales biomédicas puede ser:

- Entrada: inputNivel ECG, inputNivel EEG y inputnivel EMG que tendrán atributos encargados de detectar constantemente las señales producidas por el cuerpo.
- Salida: outputUP ECG, outputUP EEG, outputUP EMG que tendrán atributos encargados de transmitir cuando el límite de funcionamiento normal se ha sobrepasado.

4. DESCRIPCIÓN DE LA APLICACIÓN Y PRUEBAS REALIZADAS

Después de analizar los criterios para realizar una red ZigBee dentro de un entorno hospitalario para el transporte de señales biomédicas, que sirva de entrada a un sistema automático y a las limitaciones especialmente económicas, se optó en realizar la aplicación final mediante la simulación de una anormalidad del corazón (estas se pueden representar por medio de un ECG). La anormalidad serán las arritmias presentadas en el ritmo cardíaco, para más información al respecto ver el anexo A.

Por lo tanto, la aplicación final consistirá en simular con software las arritmias más sencillas (bradicardia y taquicardia) que son alteraciones del ritmo cardíaco y visualizarlo en un ECG (esté también será simulado) y realizar una comunicación inalámbrica para el transporte de ello mediante tarjetas que manejan tecnología IEEE 802.15.4 a un sistema de conmutación automática implementado con software libre que genera una comunicación para avisar a quien corresponda (ver figura 4.1).

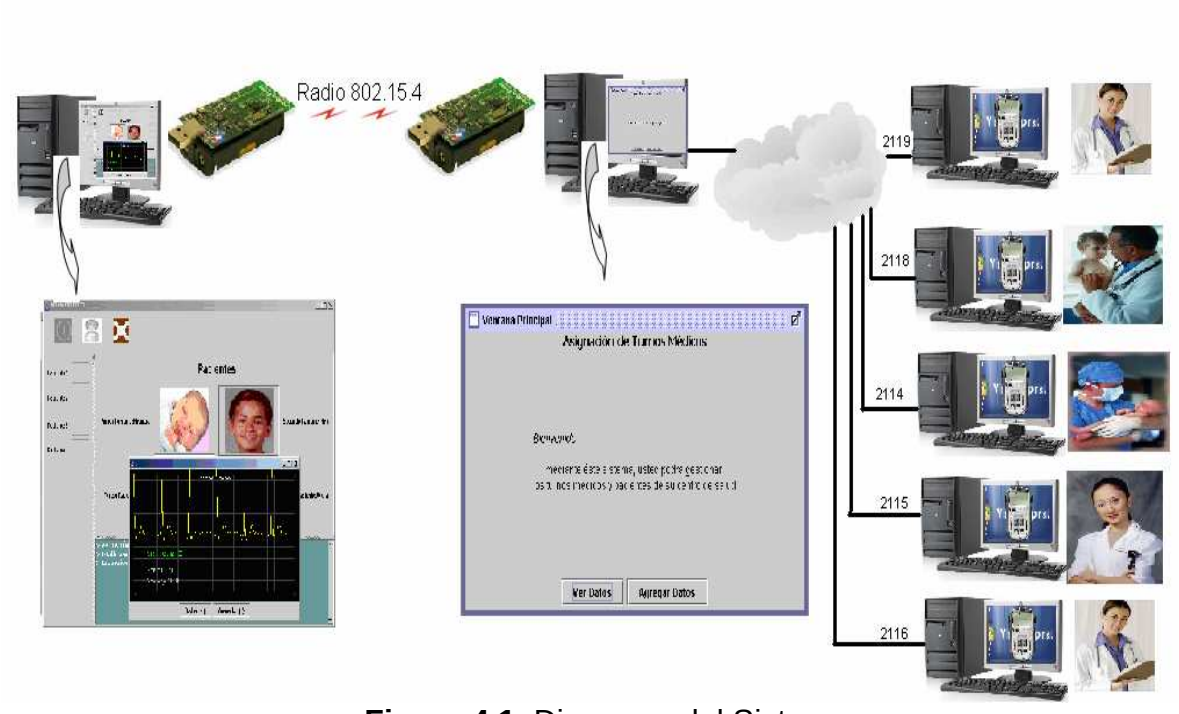

Figura 4.1 Diagrama del Sistema

4.1 COMPONENTES

En la implementación del sistema de simulación del ritmo cardíaco como entrada para un sistema automático, es necesario la utilización de componentes tanto

hardware como software; por ello, se realiza una descripción de dichos componentes.

4.1.1 Componentes Hardware

Los componentes hardware para el sistema de simulación del ritmo cardíaco de acuerdo a los dispositivos de la tabla 1.1 esta conformado por dos dispositivos IEEE 802.15.4 /ZigBee denominados TelosB Mote pertenecientes a la marca comercial Crossbow [28], una de las marcas más extendidas y conocidas en cuanto al desarrollo de kits de hardware para la investigación en redes de sensores inalámbricas. Se optó por estos dispositivos a pesar que no tienen todo el stack ZigBee porque en el momento de la compra eran los más económicos, además su conexión con el PC se realiza directamente mediante USB con lo cual se evita otro dispositivo para programarlo y porque el sistema operativo que manejan es TinyOS uno de los más usados en esta tecnología.

4.1.2 Componentes Software

Entre los componentes software para el sistema de simulación del ritmo cardíaco se encuentra TinyOS versión 1.17, que es el sistema operativo utilizado por los dispositivos inalámbricos telosB, el cual, está especialmente diseñado para programar las características específicas de los nodos de sensores y sus aplicaciones de red. TinyOS tiene la ventaja de ser “Open Source” y de tener una arquitectura basada en componentes que permite una rápida implementación e innovación, mientras que se minimiza el tamaño del código, lo cual es importante debido a la gran restricción de cantidad de memoria que existe en los sistemas embebidos. TinyOS está escrito en nesC, un nuevo lenguaje de programación de aplicaciones estructurales basado en componentes. Para más información sobre instalación y teoría de tinyOS y nesC consultar el anexo B.

TinyOS requiere para su correcto funcionamiento del uso de diversos comandos y funcionalidades de Linux, por lo tanto, si se desea trabajar en un entorno Windows es necesaria la instalación de la plataforma Cygwin [32], encargada de emular un entorno Linux en Windows. Los dispositivos traen consigo un CD de instalación de cygwin y además el sistema operativo tinyOS.

La interfaz del nodo transmisor y del receptor se realizó en el lenguaje de programación Java, utilizando la edición estándar 1.4.2 del kit de desarrollo de software, y el entorno de desarrollo integrado NetBeans IDE 3.6.

Para el sistema central automático de acuerdo a la tabla 4.1 se observa que asterisk [29] es el más completo de todos, por tal razón se optó por esté para hacer el enrutamiento del mensaje.

Tabla 4.1 Comparación de servidores IP con software libre

	Asterisk	OpenPBX	Bayonne	OnDO PBX
VENTAJAS	• Muy completo • Muy confiable • Es software libre • Tiene muchas opciones de personalizar • Diseño completo para tener funcionalidad de PBX • Muy bien documentado • Muchos servicios y posibilidad de agregar nuevos	• Es software libre • Interfaz amigable • Fácil configuración	• Muy confiable • Es software libre	• Completa • Soporte • Flexibilidad y opciones de escalabilidad.
DESVENTAJAS	• No existe un soporte bibliográfico adecuado para el uso de ésta herramienta.	• Solo implementaciones pequeñas • Muy limitado • Poco soporte	• Configuración Compleja • No tiene muchas opciones de personalizar • No es diseñado para tener funcionalidad completa de PBX • No tiene mucha documentación ni soporte	• No es libre

4.2 MÓDULOS DEL SISTEMA

El sistema está conformado por dos módulos principales, un módulo transmisor y un módulo receptor (ver figura 4.2).

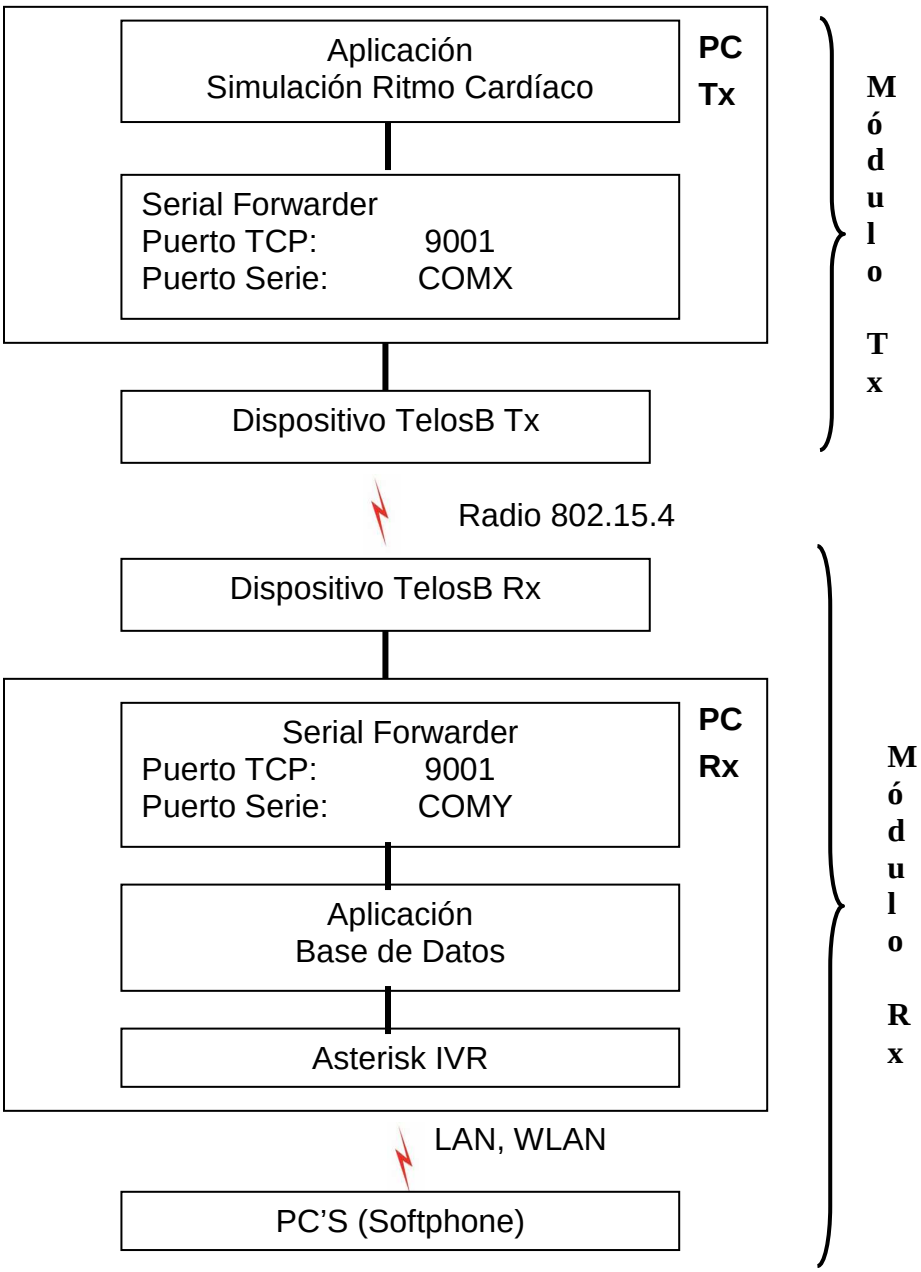

Figura 4.2 Módulos de la aplicación

4.2.1 Módulo Transmisor

El módulo transmisor es el encargado de enviar la información adquirida cuando ocurre un evento en un paciente, el cual se detecta a través de la aplicación disponible en el transmisor que permite comunicar dicho evento con el dispositivo telosB transmisor.

