



UNIVERSIDAD
DE LA REPÚBLICA
URUGUAY



UNIVERSIDAD DE LA REPÚBLICA
FACULTAD DE INGENIERÍA

ZigBee

Comunicaciones Digitales

Instituto de Ingeniería Eléctrica

Gastón Alvarez 4.850.999-3 galvado97@gmail.com
Nahuel Piñeyro 5.230.736-3 nahuel.pineyro@fing.edu.uy

Grupo 3

30 de Junio del 2022

Índice

1. Contexto y motivación	2
2. Objetivos	2
3. Introducción a ZigBee y al IEEE 802.15.4	2
4. Capas desarrolladas por ZigBee Alliance	4
4.1. Capa de Aplicación (APL)	4
4.2. Capa de Red (NWK)	4
5. Capas de Zigbee basadas en IEEE 802.15.4	5
5.1. Capa de acceso al medio (MAC)	5
5.2. Capa física (PHY)	8
5.2. a. Espectro	8
5.2. b. Binary phase-shift keying (BPSK)	8
5.2. c. Offset QPSK	10
6. Puesta en escena del ZigBee en GNU Radio	12
6.1. Transmisor:	12
6.2. Receptor:	13

ZigBee

Sistemas digitales

1. Contexto y motivación

En el marco de la asignatura Comunicaciones Digitales se nos fue encomendada la tarea de realizar este proyecto para analizar el funcionamiento de un sistema completo basado en los conceptos adquiridos en el curso. La motivación de analizar un sistema completo es interpolar los conceptos teóricos a una aplicación real

2. Objetivos

Este proyecto plantea como objetivo mostrar de manera concreta la tecnología ZigBee para redes inalámbricas[1]. Consta de dos partes, una parte teórica dónde se analiza meramente la estructura de la tecnología y una parte práctica dónde se pone a prueba el funcionamiento de las capas de ZigBee en GNU Radio[2]. Es pertinente remarcar que el proyecto no va a ahondar en todos los temas de la tecnología si no en solo aquellos que nos parecen los más adecuados para compartir conforme a lo dado en el curso.

3. Introducción a ZigBee y al IEEE 802.15.4

ZigBee es el nombre de la especificación creada por el grupo de trabajo ZigBee Alliance para la definición de un protocolo de comunicaciones inalámbrico de alto nivel [1]. Este protocolo toma como base el estándar IEEE 802.15.4 el cual define el nivel físico (Physical Layer, PHY) y el control de acceso al medio (Medium Access Control, MAC) en redes inalámbricas para un uso personal (un esquema de esto se puede ver en la figura 1) [3]. El propósito de ZigBee es brindar una solución completa para este tipo de redes, definiendo las capas superiores que el estándar no contempla en las cuales se trabaja con bajas tasas de transmisión de datos (Low-rate wireless personal area network, LR-WPAN) buscando la maximización de la vida útil de las baterías de los dispositivos conectados.

Para llevar a cabo este sistema, el grupo ZigBee Alliance formado por varias industrias, sin ánimo de lucro, trabaja codo con codo con IEEE para asegurar una integración, completa y operativa [1] [3]. La idea de la alianza es trabajar para crear un sistema estándar de comunicaciones, vía radio y bidireccional. Los miembros de esta alianza justifican el desarrollo de este estándar para cubrir el vacío que se produce por debajo del Bluetooth. Este último se concibió originalmente como un reemplazo de los cables, pero se ha ido por un camino más complicado que lo hace poco práctico para aplicaciones de bajo consumo. La tendencia hacia la complejidad aumenta el costo proporcionado por la tecnología. Los dispositivos Bluetooth requieren el reemplazo de la batería varias veces al año, lo cual no es práctico.

Resulta ser un sistema ideal para redes de automatización hogareña (domóticas), específicamente diseñado para la necesidad del mercado, obteniendo un estándar para redes Wireless de pequeños paquetes de información, bajo consumo, seguro y fiable. Esta nueva aplicación, definida por la propia

ZigBee Alliance como el estándar para la automatización del hogar, permite que las aplicaciones domésticas desarrolladas por los fabricantes sean completamente compatibles, garantizando así un buen funcionamiento [1].

Entrando más en la especificación de la tecnología podemos decir que ZigBee le agrega tres capas más al paquete de capas del IEEE (MAC y PHY), estas tres capas son la capa de aplicación (Application layer), capa de red (Network Layer) y los servicios de seguridad, las cuales las primeras dos se detallaran en la siguiente sección. Se pueden ver al igual que las capas del estándar representadas en el diagrama de la figura 1.

