Comunicaciones Inalámbricas Bluetooth®

Diana Franco
Francisco Castillo
Facultad de Ingeniería Eléctrica
Universidad Tecnológica de Panamá

Resumen - *Bluetooth define un modelo completo, tanto hardware como software, de comunicación inalámbrica de baja potencia, bajo la utilizando señales de radio en la banda de frecuencias ISM (Industrial, Científica, Médica), alrededor de los 2.4 GHz. Esta tecnología hace posible la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia en distancias cortas. Uno de los objetivos de esta tecnología es la posibilidad de reemplazar o eliminar la gran cantidad de cables y conectores que enlazan unos dispositivos con otros. Además esta tecnología pretende facilitar la interacción y sincronización de los diferentes dispositivos tanto móviles como fijos que se desee, todo ello sin necesidad de estar directamente colocados uno al lado del otro.*

Palabras Claves - Modulación *bluetooth*, pila de protocolos bluetooth, seguridad de la tecnología bluetooth.

1. Introducción Bluetooth®

Bluetooth tuvo su origen en Lund, Suecia en febrero de 1994 por iniciativa de dos empleados de Ericsson Mobile Communications, el sueco Sven Mattisson y el holandés Jaap Haartsen, que junto con otros cuatro promotores de telecomunicaciones (Nokia, IBM, Toshiba e Intel) formaron el SIG *(Special Interest Group)*. Su propósito era establecer un software que controlara un modelo universal para la interfaz radioeléctrica y que se pudiera aplicar entre distintos dispositivos de diferentes fabricantes.

El nombre *bluetooth* proviene del rey cristiano escandinavo Harald II apodado "Blåtand o diente azul" (bluetooth) que reinó sobre Dinamarca y Noruega en el siglo X y que unificó varios pueblos y reinos (noruegos, suecos y daneses) [1]. Esta relación se dio ya que de la misma manera, *bluetooth* desea enlazar diferentes tecnologías como las de los ordenadores, los teléfonos móviles y el resto de periféricos [2]

Las características principales de esta tecnología son: fiabilidad, bajo consumo, mínimo coste y comprende hardware y software desarrollado por el SIG *(Special Interest Group)* y principales fabricantes de los sectores de las telecomunicaciones y la informática.

Actualmente el SIG está compuesto por nueve compañías: 3Com/Palm, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia y Toshiba, y es apoyado por más de 2000 empresas de tecnología.

2. Protocolos Bluetooth®

Para garantizar una buena comunicación entre el receptor y el transmisor ambos deben estar sobre la misma pila de protocolos. La pila se compone por dos clases de protocolos: protocolos específicos, que implementan los protocolos propios de la tecnología *bluetooth*; y protocolos no específicos, que están constituidos por el conjunto de protocolos adoptados a otras especificaciones.

Este diseño de la pila de protocolos *bluetooth* permite aprovechar grandes ventajas de cada una de las clases. La primera clase permite utilizar los beneficios propios de la tecnología *bluetooth,* mientras la segunda clase brinda la ventaja de interactuar con cualquier clase de protocolos comerciales existentes; por otro lado ofrece el beneficio de que *bluetooth* no quede restringido a nuevas implementaciones libres o nuevos protocolos de aplicación de uso común. La pila de protocolos se muestra en la Figura 1.

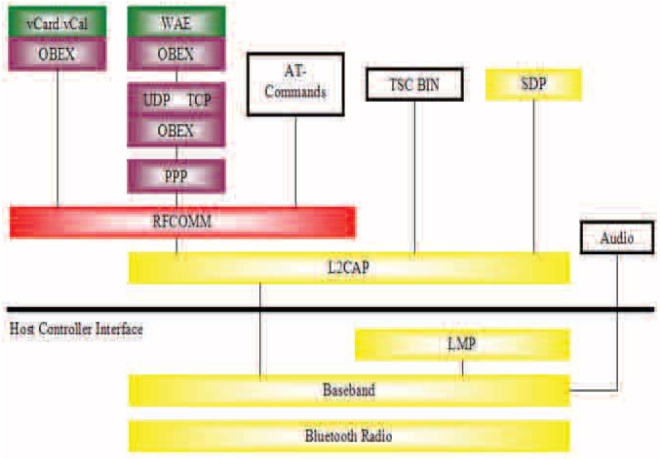

Figura 1. Pila de Protocolos [5]

La pila se puede dividir en cuatro capas lógicas:
- Núcleo de *Bluetooth*: Radio, Banda Base, LMP, L2CAP, SDP.
- Sustitución de cable: RFCOMM.
- Protocolos adoptados: PPP, UDP, TCP, IP, OBEX, WAP, IRMC, WAE.
- Control de telefonía: TCS-binary, AT-Commands [1].