El módulo transmisor está implementado en la plataforma de desarrollo Cygwin, bajo el sistema operativo tinyOS; dicho módulo se encuentra en la carpeta opt con el nombre de tinyos-1.x, y dentro de ella están las aplicaciones, librerías y herramientas necesarias para su correcto funcionamiento.

4.2.1.1 Funcionamiento del Módulo Transmisor

Para el funcionamiento del módulo transmisor se requiere ejecutar el serialForwarder, el cual, es un programa proporcionado por tinyOS para realizar la comunicación de la aplicación del transmisor (localizada por defecto en el puerto TCP 9001) con el puerto serial. Cygwin internamente asigna un puerto serie apenas se conecta el dispositivo telosB transmisor, a pesar que éste se encuentra conectado en el puerto usb del pc; en consecuencia, toda la información obtenida en el puerto serial es transferida al puerto usb y viceversa. Por lo tanto, todos los paquetes que se envían al puerto serial donde está escuchando el SerialForwarder son retransmitidos con todas las conexiones activas en ese momento, al puerto TCP con el cual está ligado la aplicación.

SerialForwarder está localizado en la carpeta *java*, que se encuentra en la ruta /opt/tinyos-1.x/tools/java (ver figura 4.3); en dicha carpeta están todas las aplicaciones de java proporcionadas por tinyOS.

Figura 4.3 Ruta de la carpeta java

Para observar en que puerto serial queda asignado el dispositivo telosB transmisor se utiliza el comando `motelist` proporcionado por tinyOS, como se observa en la figura 4.4.

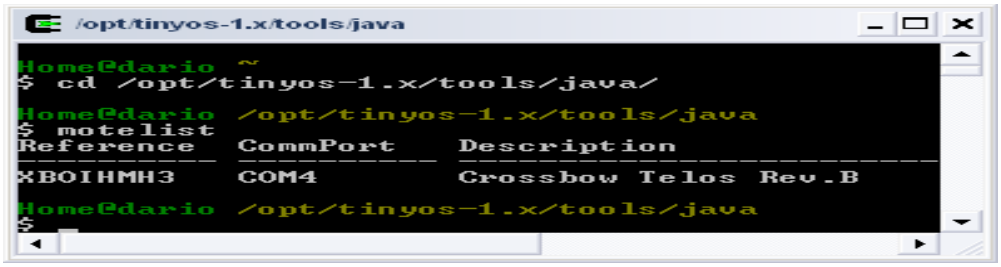

Figura 4.4 Comando motelist

Para invocar al SerialForwarder se utiliza la máquina virtual de java y el puerto serie en que quedó asignado el dispositivo telosB y se digita el siguiente comando:

```
#java net.tinyos.sf.SerialForwarder –comm serial@COM4:telos
```

Si el proceso se llevo a cabo correctamente debe aparecer una ventana como se muestra en la figura 4.5.

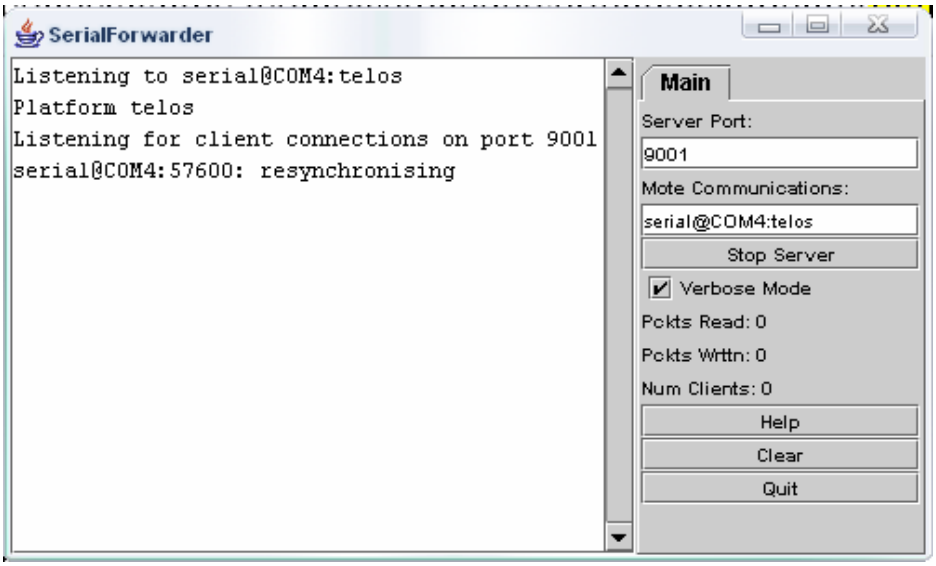

Figura 4.5 SerialForwarder

La parte izquierda de la figura 4.5 indica los paquetes leídos y enviados por el puerto TCP y el puerto serial, y si la operación se realizó con éxito debe mostrar el sincronismo establecido, lo que significa que la comunicación entre la aplicación y el dispositivo telosB se llevó a cabo favorablemente. Cuando no hay sincronismo puede ser que el puerto TCP o serial no estén bien asignados.

4.2.1.2 Instalación de la Aplicación

Una vez que se ha invocado SerialForwarder se inicia la instalación de la aplicación del ritmo cardíaco realizada en el lenguaje de programación java en el editor NetBeans .Para realizar la instalación, se copia la carpeta ritmo del directorio /Aplicación del Transmisor/ en la ruta ~/tinyos-1.x/tools/java/net/tinyos y a partir de éste se convierte en una aplicación más de las utilidades java proporcionadas por TinyOS(ver anexo B), por tanto la manera de ejecutarla es situarse en el directorio ~/tinyos-1.x/tools/java y se digita el siguiente comando

```
#java net.tinyos.ritmo.MainClass.
```

Para el funcionamiento de la aplicación del dispositivo telosB transmisor en el lenguaje de programación nesC, se coloca la carpeta SensorTx en ~/tinyos-1.x/apps/ y se digita el siguiente comando:

```
#make install.9 telosB
```

Para ver más detalle de cómo compilar una aplicación en tinyOS se puede referir al Anexo B.

4.2.1.3 Aplicación del Módulo Transmisor

La aplicación consiste en simular un sistema de monitorización de las señales eléctricas del corazón a través del electrocardiograma, el cual está enfocado en pacientes que sufren algún trastorno cardíaco, en especial arritmias (taquicardia o bradicardia). Dicho sistema analiza la señal de electrocardiograma (ECG) y genera alarmas en caso de que se produzca algún peligro. Esta alarma activa el dispositivo telosB transmisor, obligándolo a comunicarse con el telosB receptor que está conectado a un sistema de conmutación automática realizado con Asterisk; en esté sistema de conmutación es donde se genera una comunicación para enrutar la información que se ha introducido en el modelo de base de datos que maneja los turnos, y de esta manera poder localizar y dar aviso al médico correspondiente. Dicha comunicación consiste en dar aviso mediante mensajes audibles pregrabados sobre qué paciente necesita atención en ese momento. La ubicación de los médicos será simulada por medio de computadores con sistema operativo Windows 2000 la cual se realiza vía alambrada o inalámbrica.

Los componentes gráficos de la aplicación del ritmo cardíaco (ver figura 4.6), poseen información emergente, por lo tanto, si el usuario no conoce el significado de algún elemento, basta con dejar el ratón encima del elemento y aparecerá la ayuda asociada. La interfaz posee una barra de herramientas, en la cual, el primer icono se utiliza para conectarse al *SerialForwarder*, el segundo muestra un cuadro de autores y el último icono permite salirse o terminar la aplicación.

Figura 4.6 Aplicación del ritmo cardíaco

En la parte superior derecha de la figura 4.6 están representados cuatro tipos de personas, que se van a simular como pacientes, y en la que cada una dependiendo de su edad y de su condición física va tener un rango de ritmo cardíaco diferente (para más detalle consultar el anexo A), estas personas son: neonatos, niños, adultos y atletas. Como se observa en la parte inferior de la figura 4.7, se ha establecido la conexión con el SerialForwarder, cuando esto ocurre se iluminan los iconos que representan los pacientes dando inicio a la simulación.

