DESARROLLO DE EXPERIENCIAS PRÁCTICAS BASADAS EN EL ESTÁNDAR DE COMUNICACIONES INALÁMBRICAS BLUETOOTH

E. MARSAL, D. GUTIÉRREZ, M. SOTO, J. HINOJO, F. CORTÉS, F. BARRERO, S. TORAL
Departamento de Ingeniería Electrónica. Escuela Superior de Ingenieros. Universidad de Sevilla. España
estebanmarsal@us.es, dgutierrezreina@us.es, msoto@us.es, jhinojo@us.es, fcortes1@us.es, fbarrero@esi.us.es, toral@esi.us.es

Los sistemas de comunicación inalámbrica representan hoy en día el ejemplo más claro de cómo influyen las nuevas tecnologías de la información y las comunicaciones en la vida cotidiana de los seres humanos. Bluetooth, utilizado en dispositivos tan habituales como el teléfono móvil o la PDA, es uno de estos estándares de comunicación inalámbrica más empleados. El uso del estándar Bluetooth se basa en una serie de conceptos como la potencia de transmisión o los códigos de acceso y el tiempo dedicado al proceso de descubrimiento, ocultos generalmente al usuario del sistema. En este trabajo se presenta el desarrollo de una serie de actividades experimentales que permiten a los alumnos entrenarse en las características básicas del estándar Bluetooth, accediendo y modificando sus parámetros de configuración. Todas las experiencias prácticas, desarrolladas como ampliación del enfoque práctico de la asignatura denominada "Laboratorio de Instrumentación" adscrita a la titulación de Ingeniería de telecomunicaciones en la escuela Superior de Ingenieros de la Universidad de Sevilla, se basan en las librerías BlueZ y en el sistema operativo Linux.

1. Introducción

Bluetooth es un protocolo de comunicaciones inalámbrica que nos permite conectar dos o más dispositivos a corta distancia, permitiendo la transmisión de voz y de datos mediante enlaces de radio frecuencia en la banda ISM de 2.4 GHz [1]. Está adoptado como estándar (IEEE 802.15) dentro del grupo de redes inalámbricas de área personal (WPAN). Si bien las especificaciones de la norma Bluetooth son claras, las implementaciones en las distintas plataformas no son intuitivas y se hace estrictamente necesario conocer al detalle la especificación, lo que requiere un gran esfuerzo inicial por la extensión de la propia normativa (la versión 3.0 de Bluetooth se documenta en no menos de 1700 páginas). Para acercar al alumno el estándar, y debido a la situación descrita, se han desarrollado en el Departamento de Ingeniería Electrónica de la Universidad de Sevilla un conjunto de prácticas para que los alumnos de la titulación de Ingeniería de Telecomunicación, sin necesidad de un exhaustivo conocimiento teórico de la norma, puedan experimentar con algunos de los parámetros más importantes en el establecimiento de las comunicaciones inalámbricas generadas por Bluetooth, como son el proceso de descubrimiento de dispositivos y el rango de alcance. El desarrollo realizado pretende, posteriormente, que los alumnos aprendan a caracterizar los enlaces establecidos mediante un extenso análisis estadístico, a fin de aprendan a evaluar la calidad de estos.

2. El estándar Bluetooth: establecimiento y calidad del enlace inalámbrico

El proceso de descubrimiento en la especificación Bluetooth es fundamental en el establecimiento de la comunicación asociada al estándar Bluetooth. Este proceso se divide en tres fases [2]:

- En la primera fase, el dispositivo que inicializa la comunicación (que se denomina master en la norma) busca dispositivos a su alrededor. El master se encuentra en el estado

Inquiry durante esta fase, mientras que los dispositivos vecinos que estén a la escucha (slaves según la norma) se deben encontrar en el estado Inquiry Scan.

- A la fase anterior, le sigue el proceso denominado paging en el que ambos dispositivos, master y slave, realizan un handshaking, o comunicación con acuse de recibo, mediante el cual intercambian información fundamental para la formación del enlace.
- La última fase consiste en el establecimiento del enlace físico.