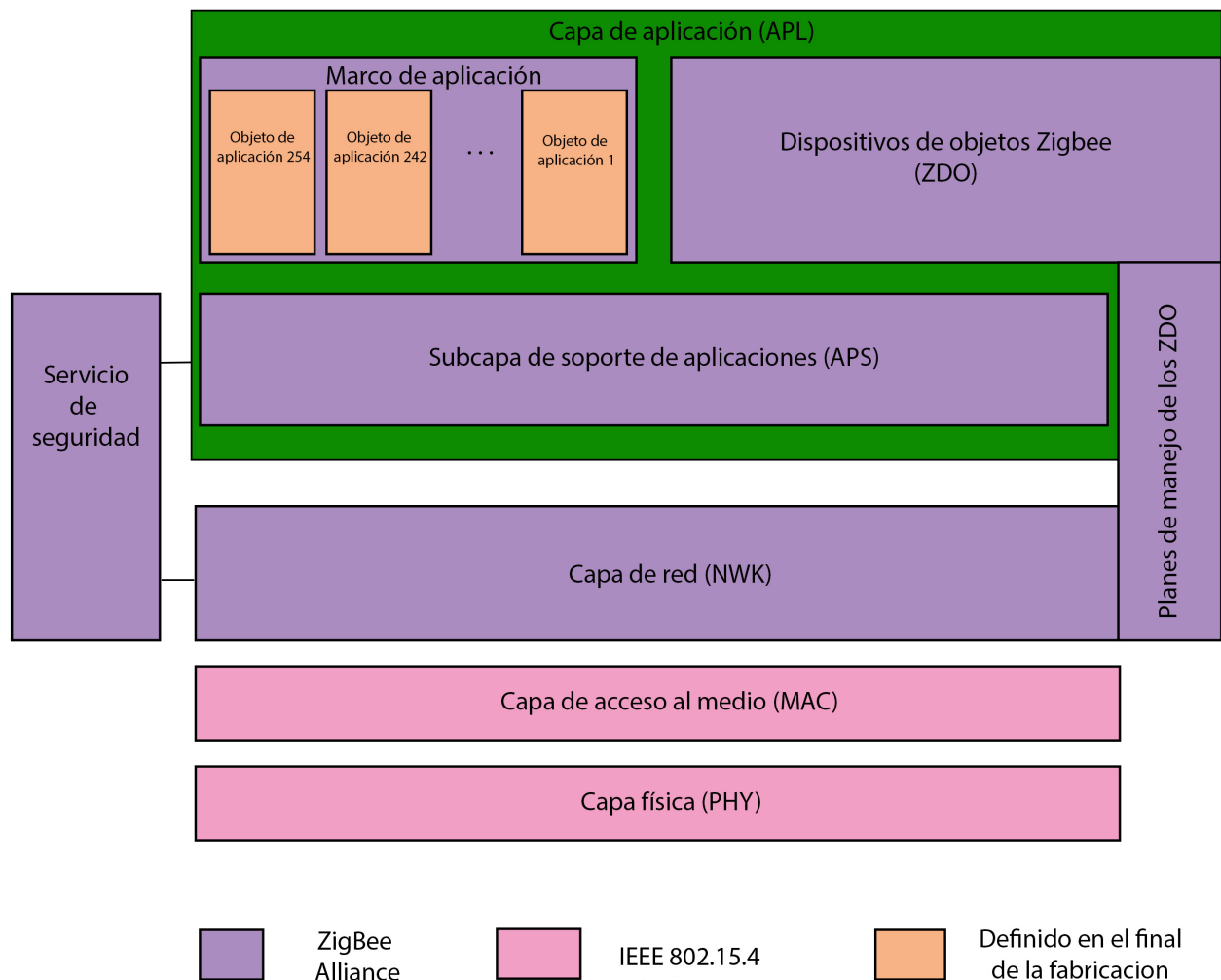


Figura 1: Diagrama de la estructura del estándar [3]

4. Capas desarrolladas por ZigBee Alliance

4.1. Capa de Aplicación (APL)

La capa de aplicación consta de tres partes, la subcapa de soporte de aplicaciones (APS), los dispositivos ZigBee y los objetos de aplicación definidos por el fabricante. Las tres partes trabajan en conjunto para facilitar a las aplicaciones la posibilidad de acceder a los servicios de las demás capas.

Definamos primero lo que es la subcapa APS, esta es la encargada de gestionar una interfaz entre la capa de red y la capa de aplicación brindando dos tipos de servicios por dos entidades diferentes, la entidad de datos y la entidad de gestión. La entidad de datos se encarga de la transmisión de datos entre dos o más entidades de aplicación ubicadas en la misma red y la entidad de gestión brinda una variedad de servicios a los objetos de la aplicación, como por ejemplo servicios de seguridad y la vinculación de dispositivos. Esta última también mantiene una base de datos de objetos gestionados.

Segundo definimos lo que son los objetos de dispositivo ZigBee (ZDO), estos brindan una interfaz entre los objetos de la aplicación, el perfil del dispositivo y el APS. Los ZDO son responsables de inicializar la APS, la capa de red y el proveedor de servicios de seguridad, además se encarga de reunir la información de configuración de las aplicaciones finales. Por último está el Marco de aplicación de ZigBee (Application Framework) el cual podemos decir que es el entorno en el que los objetos de la aplicación se alojan en los dispositivos ZigBee.