3. Núcleo de Bluetooth®

El núcleo del sistema *bluetooth* consiste en un transmisor de radio, una banda base y una pila de protocolos. El sistema permite la conexión entre dispositivos y el intercambio de distintos tipos de datos entre ellos.

Radio (RF)

Para poder trabajar en un ambiente de muchas interferencias (LANs, mandos, hornos microondas), *bluetooth* utiliza un esquema de reconocimiento rápido y saltos de frecuencia (saltos cada 645 µs [3]) para garantizar la potencia del enlace [1].

Utilizando la técnica FHSS *(Frequency Hopping Spread Spectrum)* los datos son divididos en paquetes de información, que son enviados a través de varias frecuencias, esto es conocido como "Hopping Pattern". El propósito de enviar la información por varias frecuencias es cuestión de seguridad y confiabilidad. Para llevar a cabo la transmisión de datos es necesario que tanto el transmisor como el receptor coordinen este denominado "Hopping Pattern"[4].

Este sistema opera para banda ISM, con canales RF de: f= 2402 + n MHz siendo n = 0.78 (79 canales).
En la Tabla 1 se muestra los parámetros de frecuencias utilizados en diferentes países junto a sus canales correspondientes.

Tabla 1. Radio Frecuencias Bluetooth.

Área	Banda de frecuencias (GHz)	Canales Bluetooth
USA	2.400-2.483,5	79
Europa	2.400-2.483,5	79
España	2.445-2.475	23
Francia	2.446,5-2.483,5	23
Japón	2.471-2.497	23

El espacio entre canales es de 1 MHz; sin embargo, es necesario tener márgenes de protección respecto al ancho de banda, por lo que el límite inferior de protección es de 2 MHz y el límite superior es de 3.5 MHz.

La distancia del enlace está comprendida entre 10 cm y 10 m. El consumo es 300 µA (máximo), 30 µA (standby), y aproximadamente -50 µA (hold/park).

Modulación Bluetooth

La modulación que emplea *bluetooth* es GFSK *(Gaussian Frequency Shift Keying/* modulación por desplazamiento de frecuencia con filtrado gaussiano) con un producto ancho de banda por tiempo *BT*= 0.5.

Este tipo de modulación permite un bajo coste y alcanza tasas de transmisión de 1Mbps. El índice de modulación debe estar entre 0.28 y 0.35. Un "1" binario se representa por una desviación positiva de frecuencia y un "0" binario como una desviación negativa. La desviación mínima no ha de ser menor de 115 kHz.

En el dispositivo receptor bluetooth el nivel de sensibilidad es el aspecto más importante. Para lograr la medición de una tasa de error de bit, el dispositivo receptor envía de vuelta la información decodificada. Para una tasa de error o BER (Bit Error Rate) del 0.1% se define el nivel de sensibilidad de un receptor *bluetooth* mayor o igual a –70dBm.

Banda Base Bluetooth

Banda base es la capa física del diseño de *bluetooth*. Esta define los canales físicos y los enlaces, aparte de otros servicios tales como información de conexión, errores de conexión, selección de canales y seguridad. Un canal *bluetooth* está representado por una secuencia de saltos pseudo aleatorios a través de los 79 o 23 canales RF. Dos o más dispositivos *bluetooth* que usan el mismo canal forman una *picored o piconet*, como se muestra en la Figura 2.

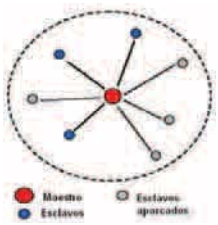

Figura 2. Picored o piconet [1].

El maestro es el responsable de la sincronización entre los dispositivos de la picored, su reloj y saltos de frecuencia controlan al resto de los dispositivos. El maestro lleva a cabo el procedimiento de búsqueda y establecimiento de la conexión de manera predeterminada. Los esclavos simplemente se sincronizan y siguen la secuencia de saltos determinada por el maestro.

La topología *bluetooth* permite la interconexión de varias piconets formando una "scatternet" (ver figura 3). Un dispositivo puede pertenecer a varias piconets haciendo uso de la demultiplexación por división del tiempo (TDD), el dispositivo solo está activo en una piconet a la vez ya que no existe sincronización entre ellas.