Una importante cuestión a tener en cuenta en el establecimiento de un enlace inalámbrico de tipo Bluetooth, es que si los dispositivos conocen sobre la existencia de otros en su rango de cobertura, esto no implica que exista ningún tipo de enlace entre ellos. Por otro lado, el proceso de descubrimiento se encuentra totalmente enmascarado en la comunicaciones ordinarias que se realizan hoy en día con dispositivos de uso común, como son los teléfonos móviles, pero cuando se requiere una respuesta rápida o con requerimientos de tiempo específicos, como son los sistemas de instrumentación electrónica, es necesario tener un mayor control sobre los parámetros que intervienen en el proceso de descubrimiento. La componente aleatoria en el proceso de descubrimiento es elevada [2, 3], requiriendo este estudio de un análisis estadístico complejo [3]. Existen muchos estudios acerca de cómo acelerar el proceso de descubrimiento empleando la norma Bluetooth, [4, 5, 6], y en la actualidad se está estudiando la introducción de nuevas tecnologías, mecanismos fuera de banda, para intentar mejorar este proceso de descubrimiento y emparejamiento. En concreto, y a partir de la especificación Bluetooth 2.1 y 3.0, se incluye la tecnología NFC como forma de intercambiar información de emparejamiento.

Ahora bien, una vez establecida una conexión Bluetooth, existen una importante variedad de parámetros relacionados con la calidad de la transmisión y entre sí, por lo que llegar a concluir cómo es esta calidad resulta una tarea complicada, especialmente por la cantidad de variables que intervienen, algunas muy difíciles de controlar debido a su componente aleatorio como se puede observar en los modelos de propagación de la señal que se suelen utilizar [7, 8]. Muchas de estas variables dependen del dispositivo particular y de su diseño particular, lo que nos lleva por ejemplo al tipo y comportamiento de los amplificadores internos o las antenas [9].

El acercamiento de forma práctica a las tecnologías inalámbricas de tipo Bluetooth se plantea como objetivo docente a cumplir, dado su extenso uso a nivel de electrónica de consumo, en una asignatura de origen práctico como es el Laboratorio de Instrumentación del 5º de la titulación Ingeniero en Telecomunicación adscrita al Departamento de Ingeniería Electrónica de la Universidad de Sevilla. De esta manera, se instruye experimentalmente a los alumnos a nuevas formas de instrumentación sin cables utilizando el aire como medio de transmisión.

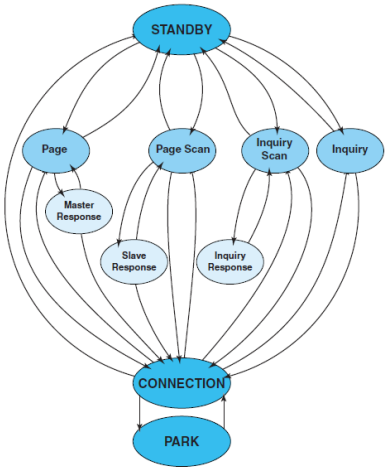

Figura 1. Diagrama de estados en el controlador de enlaces Bluetooth.

El objetivo de estas prácticas es hacer que los alumnos se paseen por los distintos estados del controlador de enlaces Bluetooth sin que eso suponga un excesivo gasto de tiempo y esfuerzo. Tres son los estados principales involucrados en el establecimiento de una conexión inalámbrica Bluetooth (Fig. 1): STANDBY (Espera), CONNECTION (Conexión) y PARK (Aparcar). Aparecen, además, otros siete subestados denominados paginación, detección de paginación, búsqueda, detección de búsqueda, respuesta del maestro, respuesta del esclavo y respuesta a la búsqueda. Los subestados son estados transitorios que se usan para establecer conexiones y permitir el descubrimiento de dispositivos. Para pasar de un estado o subestado a otro, se usan comandos del gestor de enlaces o bien señales internas del controlador de enlaces.

Desde el punto de vista del conjunto de aplicaciones desarrollada para la configuración de cada uno de los parámetros de los dispositivos Bluetooth, así como la gestión de las comunicaciones entre los mismos, se ha empleado BlueZ [10], que es la implementación de la pila de protocolos Bluetooth para sistemas operativos basados en Linux, que ofrece todo un extenso conjunto de módulos, librerías y aplicaciones para el trabajo con esta tecnología. A pesar de que existen otras implementaciones, como la desarrollada por el centro de investigación de Nokia y denominada Affix, el hecho de decantarse por BlueZ es prácticamente obligado, teniendo en cuenta que ofrece una serie de prestaciones que no ofrece ninguna de las otras implementaciones posible, tales como:

- Está definida como la implementación oficial de la denominada "Bluetooth Stack" para sistemas UNIX.
- Viene por defecto instalada y completamente integrada en la mayoría de distribuciones Linux del mercado (lo que mejora la capacidad de interoperabilidad del alumno con la tecnología).
- Existencia de infinidad de aplicaciones y librerías.