4.2. Capa de Red (NWK)

La capa de red es la encargada de hacer la conexión de manera correcta de la MAC y la capa de aplicación. Para interactuar con la capa de aplicación se incluye conceptualmente dos entidades de servicio, estas son el servicio de datos y el servicio de gestión.

La entidad de datos (NLDE) brinda un servicio de datos para permitir que una aplicación transporte unidades de datos del protocolo de aplicación (APDU) entre dos o más dispositivos y se encarga también de asegurar la autenticidad como la confidencialidad de una transmisión.

Por otro lado, la entidad de gestión (NLME) desempeña una cantidad numerosa de tareas, entre ellas se encuentra configurar nuevos dispositivos es decir asignarles una dirección correspondiente, crear, unirse, volver a unirse o salir de redes. Se encarga también descubrir nuevos vecinos, descubrir nuevas rutas y controlar la recepción, es decir, cuándo se activa el receptor y durante cuánto tiempo, habilitando la sincronización de la subcapa MAC.

5. Capas de Zigbee basadas en IEEE 802.15.4

5.1. Capa de acceso al medio (MAC)

La capa MAC es en realidad una subcapa de la capa de enlace de datos, pero nos interesa estudiar dicha subcapa ya que es la encargada de controlar el acceso al medio. La subcapa proporciona dos servicios: el servicio de datos MAC y el servicio de gestión MAC. El servicio de datos MAC permite la transmisión y recepción de unidades de datos del protocolo MAC (MPDU) a través del servicio de datos PHY.

Las características de la subcapa MAC son la gestión de balizas (utilizadas por los nodos para sincronizarse), el acceso al canal, el intervalo de tiempo garantizado (GTS), validación de tramas, entrega de tramas reconocidas, asociación y disociación. Además, la subcapa MAC proporciona enlaces para implementar mecanismos de seguridad apropiados para la aplicación.

Para empezar, un sistema conforme a esta norma consta de varios componentes. El más básico es el dispositivo. Un dispositivo tiene una sola interfaz de radio que implementa 802.15.4 MAC y PHY. Dos o más dispositivos que se comunican en el mismo canal físico constituyen una red de área personal inalámbrica (WPAN). Dentro de los dispositivos que se puede tener en una WLAN, existen 2 tipos diferentes que pueden participar en una red IEEE 802.15.4, estos son un dispositivo de función completa (FFD) y un dispositivo de función reducida (RFD).

1. FFD: También llamado nodo activo, se encarga de recibir mensajes en el formato del estándar. Este dispositivo es capaz de actuar como coordinador o router de área personal (PAN).
2. RFD: También llamado nodo pasivo, sus capacidades y funcionalidades son limitadas, buscando así obtener un bajo coste y consumo. En pocas palabras, son los sensores/actuadores que conforman la red.

Es importante notar que una WPAN incluye al menos un FFD que actúa como coordinador de la PAN, esto se ve claramente en la siguiente figura en la cual se muestran algunas posibles topologías.

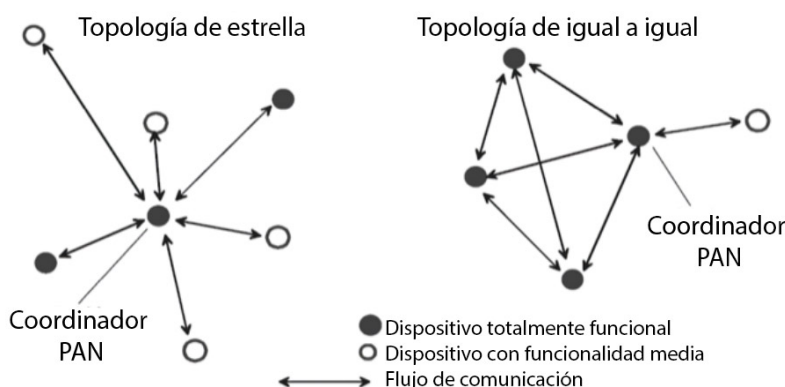


Figura 2: Topologías usadas en la MAC [3] .

Los dispositivos FFD se comunican entre sí y con los dispositivos RDF, mientras que los RDF solo se comunican con los FFD y lo hacen con uno solo a la vez. Por lo tanto, la red consiste en dispositivos

FFD que se encargan de realizar tareas de control de la red y los dispositivos RFD que se encargan de detectar y tomar los datos. Los dispositivos FFD determinan la manera en la que accederemos al canal, ya que dependiendo de el modo en el que estén operando es la forma en la que se accede al medio.

Para enviar los datos es necesario definir una unidad de envío de datos, es decir una trama. Las estructuras de la trama fueron en este caso diseñadas para mantener la simplicidad al máximo y no tener problemas con los canales ruidosos. Las tramas MAC se pasan a PHY como PSDU, que se convierte en la carga útil de PHY, el protocolo PHY unidad de datos (PPDU) se ilustra en la figura 2.