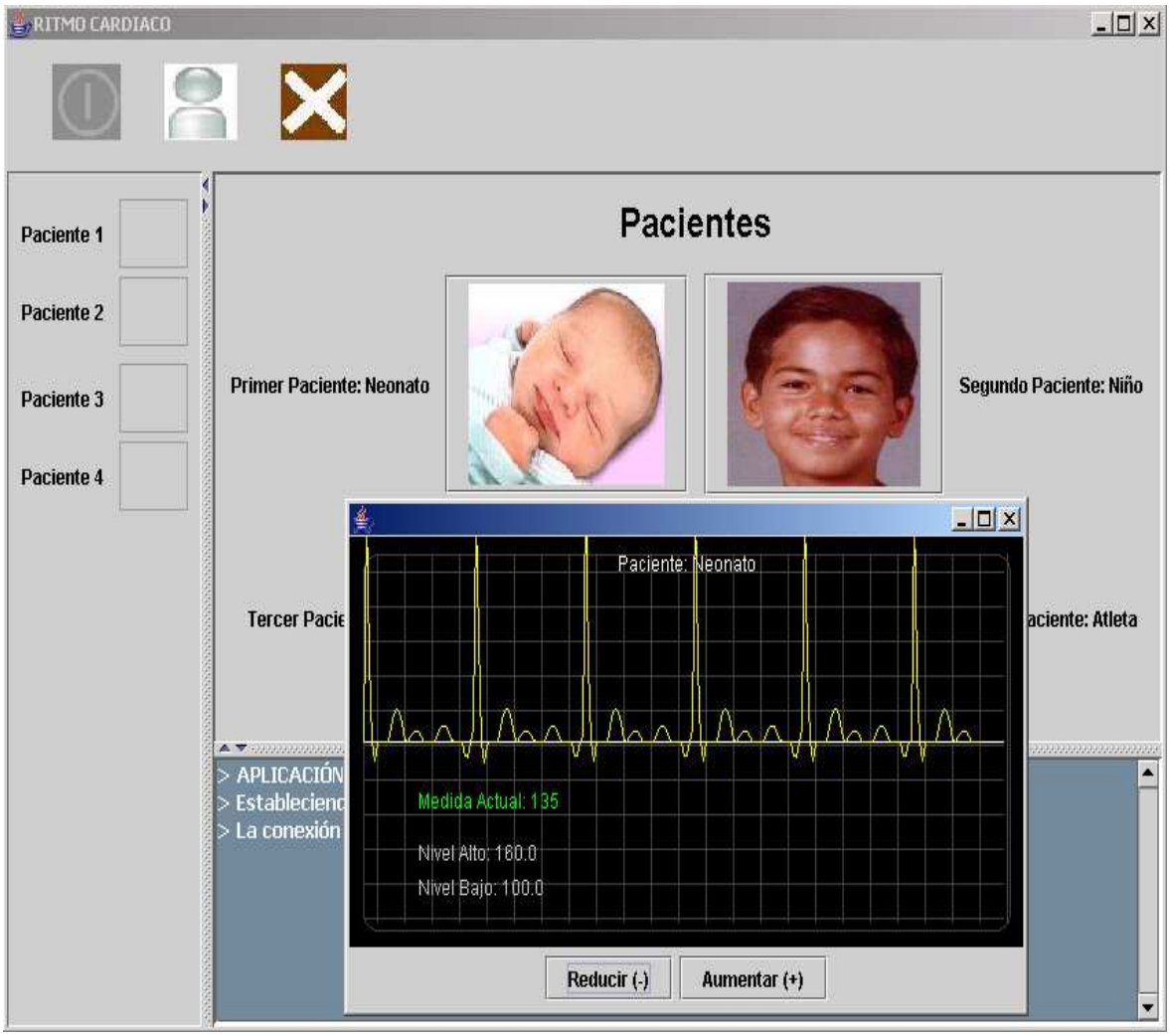

Figura 4.7 Inicio de la aplicación

Para iniciar la simulación de las señales eléctricas del corazón a través del ECG en un paciente determinado se debe dar click sobre dicho paciente**;** dependiendo del paciente se obtiene un ritmo cardíaco diferente, es decir, tendrán un rango distinto en el cual los latidos del corazón es normal y cada vez que se pase de ese rango presentará un trastorno cardíaco; dicho trastorno cardíaco se presenta cuando el ritmo se encuentra en un nivel alto (taquicardia) o un nivel bajo (bradicardia), éstos niveles se controlan por medio de los botones que están debajo de la señal ECG , como se muestra en la figura 4.6. Para ver con más detalle sobre el ritmo cardíaco consultar el anexo A.

La aplicación del ritmo cardíaco (a través de una clase llamada EnviarAction) le informa al telosB transmisor por medio del SerialForwarder que ha sucedido algún problema con un paciente, entonces esté dispositivo transmite la información al telosB receptor anunciando que a ocurrido un evento, el telosB transmisor solo transmite el paquete una sola vez y si transcurridos veinte segundos la simulación

continua en el mismo estado, ya sea taquicardia o bradicardia el sistema vuelve a transmitir de nuevo el evento permitiendo que si el médico no ha escuchado el mensaje pregrabado lo escucha nuevamente.

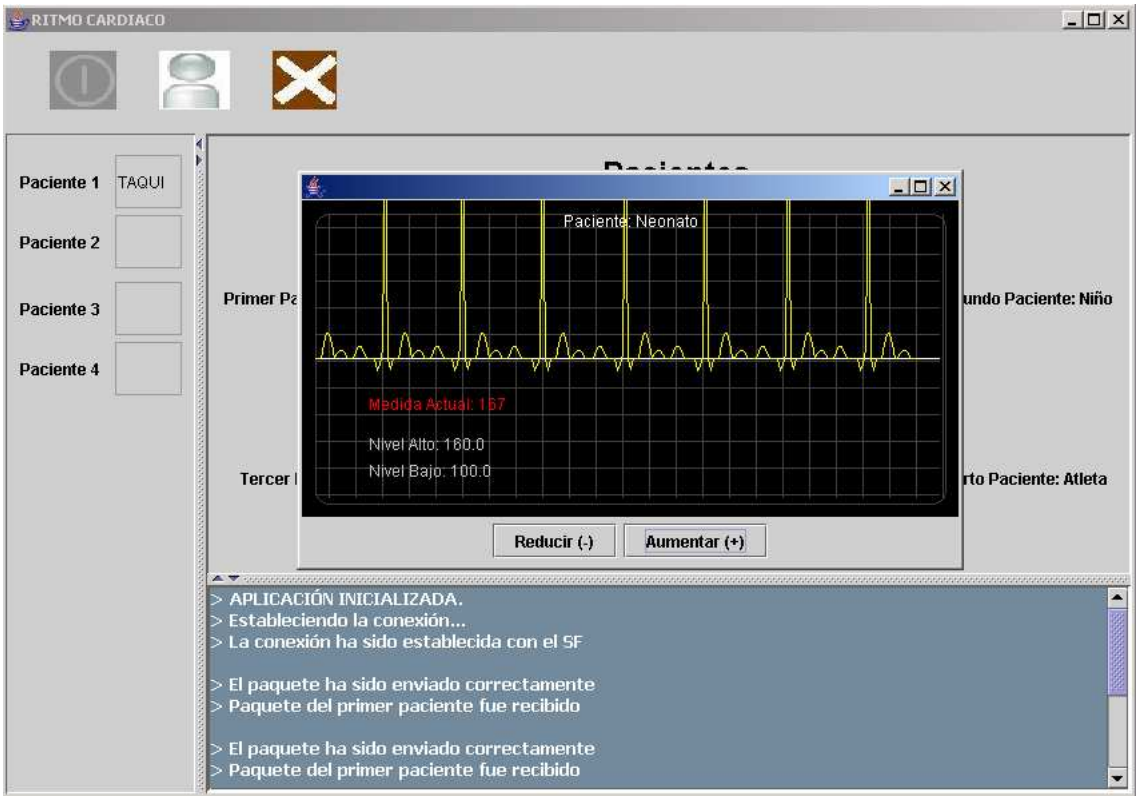

Figura 4.8 Un evento de un paciente

Como se observa en la figura 4.8 cuando surge un problema con uno de los pacientes se despliega en la parte inferior un mensaje que indica que se ha enviado el paquete con la información del paciente, y al mismo tiempo en la parte derecha de la figura 4.8 aparece el problema que ha tenido el paciente; cuando el telosB transmisor recibe el ACK despliega en la parte inferior un mensaje que informa que se ha recibido el paquete con éxito.

4.2.1.4 Lógica de Programación de nesC

Como se ha dicho anteriormente, los dispositivos telosB se programan en el lenguaje de programación nesC que es un lenguaje orientado a componentes. Un usuario puede crear un componente con la ayuda de los ya creados por defecto, para más detalle se puede consultar el anexo B. Se creó un componente llamado SensorTx en el caso del transmisor y SensorRx en el caso del receptor, ambos componentes tienen la misma funcionalidad de enviar y recibir una trama pero se diferencian en la identificación del destino. SensorTx y SensorRx utilizan otro llamado GenericComm que proporciona mecanismos para poder enviar y recibir

paquetes vía radio y vía puerto serie. Por lo tanto, el GenericComm actúa como switch entre la radio y el puerto serie, de tal manera que permite capturar los mensajes y llevarlos al puerto serie. NesC utiliza el modelo de mensajes activos (AM Active Message)[8] estándar de TinyOs por lo que se basa en el envío de paquetes TOSMsg, estos paquetes poseen la siguiente estructura;

```
uint16_t addr;
uint8_t type;
uint8_t group;
uint8_t length;
int8_t data[TOSH_DATA_LENGTH];
uint16_t crc;
```

El significado de cada uno de los campos es el siguiente:

- addr , es la dirección a la que va destinado el paquete, existen ciertas direcciones especiales:
  - TOS_BCAST_ADDR – Es la dirección de broadcast
  - TOS_LOCAL_ADDRESS – Es la dirección local (localhost)
  - TOS_UART_ADDR – Es la dirección del puerto serie

- type, es el tipo de paquete que se está enviando, determina que instancia de la interfaz se va a hacer cargo de procesar dicho paquete.

- group, es el grupo al que pertenece el sensor que está enviando el paquete, de manera que solo lo reciban aquellos sensores que pertenezcan al mismo grupo, de esta manera pueden coexistir dos redes diferentes de sensores sobre el mismo medio físico aéreo y sobre el mismo canal de radio.

- lenght, es la longitud total del paquete.

- CRC, es la corrección de errores.

- data, este es el campo más importante y el que posibilita manipular los paquetes. En este campo se especifican los datos que se van a enviar, estos pueden ser una estructura que conforme un nuevo tipo de paquete.

Surgió la necesidad de crear un fichero cabecera llamado paquetes.h en la cual se define la estructura de la aplicación; y esté archivo se encuentra dentro del campo data del paquete TOSMsg, y sus datos son los que se envían desde la aplicación del ritmo cardíaco al dispositivo telosB, también define variables que se utiliza en el programa. Este paquete posee la siguiente estructura:

[8] Cada paquete de la red especifica un ID gestor que invoca al nodo receptor

```
uint8_t type;
uint8_t pac;
uint16_t data;
uint8_t band;
uint8_t count;
uint8_t sala;
```

El significado de cada uno de los campos es el siguiente:

• type, es un identificador que indica si el paquete va a la aplicación del ritmo cardíaco(al SerialForwarder) o al otro dispositivo telosB.
• pac, es el identificador del paciente.
• data, es el tipo de problema que tiene el paciente, puede ser bradicardia o taquicardia
• band y count, son opcionales para posteriores aplicaciones.

TinyOS tiene una aplicación llamada mig que genera una clase java con el paquete que se haya definido en este caso paquetes.h, el cual permite interactuar entre la aplicación del ritmo cardíaco y el dispositivo telosB con métodos de capturar y enviar datos con los campos de la estructura.

Cuando se envía de la aplicación del ritmo cardíaco un evento, como por ejemplo que un paciente tiene una arritmia, el telosB transmisor interactúa con la clase mig para recoger los datos del paciente y ubicarlos en la estructura, asignando al campo type el valor de “1” indicando que toda la trama tiene que ser enrutarla al telosB receptor y enviarla inalámbricamente, cuando el valor es “2” indica que el telosB receptor le devolvió una confirmación de ACK haciendo que el dispositivo telosB transmisor recoja la trama y se la envía a la interfaz de la aplicación del ritmo (a través de la clase llamada RecibirAction) confirmando que el paquete llegó con éxito al receptor .

4.2.2 Módulo Receptor

En el módulo receptor se encuentran cuatro componentes que son: dispositivo telosB receptor, la base de datos de los pacientes y médicos, asterisk y el usuario final que está representado en el *sofphone*. El módulo receptor está conformado por un sistema de conmutación automática (Asterisk) implementado con software libre (Linux con distribución Debian 3.1) con el propósito de reducir costos para aumentar la viabilidad de la introducción en el uso. Como ya se había mencionado la lógica de programación de los dispositivos es la misma que en el módulo transmisor a excepción que su direccionamiento es diferente según la dirección del otro dispositivo telosB.

La instalación de todos los paquetes necesarios para el correcto funcionamiento de tinyOS y de nesC en este módulo, es muy diferente como se realiza en el

módulo transmisor, ya que en el sistema operativo Windows con dar click al ejecutable de tinyOS se instalan todos los paquetes, por el contrario en Linux se debe instalar paquete por paquete complicándose dicho proceso. En cuanto a la instalación de tinyOS y de nesC en Debian se pueden consultar el anexo B.

