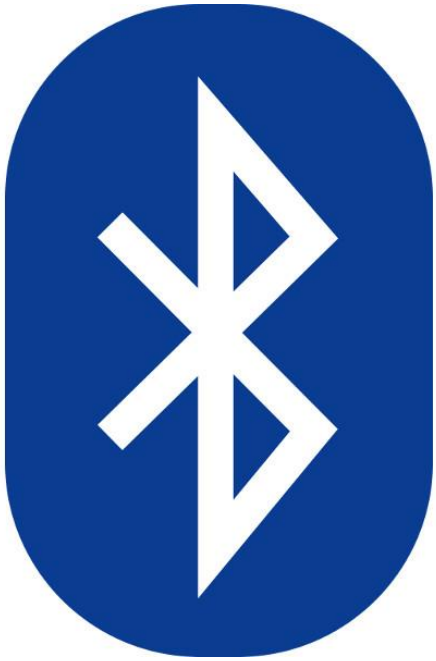
DEPARTAMENTO DE ELECTRONICA

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

ELO322: Redes de Computadores I

“bluetooth”



Gabriela González Moreno	201421053-1
Fabián López Peña	201421043-4
Aníbal Weippert Martínez	201421030-2

13/08/18

I. Resumen

Vivimos en una época donde las tecnologías de la información forman parte de nuestras vidas cotidianas, y cada vez toman más importancia. Sin embargo, la mayoría de las personas desconoce cómo estas tecnologías funcionan e interactúan entre sí. En cambio, quienes las entienden y las desarrollan pueden influir en cómo cambia nuestro mundo.

En ese contexto un tema importante es el entender que son las redes de computadores y como se crean. Una tecnología de particular interés para nosotros asociado a las redes de computadoras, es la tecnología Bluetooth que permite crear pequeñas redes para uso personal.

En el presente trabajo, se explica qué es Bluetooth, como funciona, y se mencionan algunos temas asociados, como la pila de protocolos de Bluetooth, explicando las principales capas dentro del protocolo, tales como LMP, L2CAP, SDP, RFCOMM y OBEX.

Se finaliza mostrando una transmisión típica de datos por Bluetooth con la ayuda de Wireshark, observando un seguimiento del envío de paquetes de datos para probar su funcionamiento.

II. Introducción

Una de las grandes problemáticas humanas de hoy en día es vivir en la ignorancia de lo que nos rodea ya que estamos viviendo la cotidianidad de nuestros días sumergidos en un mundo tecnológico y la mayoría de las personas que usan esta tecnología son ignorantes frente al tema del funcionamiento a nivel hardware como software de cada una de ellas. Por esta razón, nos sentimos motivados para tratar de entender y explicar de manera simple y lo más genéricamente posible una de las principales tecnologías utilizadas en la actualidad, la cual es Bluetooth.

III.¿Qué es Bluetooth?

Es una interfaz universal que nos permite la conexión de forma inalámbrica de una serie de dispositivos electrónicos, para crear Redes Inalámbricas de Área Personal (WPAN), y realizar la transmisión de datos y voz entre los dispositivos. Esta tecnología opera entre las capas de enlace y físicas.

La transmisión de voz y datos se realiza mediante enlaces de radiofrecuencia entorno a la banda de los 2,4 Ghz. Es una tecnología de corto alcance que posee 4 niveles de potencia:

	Clase 1	Clase 2	Clase 3	Clase 4
Consumo [mW]	100	2.5	1	0.5
Rango [m]	<=100	<=20	<=1	<=0.5

Tabla 1 Rangos y consumos de cada clase

Entre menos sea la potencia usada, menor será el alcance. Generalmente los dispositivos que usamos a diario, son de clase 3 ó 4.

IV.¿Cómo funciona Bluetooth?

El primer paso para comprender el funcionamiento de éste, es entender el funcionamiento en la capa física. Tal como se mencionó previamente este protocolo funciona entre los 2.4 y 2.484 GHz, perteneciente a la banda ISM (industrial, scientific and medical). Esta se divide en 79 canales de 1 MHz utilizando una modulación GFSK (Gaussian Frequency Shift Keying, ver figura 1).