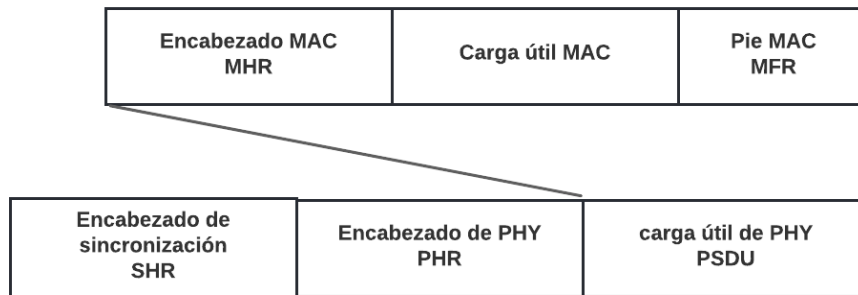


Figura 3: Vista esquemática del PPDU [3] .

Estos dispositivos son capaces de determinar dos maneras posibles para acceder al medio: El modo con balizas y el modo sin balizas.

Modo sin balizas:

Cuando la red se encuentra operando en este modo, la manera de acceder al canal es a través del algoritmo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), este algoritmo proporciona un acceso aleatorio al canal. Cuando un dispositivo quiere usar el canal para transmitir información, la red debe fijarse primero si no se encuentra otro dispositivo transmitiendo, en caso de ser así, el acceso al canal se debe realizar posteriormente hasta que éste se encuentre disponible. Este protocolo no busca detectar las colisiones sino que quiere evitarlas.

Para este algoritmo se necesita que los dispositivos estén activos constantemente, ya que cualquier sensor puede despertarse y mandar datos en cualquier momento.

Modo con balizas:

Cuando utilizamos el modo con balizas, la comunicación es facilitada por una estructura de supertrama (superframe) para facilitar y coordinar el acceso al canal. Cuando se opera en este modo, un coordinador PAN de la red transmite superframes de guías cada cierto intervalos de tiempos definidos. Estos intervalos pueden ser tan cortos como de unos 15 ms a tan largos como 50s. A continuación se muestra una imagen de ejemplo de lo que sería la estructura de un superframe:

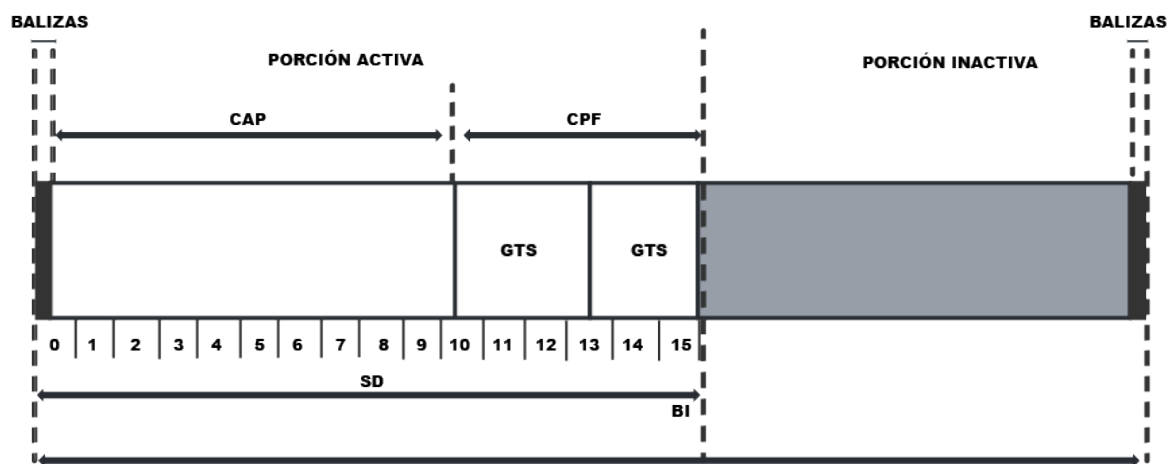


Figura 4: Ejemplo de estructura de un superframe [3].

Como vemos en la imagen, la estructura tiene una parte activa e inactiva. El coordinador y los nodos pueden comunicarse durante la parte activa y entran en modo de bajo consumo o apagado durante el periodo inactivo. Es en la parte inactiva en donde logramos reducir el consumo energético de los dispositivos, ventaja que mencionamos a favor del ZigBee. Para lograr esto, se debe adaptar el ciclo de trabajo y la longitud que se necesite para el período activo, cabe destacar que se maneja cierto compromiso al momento de manejar estos parámetros, ya que por ejemplo, si tomamos ciclos de trabajo muy largos con un largo período activo tendremos buen ancho de banda para los dispositivos, pero por otro lado el sistema estaría despierto por mucho tiempo aumentando el consumo energético. Los diferentes parámetros son ajustados según los requerimientos del sistema.