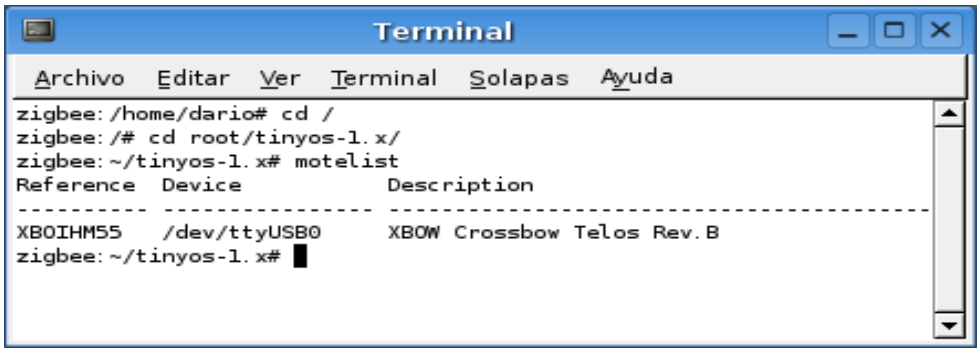

Figura 4.9 Motelist en debian

Para invocar al SerialForwarder se necesita saber en que puerto serial quedó asignado el dispositivo telosB como se hace en el módulo transmisor; pero teniendo en cuenta que bajo el sistema operativo Linux a dicho dispositivo no se le asigna directamente un puerto serial sino un puerto usb (como se muestra en la figura 4.9), se necesita hacer un enlace entre el puerto usb al puerto serial, para que el puerto usb se vea como serial, esto se consigue a través del siguiente comando.

```
#ln -sf /dev/ttyUSB0 /dev/ttyS0
```

Donde:

> /dev/ttyUSB0 significa el puerto usb en que quedó asignado el dispositivo telosB (en la mayoría de los casos queda asignado al USB0).
>
> /dev/ttyS0 es el número de puerto serial que quisiera que se convirtiera el puerto usb, se puede escoger otro número si se desea. /dev/ttyS0 es equivalente al puerto COM1.

Después se habilita el permiso al puerto a través del siguiente comando:

```
# chmod 666 /dev/ttyUSB0
```

Una vez se verifique la instalación de los paquetes java y javax.comm (ver anexo B) como uno de los requerimientos para interactuar con el SerialForwarder, se debe digitar el siguiente comando:

```
#export MOTECOM=serial@COM1:telos
```

Este comando hace referencia a que cada vez que se quiera conectar el dispositivo telosB; la variable de entorno [9] MOTECOM simplifica la conexión con la aplicación, diciéndole a java que paquetes debe escuchar por el puerto.

4.2.1.1 Instalación de la Aplicación

Para realizar la instalación, simplemente se copia la carpeta base del directorio /Aplicación del Receptor/ en la ruta ~/tinyos-1.x/tools/java/net/tinyos; para ejecutar la aplicación primero es necesario situarse en el siguiente directorio:

```
#cd ~/tinyos-1.x/tools/java
```

Posteriormente se ejecuta el siguiente comando:

```
#java net.tinyos.base.MainClass.
```

La aplicación del dispositivo telosB receptor implementada en el lenguaje de programación nesC para su funcionamiento se debe colocar la carpeta SensorRx en ~/tinyos-1.x/apps/. Para ver mas detalle de cómo compilar una aplicación en tinyOS se puede consultar al anexo B.

Para la instalación de asterisk se utilizó el recurso de gestor de paquetes[10] , se instaló la versión 2.7 .Los softphones utilizados son los x-lite con su última versión la 3.0 (ver figura 4.10).

Figura 4.10 Softphone X-lite

[9] nombre asociado a una cadena de caracteres
[10] digitando el comando `synaptic`

4.2.1.2 Aplicación del Módulo Receptor

La aplicación del módulo receptor consiste en una base de datos, pero en si no es una base de datos como tal, es un simulador ya que la idea es hacer un proyecto piloto para demostrar que puede funcionar si se lleva a la práctica. La aplicación inicia como se muestra en la figura 4.11. El código de programación se puede ver en el anexo C o en el CD de apoyo.

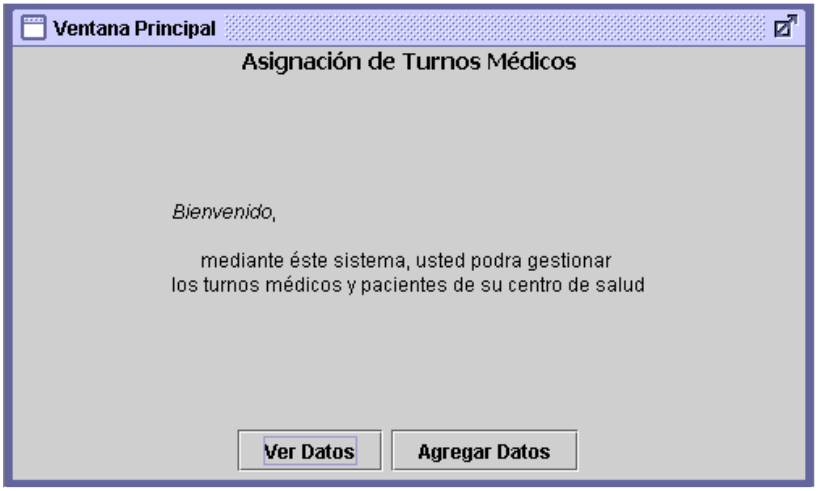

Figura 4.11 Asignación de turnos médicos

En la figura 4.11 se observa, que pueden ingresar dos tipos de usuarios al modelo de base de datos, uno de ellos es la persona encargada de agregar y ver los datos tanto de los pacientes como los médicos, el cual puede ser el administrador del hospital (presionando “Agregar datos”);el otro usuario es el médico que puede ver la información de los pacientes como la asignación de los turnos(presionando “Ver Datos”). Para el usuario que desea agregar datos le aparece una ventana como se muestra en la figura 4.12, en la cual tiene que logearse correctamente con su nombre y debe digitar un password para ingresar a la base de datos.

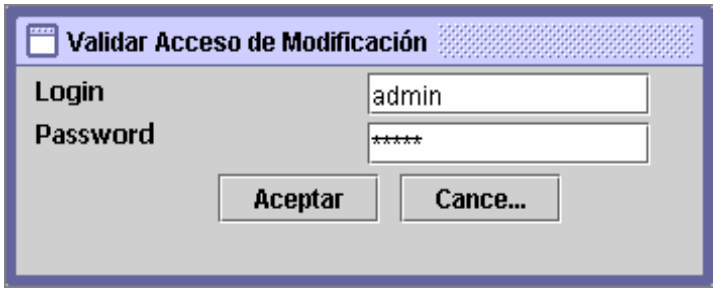

Figura 4.12 Validar acceso del administrador

Una vez que el administrador haya diligenciado correctamente los datos (en este caso admin y ritmo respectivamente), tiene dos opciones; ingresar los datos de los pacientes como se muestra en la figura 4.13 en donde puede guardar o borrar la

información de los pacientes; y la segunda opción consiste en ingresar los datos de los médicos con su respectivo identificador como se muestra en la figura 4.14.

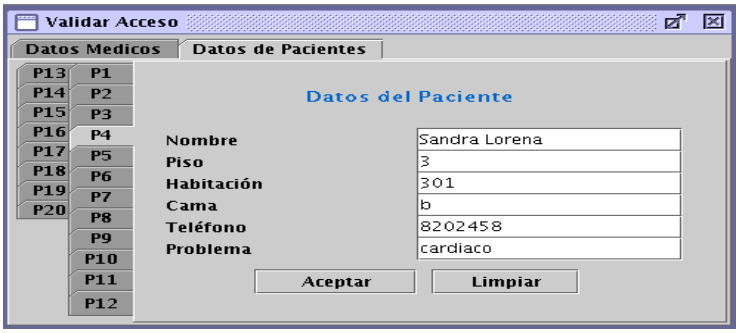

Figura 4.13 Datos de los pacientes

Una vez el administrador ha ingresado el nombre del médico con su identificador, se realiza la asignación de horario de turnos, está se puede llevar a cabo una vez se ingrese los datos (nombre e identificador) de cada médico o cuando se hayan ingresado los datos de todos los médicos en servicio (ver Figura 4.15).

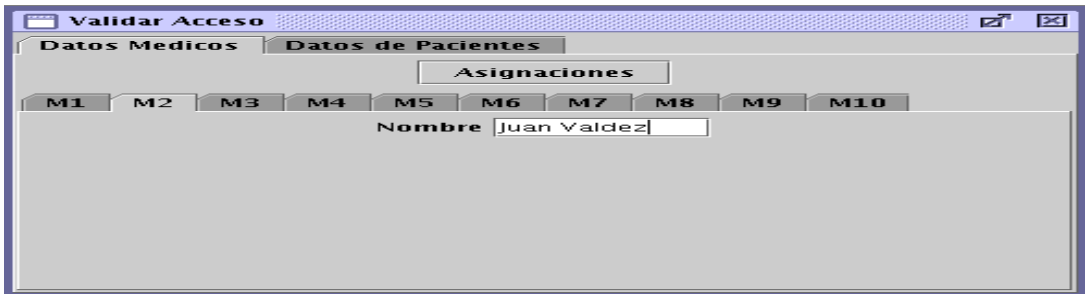

Figura 4.14 Datos de los médicos

	Lunes	Martes	Miercoles	Jueves	Viernes	Sabado	Domingo
12-6 AM	m3	m1	m2	m5	m4	m2	m5
6-12 AM	m5	m3	m4	m1	m2	m3	m4
12-6 PM	m4	m5	m5	m2	m1	m4	m3
6-12 PM	m2	m4	m1	m3	m3	m1	m2

Figura 4.15 Asignación de turnos de los médicos

Se debe tener en cuenta que a cada médico se le asigna un número de extensión, con el fin de localizarlo cuando se presente un problema con los pacientes, esté número es necesario para la interacción con asterisk.

Asterisk es una aplicación de código abierto de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP. Es considerada una aplicación "servidor" que permite que terminales "clientes" que pueden ser softphone o teléfonos IP se conecten a él, permitiendo que distintos dispositivos puedan tener comunicaciones de VoIP entre sí. Al igual que cualquier PBX de oficina, cada dispositivo recibe un número de extensión para identificarlo, esté número es ubicado en el archivo sip.config el cual sirve para configurar todo lo relacionado con el Protocolo de iniciación de sesión (SIP- *Session Initiation Protocol*) y añadir nuevos usuarios o conectar con proveedores SIP. También dentro de asterisk existe otro archivo llamado extensions.conf el cual es el más importante de Asterisk y tiene como misión principal definir el dialplan o plan de marcado que seguirá la PBX para cada contexto, y por tanto para cada usuario. El archivo de configuración sip.conf como el extensions.conf se encuentra en el anexo C o en el CD de apoyo.

El número de extensión se asigna a cada médico el cual es configurado en su softphone o teléfono IP (ver figura 4.16), por ejemplo, al médico Juan Valdez se le asignó el número de extensión 2116 y tiene como dirección IP del servidor de asterisk al 172.16.42.81.