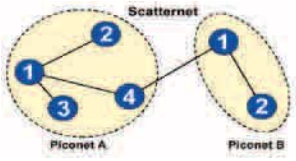

Figura 3. Scatternet, 1 (maestro), 2,3,4 (esclavos)[5].

El canal está dividido en ranuras de tiempo *(timeslots o slots)*, cada ranura corresponde a una frecuencia de salto y tiene una longitud de 625 µs. Cada secuencia de salto en una piconet está determinada por la dirección del maestro (48 bits). Todos los dispositivos conectados a la piconet están sincronizados con el canal en salto y tiempo. Durante la transmisión de un paquete la frecuencia es fija, cada paquete debe estar alineado con el inicio de una ranura y puede tener una duración de hasta cinco ranuras. Para evitar fallos en la transmisión *(crosstalk)*, el maestro inicia enviando en las ranuras pares y los esclavos en las ranuras impares como se muestra en la siguiente figura [1].

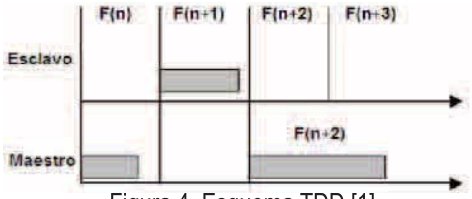

Figura 4. Esquema TDD [1].

El nivel de banda base maneja dos tipos de enlaces: SCO *(Synchronous Connection-Oriented)* y ACL *(Asynchronous Connection-Less)* [5].

Pila de protocolos

El LMP *(Link Manager Protocol)* controla activamente el establecimiento de comunicación, autenticación y configuración del enlace.

El L2CAP *(Logical link control and adaptation layer protocol)* está situado sobre el protocolo de banda base, en la capa de enlace de datos. Éste realiza la segmentación y la unificación de los datos de las aplicaciones y la multiplexación y demultiplexación de varios canales a través de un enlace lógico compartido. Permite a las capas superiores enviar y recibir paquetes de datos L2CAP de hasta 64KB. Esta especificación está definida únicamente para enlaces ACL.

El SDP (Protocolo de descubrimiento de servicio) provee un conjunto de aplicaciones cuyo objetivo es descubrir servicios que están disponibles y determinar las características de los mismos.

En el entorno *bluetooth* se necesita un protocolo específico de este tipo, ya que los servicios disponibles cambian dinámicamente basándose en la cercanía radioeléctrica de los dispositivos en movimiento, cualitativamente diferentes a los servicios de descubrimiento de las redes convencionales. Por esto, el SDP definido para bluetooth debe estar enfocado a las características únicas del entorno bluetooth.

El protocolo RFCOMM proporciona emulación de puertos serie sobre el protocolo L2CAP. Está basado en el estándar ETSI TS 07.10.

5. Formato de paquetes Bluetooth®

Los datos transmitidos a través de un canal son fragmentados y enviados en paquetes.

La información se encuentra protegida mediante códigos detectores y/o correctores de errores. En cada ranura sólo se puede enviar un paquete. El receptor los recibirá y los procesará empezando por el bit menos significativo.

Los paquetes son clasificados en diferentes tipos atendiendo al número de ranuras que ocupan y dependiendo de sus enlaces:

Enlaces asíncronos: La tasa de transmisión máxima que se logra es aproximadamente 723 kbps. El campo de datos es de longitud variable. Hay tres tipos de paquetes según el número de ranuras: 1, 3 o 5 ranuras.

Enlaces síncronos: El campo de datos del usuario es fijo. Este tipo de enlaces soporta *full-duplex* con unas tasas de transmisión mucho menores que en el caso de los enlaces asíncronos, aproximadamente 64 kbps en los dos sentidos. Sólo hay paquetes que caben en 1 ranura.

Las multiranuras son paquetes que ocupan 3 o 5 ranuras. Estos no utilizan saltos de frecuencia. Todas las ranuras que ocupe el paquete se envían por la misma frecuencia. Al finalizar la transmisión se cambia la frecuencia.

6. Conceptos generales, arquitectura de red y seguridad

De los conceptos generales del *bluetooth* se puede decir que es una tecnología inalámbrica que tiene dos rangos de cobertura o distancia a la que se puede transmitir datos.

Las coberturas son: las de corta distancia que tiene un pequeño alcance de 10m, y la cobertura de largo alcance que puede abarcar un radio de longitud de 100 m. Este enlace radio es capaz de enviar voz y datos a una velocidad de aproximadamente unos 720 kbps.