Ahora observemos con más detalles esta estructura, la duración del superframe queda determinada por el parámetro BI y el largo de la parte activa por el parámetro SD de la manera en la que se ve en la imagen.

La porción activa esta dividida en 16 slots de tiempos iguales, y dicha porción se reparte los slots en 3 secciones: una baliza, un período llamado CAP (Contention Access period) y otro llamado CFP (Contention Free Period). La baliza es transmitida por el coordinador al principio, son las balizas lo que determinan el inicio y final del superframe además de que los nodos los utilizan para sincronizarse. Luego le sigue el período CAP, en el cual se utiliza un enfoque CSMA/CA ranurado para los dispositivos que quieran acceder al canal.

Cuando se habla de un sistema CSMA/CA ranurado, significa que cada dispositivo puede consultar la disponibilidad del canal durante el inicio de una ranura de tiempo, en caso de encontrarse ocupado, el dispositivo se repliega un número aleatorio de ranuras. Si el dispositivo logra acceder en dicha ranura de tiempo, debe realizar su transmisión en el tiempo determinado.

Continuando con la estructura del superframe, vemos que en el período CFP usa el protocolo estándar de GTS (Guaranteed Time Slot), espacio asignado para los dispositivos que requieran exclusividad al momento de transmitir.

El protocolo GTS permite que los dispositivos soliciten al coordinador PAN un determinado conjunto de ranuras de tiempo. En caso de que el pedido sea aceptado, los dispositivos tienen la posibilidad de enviar sus paquetes en determinadas ranuras de tiempo dedicadas y libre de colisiones.

5.2. Capa física (PHY)

Las características de la capa física son la activación y desactivación del transceiver de radio, la detección de energía (ED), la indicación de calidad del enlace (LQI), la selección de canales, CCA, el rango y la transmisión, así como la recepción de paquetes a través del medio físico.

5.2. a. Espectro

En el estándar 802.15.4 se definen tres bandas operadoras:

- 868-868,8 MHz.
- 902-928 MHz.
- 2400-2483,5 MHz.

Una ilustración de la distribución del espectro se muestra en la figura 5.

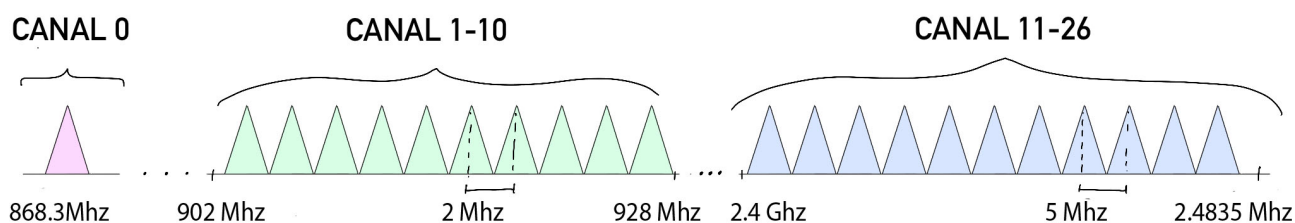


Figura 5: Partición del espectro

Técnicas de Modulación:

Hoy en día dentro del estándar se definen al rededor de 20 técnicas de modulación diferentes. En la versión de 2003, especifica dos niveles físicos basados en espectro ensanchado por secuencia directa (direct sequence spread spectrum, DSSS), esta técnica se basa en que la información a transmitir se mezcla con un patrón pseudoaleatorio de bits para extender los datos antes de que se transmitan [4]. Los dos niveles físicos basados en DSSS son los que posteriormente adopta ZigBee, estos son:

a) Modulación O-QPSK (Offset Quadrature Phase Shift Keying): consiste en realizar una transición de fase en cada intervalo de señalización de bits, por portadora en cuadratura [5].

b) Modulación BPSK (Binary Phase Shift Keying): se tiene como resultados posibles dos fases de salida para la portadora con una sola frecuencia. Una fase de salida representa un 1 lógico y la otra un 0 lógico.

5.2. b. Binary phase-shift keying (BPSK)

Descripción general:

El BPSK es un esquema de modulación de desplazamiento de fase de 2 símbolos. Un posible diagrama de modulación de referencia se muestra en la figura 5 para especificar las funciones de modulación y expansión BPSK PHY. Cada bit de la PPDU se va a procesar a través de la codificación diferencial, el mapeo de bit a chip y las funciones de modulación en orden de octetos.

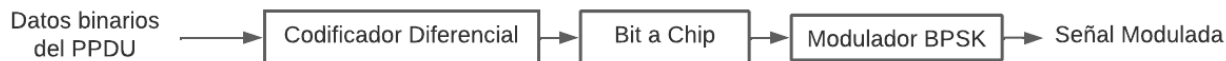


Figura 6: Modulador BPSK de referencia [3]

Mapeo Bit a Chip:

En esta modulación se usa el chip como convención del pulso para el método DSSS, cada bit de entrada se hará corresponder con una secuencia PN (pseudo-random noise) de 15 chips como se especifica en el cuadro de la figura 7.