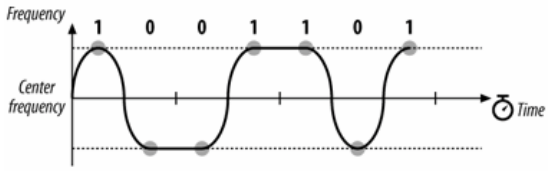


Figura 1 Esquema modulación GFSK

Después del envío de cada paquete de datos, ambos dispositivos cambian a una frecuencia de forma pseudo aleatoria y coordinada mediante la técnica de espectro expandido por salto de frecuencia (FHSS) generando una mayor seguridad y resistencia al ruido e interferencia. El canal de transmisión se divide en unidades llamadas *"slots"* que son intervalos de 625 ms. Normalmente se realiza un salto de frecuencia por paquete, que puede ser de 1, 3 o 5 slots.

En una red Bluetooth se pueden encontrar dos tipos de dispositivos: maestros y esclavos. El primero de éstos se encarga de establecer la secuencia de frecuencias que se utilizaran en la transmisión (FHSS), actuando como una especie de director de orquesta de los dispositivos esclavos conectados a éste, que se encargan de sincronizarse en tiempo y frecuencia con el maestro para seguir los saltos de frecuencia que éste realiza.

Las redes Bluetooth son catalogadas de dos formas: Piconet y Scatternets:

- Piconet: Grupo de esclavos conectados a un maestro, tal como se ve en la figura 1.2. El máximo de esclavos posibles bajo esta estructura es de 7.
- Scatternet: Grupo de piconets conectadas entre si mediante alguno de sus dispositivos que están presentes en ambas redes, ver en figura 2.

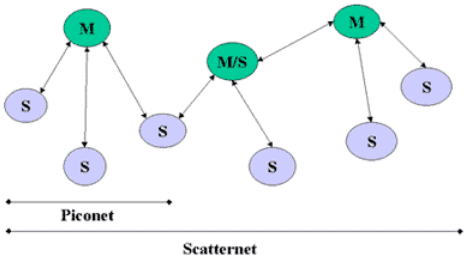


Figura 2 Piconet y Scatternet

V. Pila de protocolo Bluetooth

La pila de protocolos de Bluetooth se puede dividir en dos componentes, el host y el controlador Bluetooth (o módulo radio):

- El host también es conocido como la capa alta de la pila de protocolos y normalmente está implementado en software. Generalmente se encuentra integrado con el software del sistema o sistema operativo del dispositivo. Los perfiles están construidos por encima de los protocolos, generalmente en software.
- El módulo radio o controlador de Bluetooth normalmente es un módulo hardware, como podría ser una PC card conectada al dispositivo en cuestión, aunque lo normal es que éste módulo vaya ya integrado en el hardware del dispositivo.

Los datos en la pila fluyen a través de todas las capas a excepción de la información de audio, que va directamente desde la banda base hacia la aplicación con alto grado de prioridad, para garantizar la calidad de servicio en tiempo real, esperada en aplicaciones de audio.

En la figura 3, se muestra cómo se estructura la pila de protocolo Bluetooth.

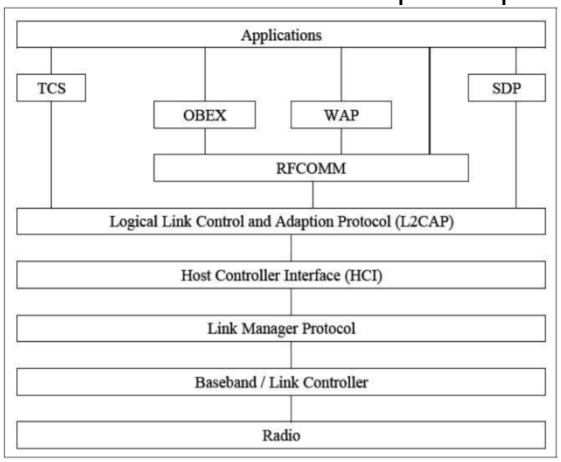


Figura 3 Pila de protocolos de Bluetooth

Breve explicación de las principales protocolos usados:

RFCOMM: Este protocolo es un conjunto simple de protocolos de transporte. Suministra una interfaz serial sobre L2CAP proporcionando el mecanismo de transporte a servicios de capas más altas, permitiendo realizar múltiples conexiones con un dispositivo al mismo tiempo.