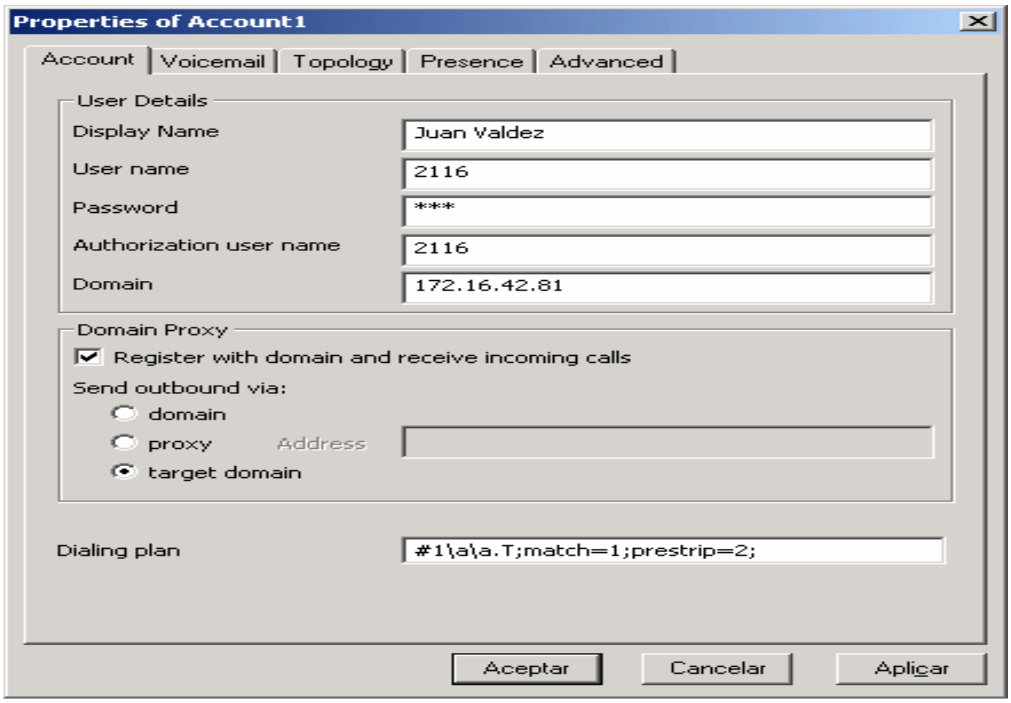

Figura 4.16 Configuración del softphone

Asterisk, también permite la utilización de mensajes pregrabados, los cuales en este caso son necesarios para informar a los médicos el estado del paciente. Los mensajes pregrabados son archivos con extensión .gsm por lo que asterisk sólo

reconoce estos archivos y deben ser colocados en el siguiente directorio var/lib/asterisk/sound y a su vez ser configurados en el archivo extensions.conf. El archivo extensions.conf permite realizar la operación lógica y enlazar los mensajes; hay seis tipos de mensajes pregrabados, los primeros cuatros dicen “el paciente x” donde x hace referencia al paciente y los otros dos dicen que problema a sufrido, por ejemplo se puede enlazar el paciente 1, 2, 3, o 4 con uno de los problemas de trastornos cardiacos, ya sea, bradicardia o taquicardia, por lo tanto, el mensaje completo que se escucha es: el paciente 1 (enlace) sufre bradicardia.

4.3 PRUEBAS REALIZADAS Y RESULTADOS OBTENIDOS

Es necesario aclarar para las pruebas finales que:

- Los signos vitales que se van a transmitir son simulados, luego el transporte se hace a través de los dispositivos telosB, es decir, no se realiza una captura física en tiempo real con los sensores; sino que se genera un dato mediante la simulación del ritmo cardíaco para trasmitirlo con periodo de un segundo, en este proceso los dispositivos transmitieron sin ningún problema. Fue necesario simular los signos vitales ya que no se contaba con los sensores adecuados para percibir el ritmo cardíaco del paciente, este elemento es de vital importancia para el proceso de transmisión de datos del sistema; además no era conveniente para la salud del paciente someterlo a numerosas pruebas que se tuvieron que realizar para el funcionamiento de los dispositivos. El cambio que se daría para un sistema real sería a nivel de hardware ya que se requiere de sensores que van conectados al paciente y éstos al dispositivo telosB transmisor**,** es decir, cada paciente tendría conectado un sensor llamado pulsímetro(utilizado para medir velocidad de los latidos del corazón o pulso cardíaco) y éste a su vez conectado al dispositivo telosb (mediante los pines de expansión), que en caso de presentar un problema con el paciente genera una comunicación inalámbrica a un sistema de conmutación automática para avisar al medico correspondiente.

- El enrutamiento en la parte receptora se presentó sin inconvenientes (porque solamente hay un dispositivo transmisor), por lo tanto, todo paquete que llego al sistema de conmutación automática fue dirigido a su destino,

Como solo se tienen dos dispositivos no se puede generar un tráfico, por lo tanto la viabilidad de esté proyecto esta que no se caiga el enlace para que no se pierdan paquetes entre transmisor y receptor; por lo tanto, el plan de pruebas se realizó para constatar el funcionamiento de los parámetros que permiten observador esta característica , dentro del estándar ZigBee son el Indicador de calidad del enlace (LQI *Link Quality Indication*) y la intensidad de la señal recibida (RSSI-*Received Signal Strength Indicator*), y adicionalmente constatar la caiga de voltaje de las baterías de dichos dispositivos.

4.3.1 Caracterización de la Calidad del Enlace 802.15.4

La calidad del enlace es de gran importancia especialmente en sistemas de transmisión inalámbrica, debido a ello, en el estándar 802.15.4 existen algunos parámetros que permiten medir dicha característica, entre ellos están el LQI y el RSSI. Como se vio en la sección 2.3.1 del capitulo 2**,** los valores de LQI y RSSI los proporcionan las capas PHY (física) y MAC del IEEE 802.15.4, y están implementados en el chip CC2420. Los paquetes 802.15.4 se transmiten teniendo dos bytes de FCS que se comprueba en el extremo receptor. Cuando el paquete pasa a la capa MAC del receptor, este campo de dos bytes es reemplazado. El RSSI, medido sobre los primeros ocho símbolos que siguen al SFD, ocupará el primer byte del FCS. El bit más significativo del segundo byte corresponde al CRC, que indica si la trama recibida es correcta. Y por último, los 7 bits menos significativos del segundo byte del FCS se reemplazan con el LQI, que se basa en un muestreo de la tasa de error de los primeros ocho símbolos de la cabecera de la trama recibida de la capa PHY. Este muestreo genera un valor de correlación dentro del rango [50,110]. En la figura 4.17 se muestra gráficamente los campos comentados.

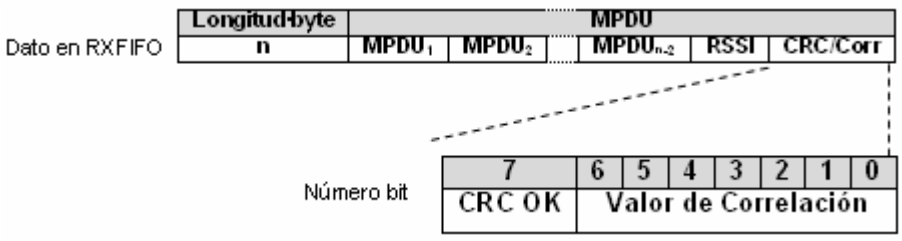

Figura 4.17 Datos en RXFIFO [33]

4.3.2 Pruebas Realizadas

Las pruebas realizadas se hicieron teniendo en cuenta las potencias y los canales utilizados, las características de la calidad del enlace, y la duración de las baterías. Se realizó un programa en nesC tanto para el dispositivo telosB transmisor como para el receptor, en cual, el telosB transmisor envía un paquete al telosB receptor, posteriormente cuando se recibe el telosB receptor empieza a enviar un paquete cada 10ms al telosB transmisor hasta llegar a 200 paquetes; una vez el telosB transmisor recibe los paquetes, se recopilan los parámetros deseados a través del SerialForwarder y de la aplicación en java (utilizando la misma aplicación del ritmo cardíaco pero modificando la interfaz), luego se imprimen los datos en pantalla. El código de programación de está prueba se puede ver en el anexo C o en CD de apoyo.

4.3.3 Escenarios

La prueba se realiza en el pasillo del tercer piso de la facultad de ingeniería electrónica y telecomunicaciones de la Universidad de Cauca, el cual, cuenta con una distancia máxima de 50 metros de longitud (se lleva a cabo en esté lugar ya que se asemeja a un entorno hospitalario). Las pruebas se realizaron en el canal 11 y en el canal 26, utilizando varias potencias de transmisión -25, -20,-15 y 0 dBm, en la cual ambos dispositivos están configurados con la misma potencia para cada prueba. En la toma de medidas en algunos instantes se encuentran personas transitando por el lugar lo que se asemeja en condiciones reales.

4.3.3.1 Escenario 1: En el pasillo

El escenario en el pasillo se implementa de la siguiente forma: el dispositivo telosB transmisor se encuentra fijo al pc de la aplicación de toma de datos que esta ubicado en el interior de una oficina, pero con una extensión usb se prolonga hasta el comienzo del pasillo, posteriormente se dispone a alejar el otro dispositivo metro por metro hasta llegar al punto donde no hay transmisión; como se muestra en la figura 4.18. Este escenario tiene la finalidad de ver cual es el alcance de transmisión de los dispositivos en un entorno similar al hospitalario.

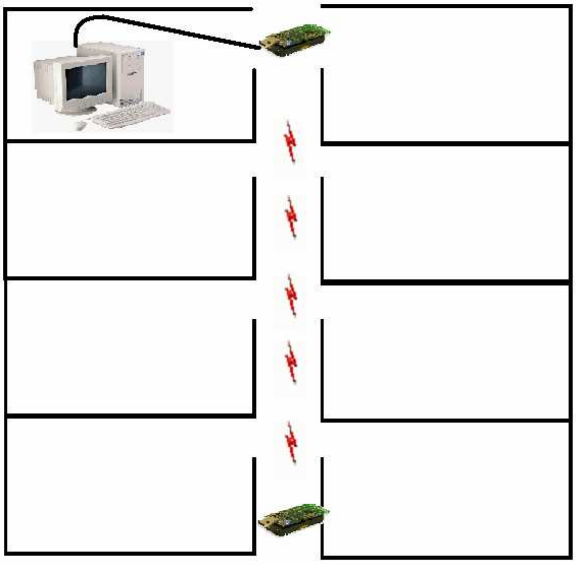

Figura 4.18 Escenario 1 en el pasillo

- **LQI**

Los valores de LQI pueden ir de 50 a 110, donde el valor 50 va asociado a la mínima calidad y 110 a la máxima. Una vez conocidos los rangos de valores que deberían obtenerse en las medidas, se pasó a diseñar las pruebas para caracterizar el comportamiento del LQI con la distancia. Los valores tomados para LQI son valores medios.