Bits	Valores de los chips (c0 ... c14)
1	1 1 1 1 0 1 0 1 1 0 0 1 0 0 0
0	0 0 0 0 1 0 1 0 0 1 1 0 1 1 1

Figura 7: Mapeo de símbolo a chip [3]

Durante el tiempo de símbolo la forma en que se envía el PN es primero el chip 0 y por el último el chip 14. Las secuencias de chip se modulan en la portadora usando BPSK con forma de pulso de coseno alzado con un factor de roll-off = 1 donde un valor de chip de uno corresponde a un pulso positivo y un valor de chip de cero corresponde a un pulso negativo.

Espectro de la banda utilizada:

La modulación BPSK se utiliza en las bandas de:

$$\begin{cases} 868,0 - 868,8\text{MHz} \\ 902 - 928\text{MHz} \end{cases}$$

En la primera banda se usa un bit rate (r_b) de 20 kb/s y de 40 kb/s para la banda de 915 MHz. Como se mencionó anteriormente, los bit se hacen corresponder a una secuencia PN de 15 chips, por lo tanto esto nos lleva a tener un chip rate de 300 kchip/s y 600 kchip/s respectivamente. Es por esto que, la tasa de bits que tenemos que utilizar para hacer las cuentas que corresponden al ancho de banda es el chip rate, dado que en definitiva es la tasa de bits que ingresan y salen del modulador BPSK.

$$BW = (\text{Largo de la secuencia PN}) \cdot r_b(1 + \rho) = r_{chips}(1 + \rho)$$

Por lo tanto el ancho de banda para una tasa de 20kb/s es de 600kHz y para la tasa de 40kb/s un ancho de banda de 1.2MHz. Una magnitud que nos sirve para medir la robustez del sistema en recepción es la sensibilidad, en este caso por lo especificado anteriormente, un dispositivo compatible debe ser capaz de lograr una sensibilidad de -92 dBm o mejor y por otro lado deberá ser capaz de transmitir a un nivel de potencia de al menos -3 dB.

Forma del pulso:

La forma de pulso de coseno alzado (factor de roll-off = 1) utilizada para representar cada chip de banda base se describe como:

$$p(t) = \begin{cases} \frac{\sin(\pi/T_c) \cos(\pi/T_c)}{\pi/T_c \cdot 1-4t^2/T_c^2}, & \text{si } t \neq 0 \\ 1, & t = 0 \end{cases}$$

5.2. c. Offset QPSK

Offset QPSK (OQPSK) es la modulación utilizada por el estándar en la banda de 2.4GHz, es una variante de la modulación PSK tradicional. Para la modulación en QPSK tomamos dos bits a la vez para construir cada símbolo, esto permite que la fase de la señal pueda llegar a tener saltos de hasta 180. Al momento de filtrar la señal por un pasa bajos, estos saltos en frecuencia pueden llevar a grandes fluctuaciones en la amplitud, llevando a una baja en el rendimiento del sistema [5]. Lo que se hace para resolver este problema es agregar un período de bit, o medio período de símbolo a los bits pares e impares, de tal manera que las componentes en fase y cuadratura no van a cambiar ambas al mismo tiempo.

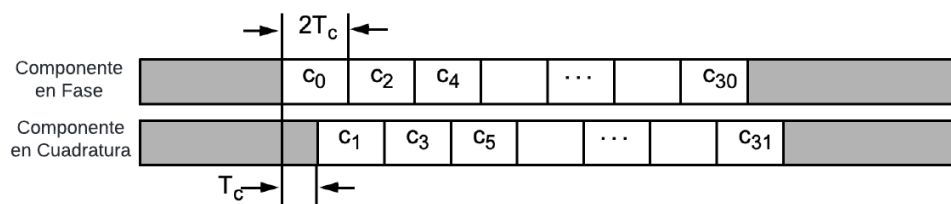


Figura 8: Diagrama representativo del desfase [3]

La capa física OPQSK emplea una técnica de modulación semi-ortogonal 16-aria, utilizando el método DSSS mencionado anteriormente. Un posible diagrama de modulación de referencia se muestra en la figura 8 para especificar las funciones de bit a símbolo y expansión OQPSK PHY [5].

Modulador de referencia:

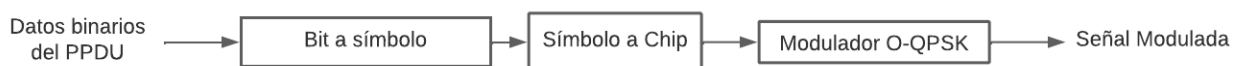


Figura 9: Modulador OQPSK de referencia [3]

Mapeo de bit a símbolo:

Toda la información binaria contenida en la PPDU, debe ser codificada de la forma en la que se observa en el modulador de referencia de la imagen anterior. Dicho mapeo de bit a símbolo consiste en ir tomando la información en bytes, para luego mapear los 4 bit menos significativos del byte en un símbolo y los 4 más significativos son mapeados al símbolo siguiente.