Protocolo de adaptación y enlace lógico (L2CAP): Distribuye y acondiciona el tamaño de paquetes para las capas altas. También permite el control de flujo por canal y la retransmisión.

Protocolo Manejador de enlace (LMP): Se responsabiliza del establecimiento y configuración del enlace entre los dispositivos, gestionando y negociando el tamaño de los paquetes de banda base, también se encarga de los aspectos de seguridad, como la autenticación y encriptado.

Protocolo de descubrimiento de servicio (SDP): Provee un conjunto de aplicaciones cuyo objetivo es descubrir servicios que están disponibles en su entorno 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. Por esto, el SDP definido para Bluetooth debe estar enfocado a las características únicas del entorno Bluetooth.

Protocolo OBEX: Su objetivo es permitir el intercambio de objetos de datos entre dispositivos.

El protocolo Obex proporciona:

- Un modelo para la representación de los objetos.
- Un protocolo de sesión, que estructura el diálogo entre 2 dispositivos.

Modelo para la representación de los objetos: Los objetos son representados mediante una secuencia de headers.(Se puede ver como son en la figura 4 del anexo) .
Cada header se compone de 2 partes, Header ID y VALUE.
Header ID: Describe lo que el header contiene y como se formatea y Value: Describe el sentido especificado por el header ID.

Protocolo de sesión:

- Obex sigue el paradigma cliente/servidor de petición-respuesta para el formato de la conversación. Las operaciones OBEX están formadas por pares de petición- respuesta: Después de enviar una petición, el cliente espera una respuesta del servidor antes de emitir una nueva petición.
- Las operaciones OBEX son:

Connect: Antes de transmitir un objeto es necesario establecer una conexión, la sesión se inicia mediante el envío de una petición de conexión Connect.
Disconnect: Se produce si se cierra la aplicación o la aplicación quiere cambiar el equipo al que se envían las peticiones.
Put: Se utiliza para enviar un objeto OBEX
Get: Se utiliza para obtener un objeto OBEX
SetPath: Se utiliza para establecer la "carpeta actual" en el lado receptor en el caso que la transferencia requiere información adicional sobre las carpetas.
Abort: Se utiliza cuando el cliente decide poner fin a una operación de múltiples paquetes antes de su fin natural.

Resultados de la parte práctica

Se procedió a activar la opción "Registro de Búsqueda de Bluetooth" que aparece en configuraciones del celular para sistemas Android, el cual almacena la captura de todos los paquetes de HCI Bluetooth al momento de activar Bluetooth en un archivo .log.
Se envió desde una Laptop un mensaje de texto al celular y luego se desactivó la opción "Registro de Búsqueda de Bluetooth" para que dejara de almacenar paquetes. Una vez hecho esto, se envió el archivo .log a un computador para su posterior análisis.

Una vez obtenido el archivo en un computador, se abrió el archivo con WireShark, el cual nos mostró el tráfico de los paquetes intercambiados entre el celular y la laptop.
El block de notas enviado decía "Hola mundo" tal como indica la figura 5 del anexo.
Gracias a esto logramos analizar el tráfico de datos que hubo entre el Laptop y el celular. En la figura 6 adjunta en el anexo, se puede ver una imagen de Wireshark, que muestra claramente cómo recibió el texto el celular, a través del protocolo Obex, en el cual se muestra en la parte inferior de la misma figura el desglose de los headers que contienen el nombre, tipo, largo y cuerpo del archivo transmitido.
Además, se muestra en la figura 7 adjunta en el anexo, las operaciones OBEX usadas para esta transmisión, para mostrar claramente cómo funciona el protocolo a través de Wireshark.