La tecnología *bluetooth* puede llevar a cabo dos tipos de transmisiones, para cada una de estas transmisiones se tienen las características siguientes:

Voz: La tecnología *bluetooth* ofrece la posibilidad de poder usar tres canales simultáneos síncronos de voz, o también la posibilidad de compartir un solo canal para el transporte simultáneo de datos asíncronos y voz síncrona. Cada canal de voz soporta un canal síncrono a 64 kbps, en tanto para el enlace de subida como para el de bajada.

Datos: El canal de transporte de datos asíncronos es capaz de soportar tasas de hasta 723.2 kbps en modo asimétrico, mientras que en transmisión simétrica otorga tasas de transmisión de hasta 433.9 kbps. Por otra parte, un dispositivo que realice el rol de maestro, puede compartir de manera simultánea un canal asíncrono con 7 dispositivos esclavos en la misma picored.

La arquitectura de red considera que los dispositivos *bluetooth* que estén dentro del límite de cobertura de otros dispositivos *bluetooth* pueden ser configurados logrando así formar redes *ad hoc* punto a punto o bien redes que establezcan conexiones punto a multipunto.

La especificación actual de *bluetooth* permite la comunicación simultánea de 7 esclavos activos con un maestro. Además, puede haber un número ilimitado de dispositivos bajo la gestión del maestro, preparados para iniciar una comunicación, si así lo requieren.

El proceso de seguridad de *bluetooth* consta de tres pasos:

Autenticación: Se basa en un proceso *challenge-response*, previene problemas de alteración de origen de mensajes y acceso no permitido a bases de datos críticas.

Cifrados: Previene el problema de intercepción de los datos que circulen por el canal, manteniendo la privacidad del enlace.

Generación de clave de sesión: Dichas claves pueden ser cambiadas durante una conexión, lo que hace imposible que alguien intercepte una conversación.

Los elementos utilizados en los algoritmos de seguridad son:

- La dirección del dispositivo bluetooth, formado por 48 bits, que es una entidad pública única para cada dispositivo.
- Una clave privada de usuario de 128 bits, la cual es secreta. Esta clave se obtiene durante la inicialización del dispositivo.
- Un número aleatorio de 128 bits, el cual será diferente para cada nueva transacción.

7. Discusión final

La tecnología inalámbrica *bluetooth* es importante a la hora de comunicar dispositivos a corto alcance de forma cómoda y sin cables, ya que ésta se trata de un estándar inalámbrico disponible en todo el mundo que conecta entre sí teléfonos móviles, ordenadores portátiles, manos libres para el automóvil, reproductores de MP3 y muchos dispositivos más.

La tecnología *bluetooth* funciona en la banda de 2.4 GHz, una de las bandas de radio industrial, científica y médica que no requiere licencia, por tanto, no existen gastos asociados al uso de la tecnología *bluetooth.*

El estándar *bluetooth* es una tecnología ad hoc, lo que significa que no se necesita una infraestructura fija y es sencilla de instalar y configurar.

La seguridad es uno de los aspectos en el cual la tecnología *bluetooth* se ha diseñado. Cuando los usuarios *bluetooth* se identifican y conectan entre sí por primera vez, se utiliza el código PIN para garantizar una conexión segura en todo momento.

Referencias

[1] J. Trujillo, Amplificadores de RF para topologías LAN inalámbricas–bluetooth, http://www.electronicafacil.net/tutoriales/tutorial109.html, [consultado 12 de octubre de 2007].

[2] CARREFOUR, Tecnología inalámbrica Bluetooth,http://www.carrefour.es/clubcarrefour/especiales/electrocasion/bluetooth.html, [consultado 12 de octubre de 2007].

[3] J. Capella, Redes de área local Bluetooth, www.redes.upv.es/ralfi/ficheros/presentaciones/07%20Inalambricas%20Bluetooth.pdf, [consultado 23 de junio de 200].

[4] OL, FHSS ("Frequency Hopping Spread Spectrum"), http://www.osmosislatina.com/conectividad/bluetooth.htm, [consultado 1 de junio de 2007].

[5] J. Arbona, Bluetooth, http://usuarios.lycos.es/XESC2000/Projectes/2494, [consultado 1 de junio de 2007].

[6] M. Miller, Discovering Bluetooth, Sybex Inc, USA, 2001.

[7] W. Stallings, Wireless communications & networks, Upper Saddle River, NJ: Pearson Prentice Hall, 2005.

[8] R. Morrow, Bluetooth: Operation and Use, McGraw-Hill Professional, USA, 2002.