Mapeo de símbolo a chip:

Cada símbolo será mapeado en una secuencia PN de 32 chips, tal como se especifica en la siguiente tabla. Cada secuencia esta relacionada entre sí, mediante cambios cíclicos y/o conjugación (o sea, invertir valores de chips en posiciones impares). Cabe destacar que hay otros mapeos según la banda en la que se trabaje.

Símbolo	Valor de los chips (c0,c1,...c30,c31)
0	11011001110000110101001000101110
1	11101101100111000011010100100010
2	00101110110110011100001101010010
3	00100010111011011001110000110101
4	01010010001011101101100111000011
5	00110101001000101110110110011100
6	11000011010100100010111011011001
7	10011100001101010010001011101101
8	10001100100101100000011101111011
9	10111000110010010110000001110111
10	01111011100011001001011000000111
11	01110111101110001100100101100000
12	00000111011110111000110010010110
13	01100000011101111011100011001001
14	10010110000001110111101110001100
15	11001001011000000111011110111000

Figura 10: Mapeo de símbolo a chip para la banda de 2.4GHz [3]

Espectro de la banda utilizada:

Si hablamos de tasas de datos, esta modulación logra una tasa de datos de 250kb/s en la banda de 2.4GHz. Como se mencionó anteriormente, los bits antes de ser mapeados a chips se mapean a símbolos de 4 bits por lo tanto podemos decir que un primer symbol rate lo calculamos como

$$r_s = \frac{r_b}{4} = 62,5k_{sym}/s$$

Por lo tanto si usamos una secuencia PN de 32 bits, vamos a tener una tasa de chips de

$$r_{chip} = 32.(62,5 \times 10^3) = 2MHz$$

Teniendo esta tasa de chip, si queremos calcular la tasa de símbolos a la salida del modulador OQPSK, lo hacemos usando la fórmula:

$$r_s = \frac{r_{chips}}{\log_2(4)} = 1MHz$$

Entonces, el ancho de banda para un $\rho = 1$ es:

$$BW = r_s(1 + \rho) = 2MHz$$

En este caso un dispositivo compatible debe ser capaz de lograr una sensibilidad de -85 dBm o mejor y por otro lado deberá ser capaz de transmitir a un nivel de potencia de al menos -3 dB. En cada caso, los mejores artículos deben de ser del orden de 10 dB mejores que las especificaciones.

Forma del pulso:

La forma del pulso es la de medio seno, utilizada para representar cada chip en banda base y es el siguiente:

$$p(t) = \begin{cases} \sin(\pi \frac{t}{2T_c}), & 0 \leq t \leq 2T_c \\ 0, & \text{en otro caso} \end{cases}$$

Este pulso es utilizado en la banda de 2.4GHz, 915MHz y 868MHz. Para la banda de 780 MHz, se utiliza el mismo pulso que en modulación BPSK, a excepción de utilizar un factor de roll-off $r = 0,8$. Dada la secuencia en tiempo discreto de muestras de chips complejos consecutivas c_k , en tiempo continuo la señal de banda base compleja conformada con el pulso es la siguiente:

$$y(t) = \sum_{k=-\infty}^{\infty} c_{2k}p(t - 2kT_c) + jc_{2k+1}p(t - 2kT_c - T_c)$$

6. Puesta en escena del ZigBee en GNU Radio

Para esta parte utilizamos un módulo en GNU Radio que dejó disponible Bastian Bloessl en su repositorio de github con un ejemplo de un flowgraph de un transceiver dónde se puede ver implementada la capa física y MAC del estándar [6].

6.1. Transmisor:

En primera instancia podemos ver en el diagrama la secuencia de bloques dónde se arma, con el mensaje a mandar, el PPDU. Como se puede ver en la figura 11 el bloque Pad Source lo que hace es traer de otro archivo los valores a enviar, el bloque Access Code Prefixer le agrega el SHR y el PHR antes mencionado y el bloque PDU to Tagged Stream convierte los PPDU's a flujos de datos.

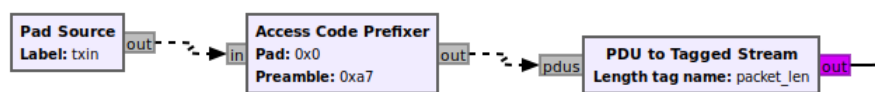


Figura 11: Proceso para la creación del PPDU y conversión a flujo.[6]

Una vez que tenemos el flujo de datos, pasamos a tomar símbolos de 4 bits con el bloque Packed to Unpacked, para luego mapearlos a un chip y luego a símbolo OQPSK. En esta implementación se hace el mapeo de símbolo a chip y a símbolo OQPSK en un solo bloque llamado Chunks to Symbols. Luego se conforma con el pulso el cual está definido por sus taps en el bloque Vector Source.