Conclusiones

En este trabajo se ha abordado de forma superficial la tecnología Bluetooth, mencionando los aspectos más importantes del funcionamiento de la misma, de los cuales podemos destacar algunos puntos:
-Al hacer uso de la técnica de espectro ensanchado por salto de frecuencia(FHSS), se permite que la información que se transmite sea altamente inmune a ruidos e interferencias, a la vez que agrega seguridad al ser difícil de interceptar, y se permite además compartir el ancho de banda en que se transmite
-Aunque una piconet tiene un número de dispositivos limitados, se pueden conectar distintas piconets para crear scatternet, y de esta forma crear redes más grandes conectadas mediante Bluetooth.
- Bluetooth trabaja con un conjunto de protocolos, entre ellos unos de los más destacados es el protocolo OBEX que se encarga del intercambio de objetos entre dispositivos.
Por esta razón, la demostración fue basada en comprobar ciertas características del protocolo OBEX, que nos ayudaron a entenderlo mejor.
Luego de investigar mejor esta tecnología, podemos entender porqué se ha masificado tanto en los últimos años, pues aparte de eliminar los cables, tiene numerosas ventajas, como bajo consumo de energía, es gratuita y mundialmente disponible. Pero también muchos aspectos pueden ser mejorados, por lo que esta tecnología está en constante desarrollo, potenciando así el uso de las redes inalámbricas de área personal (WPAN).

Referencias

- *https://es.wikipedia.org/wiki/Bluetooth_(especificación)*
- *http://bibing.us.es/proyectos/abreproy/11972/fichero/Cap%C3%ADtulo+2+-+Bluetooth.pdf*
- *http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/archundia_p_fm/capitulo3.pdf*
- *https://www.electronicafacil.net/tutoriales/Banda-Base-dispositivos-Bluetooth.php*
- *https://es.scribd.com/document/55536220/Introduccion-al-protocolo-OBEX*
- *https://dialnet.unirioja.es/descarga/articulo/4844849.pdf*
- *http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/mayoral_p_e/capitulo4.pdf*
- *https://blog.330ohms.com/2017/02/02/bluetooth-clases-y-versiones-desde-v1-0-hasta-v5-0/*

Anexos

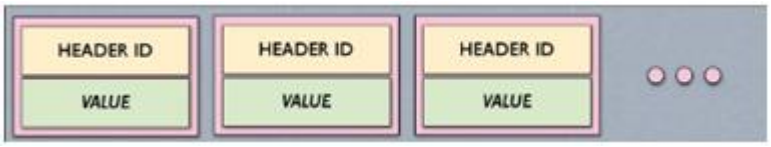


Figura 4 Estructura de “Headers”