LQI-Prueba 1

La primera prueba se realizó con una potencia máxima (0 dBm) y en el canal 11. En la figura 4.19 se observa los datos tomados del LQI con respecto a la distancia. Cuando ambos dispositivos se encuentran a una distancia de 0 metros se pude observar que tiene el valor máximo LQI y mientras se va alejando el dispositivo telosB receptor el comportamiento del LQI tiene una forma decreciente pero no lineal; esto ocurre debido a que la onda se encuentra en un entorno cerrado donde se presentan reflexiones y posibles interferencias en el medio como: paredes y personas que en ese momento se encuentran transitando por el pasillo.

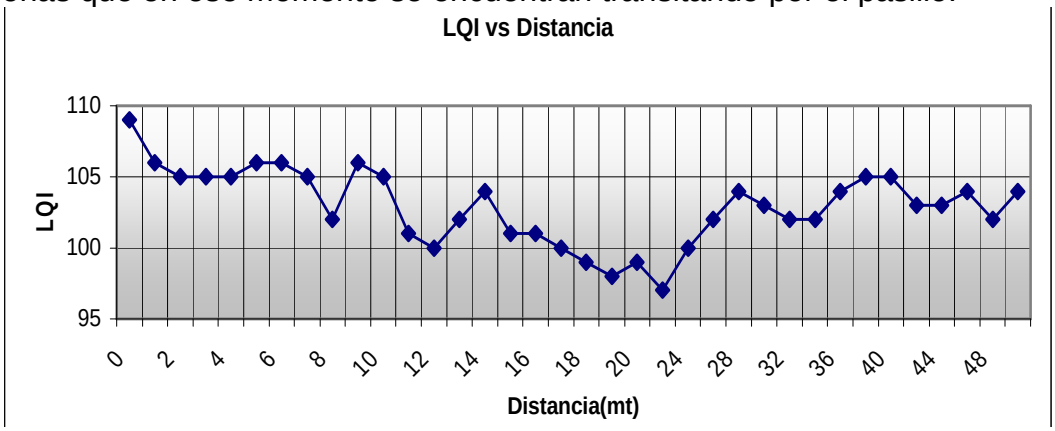

Figura 4.19 LQI vs Distancia (potencia 0 dBm, canal 11)

LQI-Prueba 2

Se realizó la misma prueba anterior pero con un nivel de potencia media (-15 dBm), y un canal de 26; dado que el comportamiento fue similar al obtenido en la prueba 1 se optó por cambiar el nivel de potencia media por un nivel intermedio entre la potencia mitad y la potencia mínima (-25 dBm), es decir, una potencia de -20 dBm, sin embargo, con este nueva potencia el comportamiento continua siendo similar al obtenido en la potencia intermedia (ver figura 4.20).

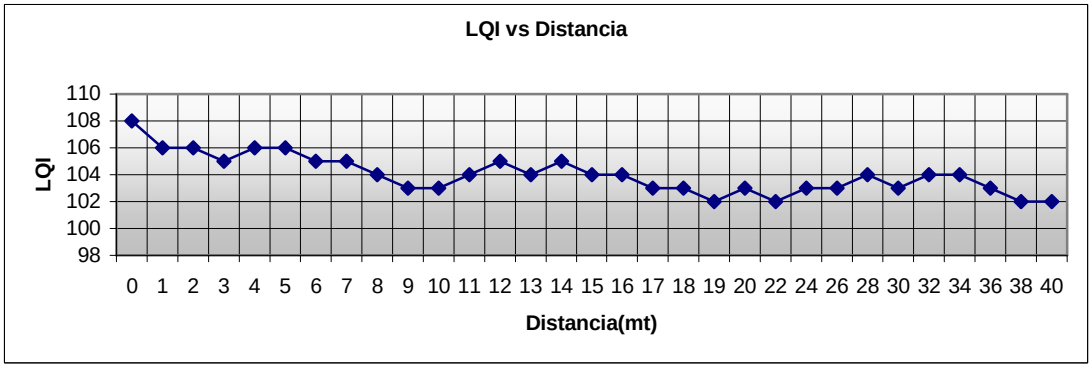

Figura 4.20 LQI vs Distancia (potencia -20dBm, canal 26)

LQI-Prueba 3

En la siguiente prueba se configuraron los dispositivos a una potencia mínima (-25 dBm) con el canal 26, pero solo se logró un alcance de 1 metro, lo cual no satisface los requerimientos que se está trabajando.

- **RSSI**

Los valores de RSSI obtenidos corresponden al valor del registro RSSI_VAL. Las potencias recibidas siempre tendrán signo negativo debido a que el rango de potencias de transmisión en telosB va de –25 dBm a 0 dBm, se debe obtener el valor real de potencia recibida, usando la siguiente la fórmula :

P_{RX} = RSSI_VAL + RSSI_OFFSET [dBm],

Donde el manual del chip CC2420 indica usar un valor de offset de – 45.

Una vez conocidos los rangos de valores que deberían obtenerse en las medidas, el siguiente paso es diseñar las pruebas para caracterizar el comportamiento del RSSI con la distancia. Los valores tomados para RSSI son valores medios que corresponde a la potencia recibida.

RSSI-Prueba 4

La primera prueba realizada con una potencia máxima (0 dBm), utilizando el canal 26, como se observa en la figura 4.21. La relación de la potencia recibida con la distancia también sufre una tendencia decreciente, que empieza por una potencia recibida de -55 dBm. Aunque la potencia de transmisión en este caso es máxima, hay que tener en cuenta que tanto las pérdidas de transmisión como de recepción y las interferencias del medio, hace que la potencia recibida alcance estos valores tan bajos. También se muestra que en la distancia de 7 metros la señal sufre un pequeño aumento, probablemente se debe a que en la pared de ese lugar del pasillo hay irregularidades (un hueco), permitiendo que la señal aumente un poco.

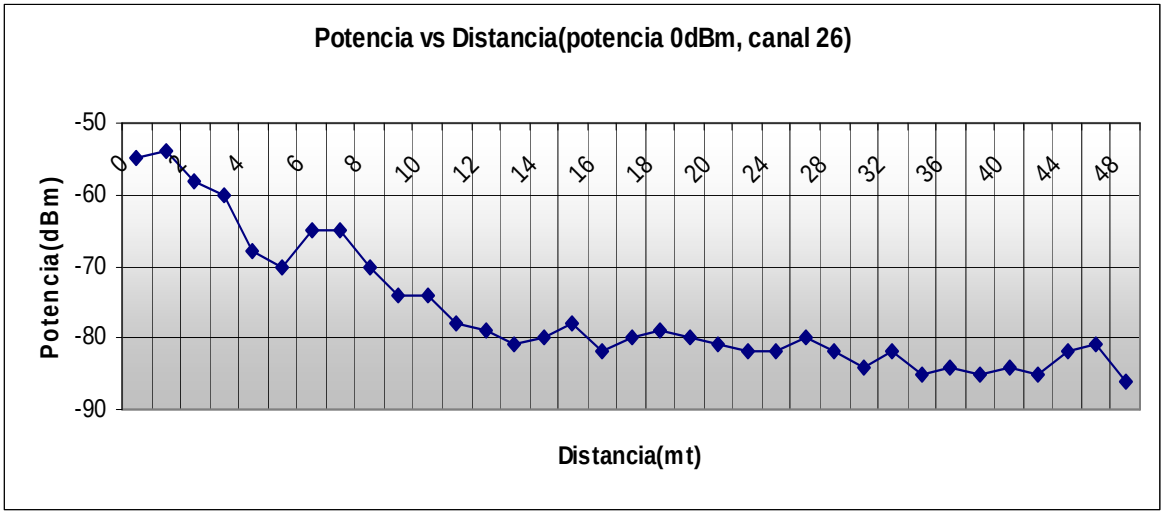

Figura 4.21 Potencia recibida vs Distancia

RSSI-Prueba 5

Igual que en el caso del LQI, se realizo una prueba con una potencia intermedia entre la potencia intermedia (-15 dBm) y la potencia mínima (-25 dBm), sin embargo, con está nueva potencia el comportamiento continua siendo similar al obtenido en la potencia intermedia (ver figura 4.22).

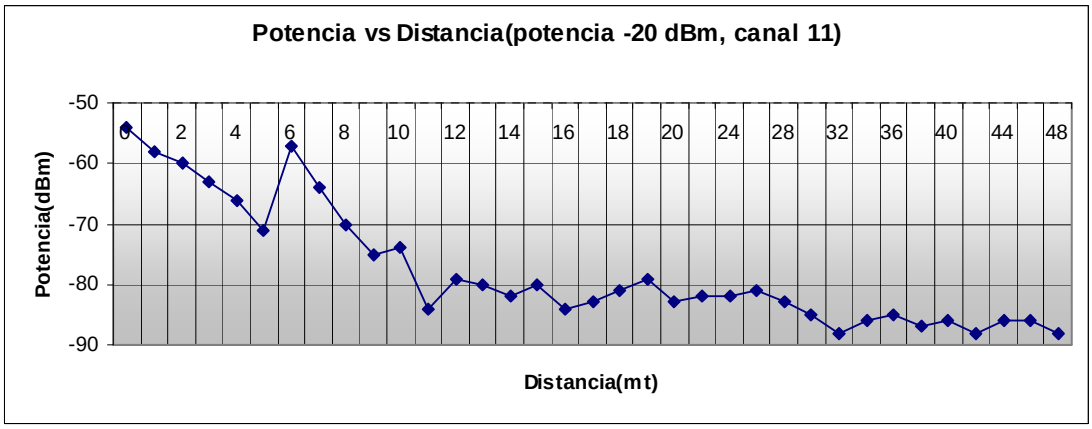

Figura 4.22 Potencia recibida vs Distancia

RSSI-Prueba 6

En la siguiente prueba se configuraron los dispositivos a una potencia mínima (-25 dBm) con el canal 26, pero solo se logró un alcance de transmisión de un 1 metro, lo cual no satisface los requerimientos que se está trabajando.

4.3.3.2 Escenario 2: Con obstáculo

El escenario 2 con obstáculo se implementó de la siguiente forma: el dispositivo telosB transmisor se deja fijo junto al pc de la aplicación de toma de datos ubicado en el interior de la oficina, de tal manera que se encuentre alejado 5 metros del inicio del pasillo, mientras el otro dispositivo telosB receptor se aleja metro por metro hasta llegar al punto donde no hay transmisión como se muestra en la figura 4.23. Este escenario tiene la finalidad de determinar cual el alcance de transmisión de los dispositivos cuando presentan obstrucciones en él y comprobar si afecta notablemente el enlace.