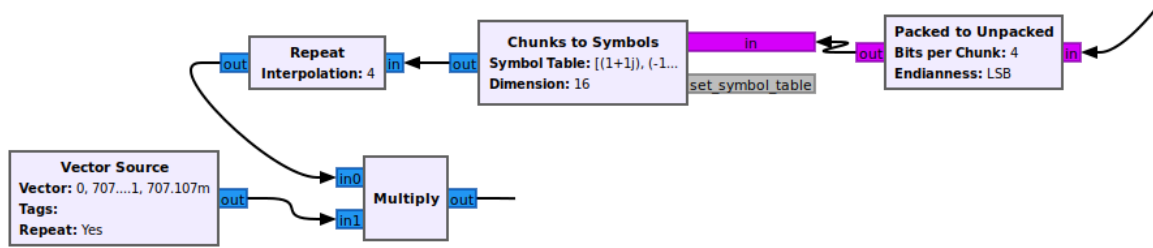


Figura 12: Proceso de modulación de la PPDU. [6]

Por último, antes de la transmisión, lo que se hace es agregarle un delay a la componente en cuadratura, de tal manera de evitar cambios al mismo tiempo entre las componentes de fase y cuadratura.

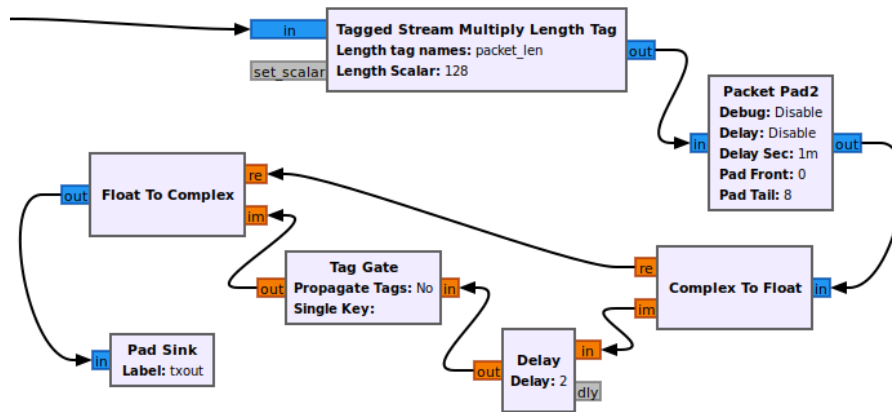


Figura 13: Desfase entre fase y cuadratura. [6]

6.2. Receptor:

Para la parte del receptor se necesita demodular la señal que viene modulada en cuadratura con el bloque Quadrature Demod, luego se resta la señal demodulada con la señal demodulada pasada por un filtro IIR de un polo. El bloque Clock Recovery MM usa una de corrección de errores temporales con la técnica de Muller-Miller, para luego ser empaquetado y enviado en los últimos dos bloques.

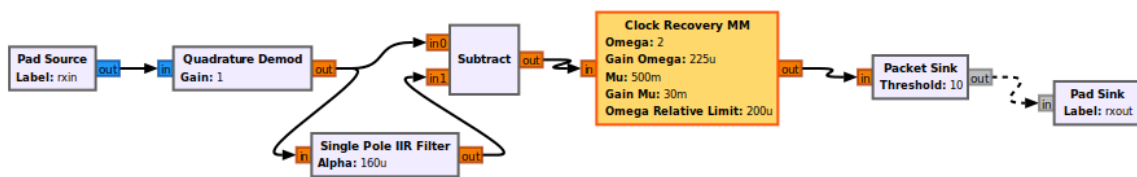


Figura 14: Desfase entre fase y cuadratura. [6]

Referencias

- [1] Zigbee Alliance. *ZigBee Specification (2005-2017)*. URL: <https://csa-iot.org/all-solutions/zigbee/>.
- [2] Eric Blossom. *GNU Radio*. URL: <https://www.gnuradio.org/>.
- [3] IEEE 802.15.4. *IEEE Standard for Low-Rate Wireless Networks(2020)*. URL: <https://standards.ieee.org/ieee/802.15.4/7029/>.
- [4] Simon Haykin. “Direct-Sequence Spread Spectrum with Coherent Binary Phase-Shift Keying”. En: *Communication Systems 4th Edition* (2000), pág. 490.
- [5] John G. Proakis. “Offset QPSK (OQPSK)”. En: *Digital Communications Fifth Edition* (2008), pág. 124.
- [6] Bastian Bloessl. En: *IEEE802.15.4 O-QPSK transceiver for GNU Radio* (19 Jul 2021). URL: <https://github.com/bastibl/gr-ieee802-15-4>.