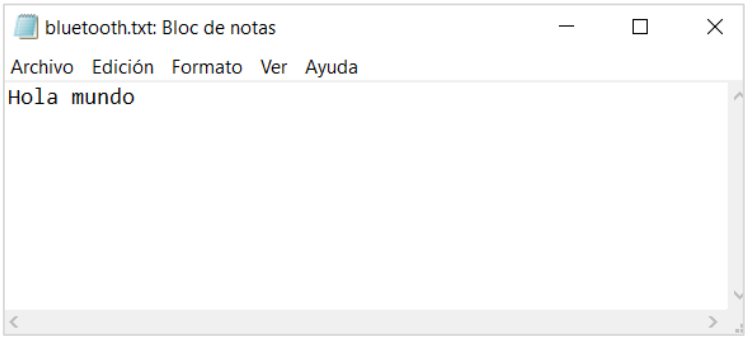


Figura 5 Texto enviado

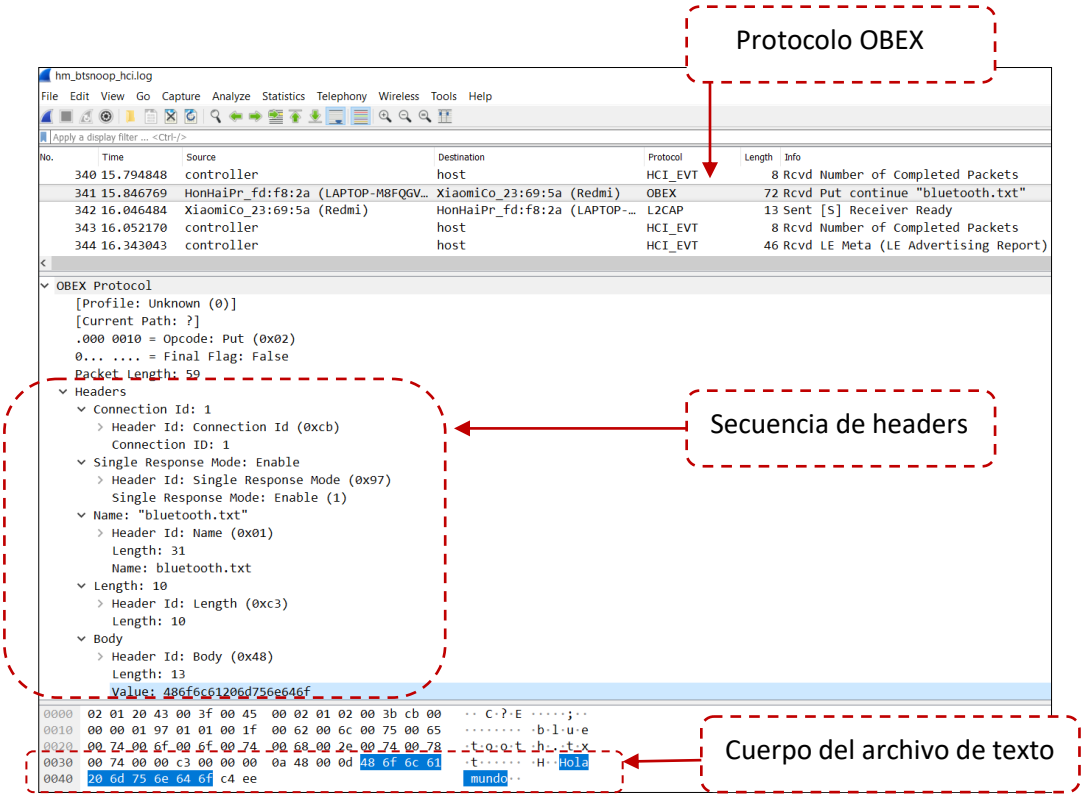
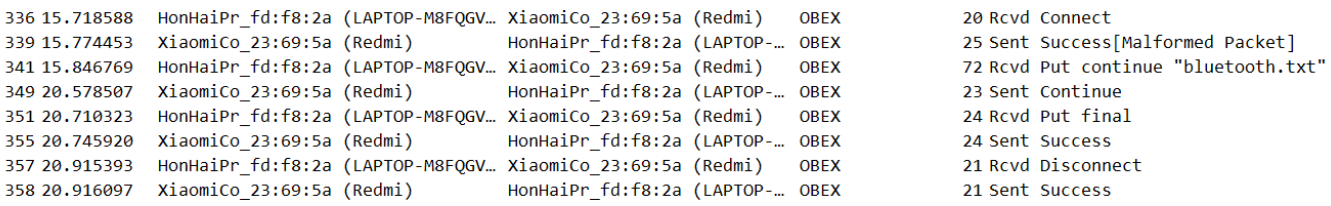


Figura 6 Pantallazo que muestra el desglose de wireshark sobre el protocolo obex



336	15.718588	HonHaiPr_fd:f8:2a (LAPTOP-M8FQGV…	XiaomiCo_23:69:5a (Redmi)	OBEX	20	Rcvd Connect
339	15.774453	XiaomiCo_23:69:5a (Redmi)	HonHaiPr_fd:f8:2a (LAPTOP-…	OBEX	25	Sent Success[Malformed Packet]
341	15.846769	HonHaiPr_fd:f8:2a (LAPTOP-M8FQGV…	XiaomiCo_23:69:5a (Redmi)	OBEX	72	Rcvd Put continue "bluetooth.txt"
349	20.578507	XiaomiCo_23:69:5a (Redmi)	HonHaiPr_fd:f8:2a (LAPTOP-…	OBEX	23	Sent Continue
351	20.710323	HonHaiPr_fd:f8:2a (LAPTOP-M8FQGV…	XiaomiCo_23:69:5a (Redmi)	OBEX	24	Rcvd Put final
355	20.745920	XiaomiCo_23:69:5a (Redmi)	HonHaiPr_fd:f8:2a (LAPTOP-…	OBEX	24	Sent Success
357	20.915393	HonHaiPr_fd:f8:2a (LAPTOP-M8FQGV…	XiaomiCo_23:69:5a (Redmi)	OBEX	21	Rcvd Disconnect
358	20.916097	XiaomiCo_23:69:5a (Redmi)	HonHaiPr_fd:f8:2a (LAPTOP-…	OBEX	21	Sent Success

Figura 7 Pantallazo de parte de la ventana “listing of capture packet” de Wireshark que muestra lo que realizó el protocolo obex