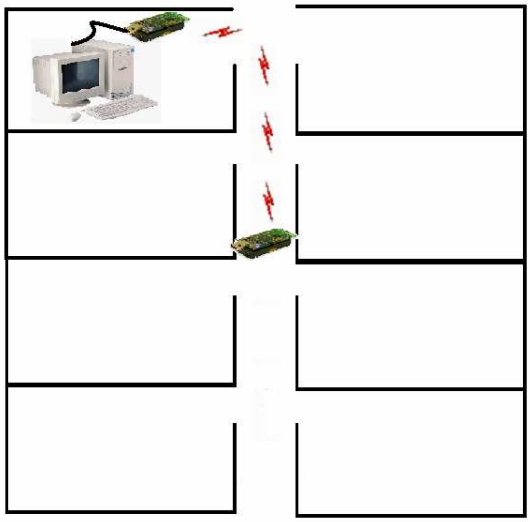

Figura 4.23 Escenario 2 Con obstáculo

- **LQI-Prueba 7**

Esta prueba se realizó con una potencia máxima y utilizando el canal 26 (ver figura 4.24), se observa como LQI tiene un comportamiento uniforme hasta los 6 metros, después comienza a decrecer rápidamente hasta los 9 metros, y a partir de los 10 metros deja de recibir paquetes. Por lo tanto, para un transporte adecuado se debe pensar en diseños libres de obstáculos así como múltiples saltos con línea de vista o malla.

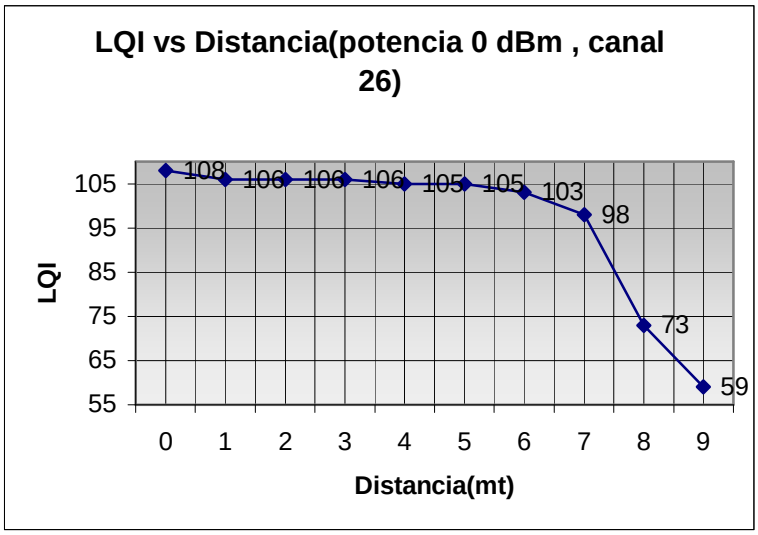

Figura 4.24 LQI vs Distancia (potencia 0 dBm, canal 26) con obstáculo

LQI-Prueba 8

Se configuró con una potencia mitad (-15 dBm) y se utilizó el canal 26 (ver figura 4.25)

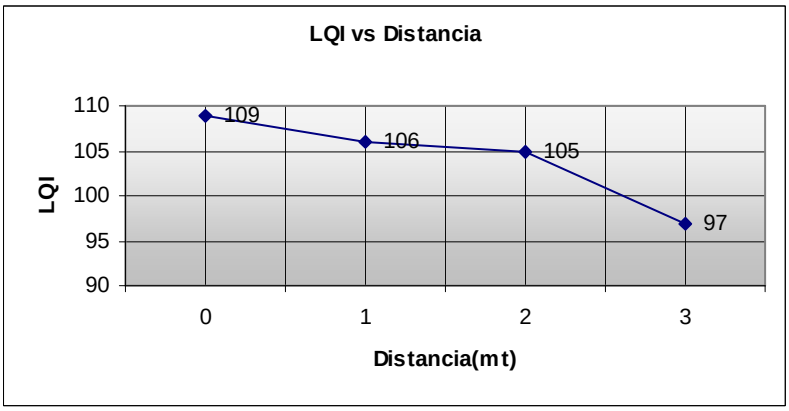

Figura 4.25 LQI vs Distancia (potencia -15 dBm, canal 26) con obstáculo

La Figura 4.25 muestra que se tiene un comportamiento similar al obtenido en la prueba 7 (ver Figura 4.24), aunque con un alcance menor debido a que se utiliza una menor potencia, el alcance es de tan solo 3 metros. En esta prueba el comportamiento de la figura 4.23 es similar al de la figura 4.22, pero en este caso el alcance es de tan solo de 3 metros.

- **RSSI-Prueba 9**

Se configuró con una potencia máxima (0 dBm), utilizando el canal 26, en la cual se logró un alcance de 9 metros con una potencian recibida de -94 dBm (ver figura 4.26).

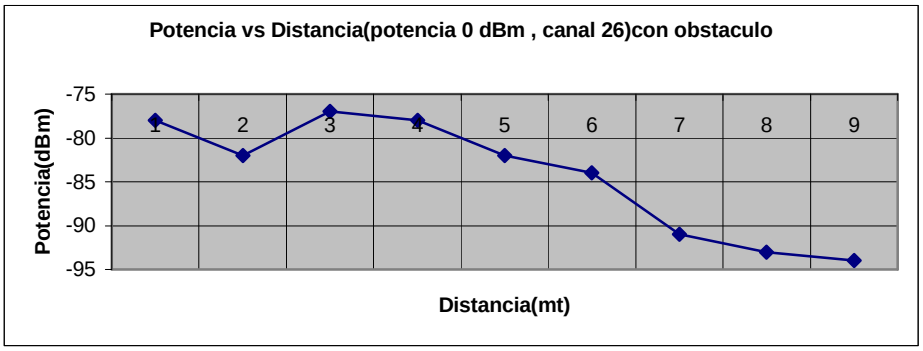

Figura 4.26 Potencia recibida vs Distancia

- **RSSI-Prueba 10**

Así mismo se realizo con una potencia intermedia (-15 dBm), utilizando el canal 26, por tener una potencia menor a la que se utilizó con la potencia máxima va a tener un alcance menor, en este caso de 3 metros como se muestra en la figura 4.27.

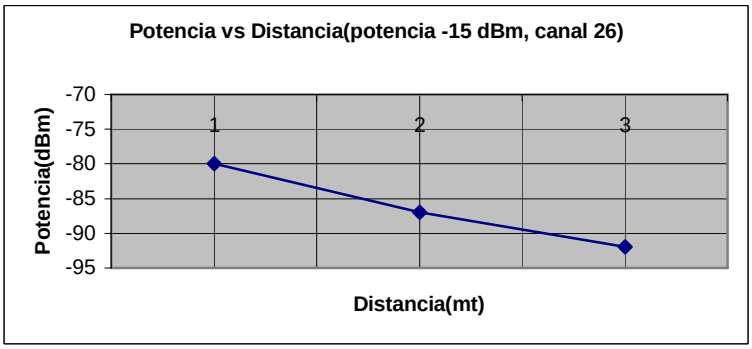

Figura 4.27 Potencia vs Distancia

4.3.3.3 Escenario 3 Prueba de batería

Para realizar las pruebas de batería se utilizaron pilas recargables, con la finalidad que al inicio de cada prueba se recargaban completamente, permitiendo tomar medidas más fiables. Las dos pruebas se hicieron dejando ambos dispositivos telosB fijos a una distancia de 50 metros, en la cual uno de ellos transmitía un paquete cada medio segundo y el otro lo recibía, se tomaban muestras con las dos baterías en serie cada 10 minutos durante un tiempo de 3 horas. Cuando

llegan los paquetes al dispositivo telosB receptor, se enciende el led rojo para confirmar que ha llegado un paquete, y que las baterias todavía tienen capacidad para seguir transmitiendo. La prueba se realizó con dos potencias: una con potencia mitad y la otra con potencia máxima como se observa en la figura 4.28 y 4.29 respectivamente.

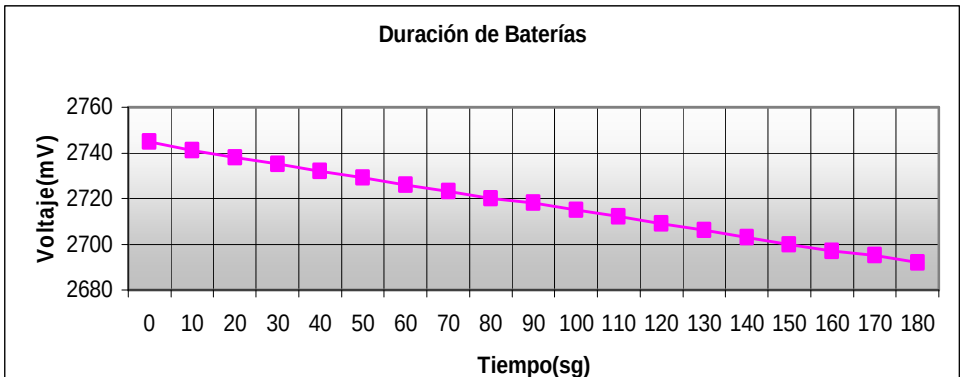

Figura 4.28 Caída de tensión de las baterías durante 3 h. .Potencia -15 dBm

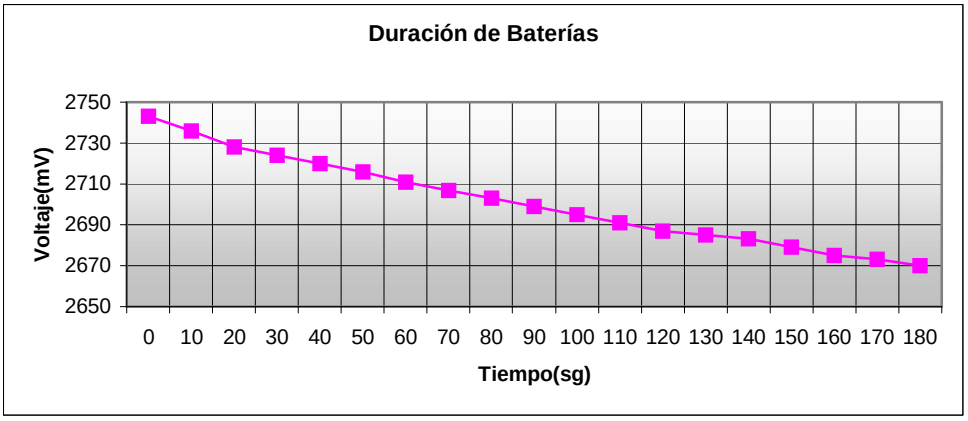

Figura 4.29 Caída de tensión de las baterías durante 3 h. .Potencia 0 dBm

El desgaste de la batería se debe a los periodos cuando esta transmitiendo de lo contrario la batería permanecería en su mismo estado En estas pruebas se observa una caída lineal del voltaje, para 0dBm existe un caída de tensión de 4mV mientras que para -15dBm la caída de tensión es más suave 3mV, que es lo esperado; a mayor potencia mayor consumo y a menor potencia menor consumo.

CONCLUSIONES , RECOMENDACIONES Y TRABAJOS FUTUROS

CONCLUSIONES

- **Generales**

  La generación de estándares nuevos como el tratado en esté trabajo de grado, ofrece un impacto fuerte sobre la demanda actual de soluciones inalámbricas con capacidades de consumo mínimo de potencia, ancho de banda reducido, entre otras, por cuanto la adopción de estos en las tecnologías de comunicación garantiza soluciones, acordes con la evolución del mercado y con la transformación continua de los requerimientos de cada entorno, mejorando la efectividad de los beneficios alcanzados en medios industrial, hospitalarios, ambientales, domóticos, etc.

  La tecnología ZigBee, trata de convertirse en unas de las principales pciones en cuanto a redes de sensores se refiere a corto y mediano plazo, para lograr el camino más efectivo y atractivo para alcanzar una penetración amplia en los diversos mercados, debido sus cualidades, volviéndose una oportunidad de negocio con expectativas ampliamente alcanzables.

  En el ámbito nacional y local es evidente que la tecnología no se ha profundizado, por lo tanto no se está a la vanguardia en el desarrollo de la misma, con lo cual es necesario profundizar en ella de manera que este proceso traduzca sus resultados en beneficios sociales trascendentales, máxime, teniendo en cuenta que en el país el acceso a las TICs (Tecnologías de la Información y las Comunicación) es uno de los objetivos estratégicos más recientes e importantes entre las políticas del gobierno y por lo tanto se puede presumir de un espacio asegurado para la penetración de tecnologías inalámbricas.

- **Especificas**

  Las WSN son redes que no tienen una estandarización aun definida, es decir, en las diferentes capas que trabaja dentro del modelo OSI existen diferentes protocolos de acuerdo al proyecto a realizar y cada uno prioriza según sus necesidades, en la actualidad apenas se puede hablar de Zigbee como estándar para estas redes. Asimismo, se puede destacar que esté tipo de redes, dentro del Departamento de Telecomunicaciones todavía no es tema de profundización.

  Con el estudio teórico del estándar Zigbee, se profundizó en su funcionamiento y las grandes vías de desarrollo que ofrece en aplicaciones dentro de las redes

WSN y las LR- WPAN, gracias principalmente a su bajo costo proyectado y un consumo de potencia extremadamente bajo mediante el uso de las tramas beacon que permiten la posibilidad de estar 'dormidos' durante grandes periodos de tiempo. Es de destacar que para esto, la bibliografía existente para el estándar IEEE 802.15.4 es amplia, contraria a las capas que específica la "Alliance ZigBee" donde la bibliografía solo se remite a la especificación.

Una red ZigBee puede estar formada por una cantidad considerable de nodos (256 o hasta 2^{16} si se utiliza direccionamiento local), además dentro de sus topologías permite las redes en malla las cuales son ideales para el cubrimiento de zonas amplias y permiten diferentes caminos para que lleguen los datos del origen al destino.

El estándar Zigbee para su operación utiliza una cantidad baja de primitivas en comparación con las que se utilizan en bluetooth lo cual hace que su estudio sea más sencillo y que presente un stack (Es el software que facilita cada empresa en su dispositivo.) de las diferentes empresas (Microchip, Ember etc.) más simple.

En la capa aplicación no existen aplicaciones finales, estas son realizadas por los usuarios basándose en perfiles aprobados por la "Alliance ZigBee" para permitir interoperabilidad. En el momento hay pocos definidos, entre los que se encuentran el control domótico e industrial, con lo cual todavía no hay homogeneidad en entornos.

Se desarrollo la aplicación mediante el lenguaje nesC y se interactuó con java con el objetivo se realizar el entorno gráfico para simular el ECG y con ello las alteraciones bradicardia y taquicardia, es decir, se pudo simular datos en la tarjeta sin necesidad que estos entrarán por medio de los sensores.

Con el piloto de aplicación los sistemas de monitorización hospitalaria pueden transmitir señales biomédicas que permiten realizar un pre-diagnóstico y pueden generar alarmas en caso de emergencia, cambiando de está manera la monitorización tradicional.

Se implementó un piloto con software libre: Asterisk y con tecnologías inalámbricas: ZigBee, para reducir costos y aumentar la viabilidad de implementación.

El estándar ZigBee puede proyectarse en entornos hospitalario para la monitorización permanente, principalmente por tres motivos: primero, por el ahorro económico que suponen las redes inalámbricas al no necesitar de una infraestructura global, es decir, el cableado; además porque el precio de los dispositivos se proyectan bajos; segundo, por la posibilidad y comodidad de usar los sistemas desde cualquier localización, y tercero, por el ahorro de

potencia que los dispositivos presentan y su diminuto tamaño que facilita la implantación en cualquier parte del cuerpo.

La implementación de este piloto de sistema de monitorización remota descrito en esté trabajo de grado demuestra la viabilidad para pacientes con algún tipo de patología cardiaca, por lo tanto, puede ser fácilmente adaptado a otros tipos de pacientes con otras patologías.

- **Resultados de las pruebas**

Los parámetros RSSI y LQI en entornos indoor sin obstáculos no varían en una cantidad significante, siempre tienen un promedio cercano al máximo, pero con obstáculos disminuyen, lo cual afecta el alcance y por lo tanto se pierde el enlace provocando la pérdida de paquetes, es decir, los parámetros RSSI y LQI están por debajo de los parámetros de funcionamiento normal. Otro factor que influye dentro de los parámetros RSSI y LQI es la potencia de transmisión, es decir a mayor potencia mayor alcance, aquí también se tiene en cuanta los obstáculos con las consideraciones expuestas.

En cuanto al consumo de potencia por parte de las baterías, depende de la potencia de transmisión (a mayor potencia más consumo) y el transceptor cuando esta los modos activo o dormido. De esta manera para una aplicación que active los sensores de forma esporádica la duración de las baterías será larga ya que no habrá un uso constante del transceptor, permitiendo que una duración de meses.

5.1 RECOMENDACIONES Y TRABAJOS FUTUROS

- Realizar profundización en las WSN, sus características, protocolos, estándares, para que sean tema de aprendizaje y desarrollo para futuros trabajos de grado.

- Trabajar sobre los perfiles definidos del estándar ZigBee, para conocer el alcance en las capas superiores, porque en esté trabajo de grado por los dispositivos usados solo se profundizó en las capas inferiores.

- Realizar la adquisición de datos para la transmisión en forma real, es decir por medio de los sensores o por los puertos de expansión de la tarjeta de telos b.

- Otra línea futura para este proyecto sería probar otras plataformas de sensores como MicaZ (dispositivo de Crossbow que no tiene conexión USB) o tener más dispositivos que aportaría una real dimensión del alcance principalmente en el diseño de la red mesh.

- Como parte del aporte de este trabajo de grado se deja sentada una base cognoscitiva de la tecnología ZigBee y teórica para futuros trabajos encaminados hacia redes de sensores, abriendo así un espacio para futuros estudios y diversas aplicaciones que se pueden desarrollar en esta área de la llave con otros aplicativos como Asterisk.

BIBLIOGRAFÍA

[1] Ruiz, B., et al., “Arquiteturas para Redes de Sensores Sem Fio”, 2004

[2] Loureiro, A., et al., “Redes de Sensores Sem Fio”, XXI Simpósio Brasileiro de Redes de Computadores. White paper.

[3] Delffino Freire, J., “Sistemas Operacionais para os nós das Redes de Sensores sem Fio”.Junio de 2006.

[4] Menezes, M., “BEAN: Uma Plataforma Computacional para Rede deSensores Sem Fio”, Federal University of Minas Gerais Brasil, Abril, 2004.

[5] Ruiz, B., “MANNÁ: Uma Arquitetura para Gerenciamento de Redes de Sensores Sem Fio”, Federal University of Minas Gerais Brazil, Diciembre, 2003.

[6] Teixeira, I., “Roteamento com Balanceamento de Consumo de Energia para Redes de Sensores Sem Fio”, Rio de Janeiro, Brasil, Abril 2005

[7] Correia, L., et al .,“Uma Taxonomia para Protocolos de Controle de Acesso ao Meio em Redes de Sensores Sem Fio”, Universidade Federal de Minas Gerais Brasil. White paper 2005.

[8] Cabrini, F., et al., “Roteamento em Redes de Sensores Sem Fio”. Laboratório de Sistemas Integráveis, Universidade de São Paulo. White paper.

[9] Giulian, L., “Roteamento em Redes de Sensores”, Universidade de São Paulo. Noviembre de 2004

[10] Gonçalves, A., “Mecanismo de Agregação de Dados Empregando Técnicas Paramétricas em Redes de Sensores”, Rio de Janeiro, Brasil. Junio de 2004.

[11] Paiva. F., et al., “Seminario de Topicos em Telecomunicacoes:Redes de Sensores sem fio”, Brasil. White paper.

[12] Nelem, R., “Protocolo Tolerante a Falhas e de Baixa Latência para Redes de Sensores Sem Fio”, Universidade Sao Carlos Brasil. Diciembre 2004.

[13] Rios, M., “Redes inalámbricas de sensores”, Universidad Nacional de Rosario Facultad de Ciencias Exactas Ingeniería y Agrimensura., Noviembre 2003

[14] Roca, I., et al., “Abordagem Dos Sistemas Operacionais Para Redes de Sensores Sem Fio”, Laboratório de Sistemas Integráveis –Universidade de São Paulo Brasil. White paper.

[15] IEEE-Computer-Society, IEEE Std 802.15.4 IEEE Standard for Information technology - Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements, part 15.4. IEEE Inc., 2003, ISBN: 0-7381-3686-7.

[16] Zigbee-Standards-Organization, Zigbee Specification v1.1. Zigbee Alliance, 2005, Document number: 053474r07.

[17] Mayné, J," IEEE 802.15.4 y ZigBee" Freescale Semiconductor.

[18] Lönn, J., Olsson J, "Zigbee for wireless networking", Linköpings Tekniska Högskola. Marzo de 2005

[19] Coleri, S., "ZigBee/IEEE 802.15.4 Summary". Communications Design Conference. Septiembre de 2004.

[20] Ramazanali, H., "Characterization and evaluation of ZigBee modules". Linköpings Tekniska Högskola, Campus Norrkoping. Febrero de 2006.

[21] Kooistra A.J., "ZigBee In the context of service discovery", University de Twente. Mayo de 2006.

[22] Muñoz, J., "Arquitectura Abierta Escalable para Monitorización Domiciliaria: Aplicación a Pacientes con Patologías Cardíacas".2003.

[23] ZigBee Alliance., Architecture ZigBee Version 1.00 Open House presentations, ZigBee Document 043120r013ZB, Junio de 2006.

[24] ZigBee Alliance., AFG Overview Version 1.00 Open House presentations, ZigBee Document 053340r06ZB, Junio de 2006.

[25] ZigBee Alliance., NWK Layer Overview Version 1.00 Open House presentations, ZigBee Document 053551r05ZB, Junio de 2006.

[27] Vidal C., Pavesa, L., "Desarrollo de un Sistema de Adquisición y Tratamiento de Señales Electrocardiográficas". Fac. Ing. - Univ. Tarapacá, vol. 13 White paper, julio de 2005.

Referencias WEB

[26] Zigbee Alliance, http://www.zigbee.org.

[28] Crossbow Technology, Inc, http://www.xbow.com

[29] Asterisk, http://www.asterisk.org

[30] Chipcon AS, http://www.chipcon.com.

[31] TinyOS, http://www.tinyos.net

[32] Cygwin, http://www.cygwin.com

[33] Chipcon AS, Chipcon AS SmartRF CC2420 Preliminary Data sheet (rev 1.3)

[34] Bluetooth, http://www.bluetooth.com