Sin embargo, a nivel didáctico ofrece lamentablemente carencias, como es la escasa documentación ofrecida, principal problema de muchos de los proyectos de desarrollo en software libre y código abierto. Esto hace que su uso en los instantes iniciales sea poco amigable, y la curva de aprendizaje necesaria para llegar a hacer un uso razonable de BlueZ sea demasiado extensa. Para resolver este tipo de inconvenientes existe la posibilidad de la generación de un conjunto de funciones y de APIs en los que los parámetros de configuración a añadir se resuelven como parámetros a introducir en dichas funciones, elevando el nivel de abstracción y permitiendo al alumno un primer acercamiento mucho más liviano y menos costoso en tiempo hacia BlueZ.

BlueZ fue desarrollada por Qualcomm desde 2001 bajo licencia GPL, promovida por el Bluetooth Interest Group desde 2005 y disponible de manera oficial como parte de la implementación de los kernels de Linux a partir de la versión 2.4.6.

3. Aplicaciones desarrolladas

Las aplicaciones para los alumnos se han hecho en código ANSI C, permitiéndoles cambiar los parámetros por línea de comando e ir así variándolos, a fin de constatar como afecta el cambio de las mismas a las pruebas siguientes. En cuanto a la aplicación a la asignatura denominada Laboratorio de Instrumentación Electrónica, se han desarrollado una serie de trabajos prácticos para ayudar al alumno a comprender los parámetros que entran en juego al establecerse un enlace inalámbrico Bluetooth, así como el rango de valores posibles que pueden tomar. Estos ensayos son:

Pruebas de búsqueda de dispositivos. El proceso de descubrimiento es asimétrico. Un dispositivo Bluetooth trata de encontrar otros dispositivos cercanos enviando mensajes de descubrimiento (inquiry requests). Los dispositivos Bluetooth que están disponibles para ser encontrados escuchan estos mensajes y responden con su dirección Bluetooth. Este proceso de descubrimiento utiliza un canal físico especial para los mensajes de búsqueda. En la prueba diseñada, se busca que los alumnos interactúen con los parámetros de búsqueda de dispositivos Bluetooth que se

detallan a continuación:

- Inquiry length. Valor que especifica el tiempo máximo que el dispositivo debe esperar las respuestas de los otros dispositivos. Puede tomar valores enteros de 1 a 30, que corresponden a múltiplos de 1,28 s.
- Number of responses. Máximo número de respuestas que el dispositivo espera. Puede tomar valores de 1 a 255 dispositivos. El valor cero significa infinitas respuestas.
- LAP. Representa a la parte baja de una dirección Bluetooth. Puede tomar valores desde 9E8B00 hasta 9E8B3F, expresado en notación hexadecimal. Si se le asigna cero, se utiliza el código de acceso general 9E8B33.
- IAC. Especifica el número de códigos de acceso de búsqueda que serán utilizados por el dispositivo local durante la fase Inquiry scan. Puede tomar valores de 1 a 40 en notación hexadecimal.
- Type. Selecciona que tipo de búsqueda realizar. Los valores pueden variar de 0 a FF en notación hexadecimal; el valor 0 implica búsqueda estándar y el 1 hará la búsqueda entrelazada. Los demás valores están reservados para usos futuros.
- Mode. Modifica el tipo de resultado esperado en las búsquedas de dispositivos. Puede tomar valores de 0 a FF en notación hexadecimal. El valor 0 representa la respuesta estándar, el valor 1 añade el valor del RSSI a la respuesta y el valor 2 es para obtener la respuesta extendida. Los valores de 3 a FF, están reservados.

```
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$ ./busqueda
./inquiry <len> <max_rsp>
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$ ./busqueda 8 255
00:22:F7:17:03:D1 jose-dell-1
00:17:E8:F4:7D:7A Jose Maria Hinojo
00:09:DD:50:19:6D deepblue-1
00:22:F7:17:03:D8 jose-dell-2
00:22:F7:17:03:87 deepblue-0
00:1D:4F:96:98:B7 Batman
00:1E:3B:D1:26:9A GoyoBT
00:23:4D:E8:AC:5C jose-dell-0
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$
```

Figura 2. Captura de pantalla de los resultados de la búsqueda de dispositivos con código de acceso general.

Se ven los resultados de la búsqueda de dispositivos cercanos (Fig. 2), se ven la dirección Bluetooth y el nombre amigable de cada dispositivo. La aplicación debe ejecutarse con los parámetros *len* y *max_rsp* como entrada, que son el tiempo de búsqueda y la cantidad de dispositivos que esperamos encontrar respectivamente. La búsqueda finaliza cuando se satisface una de las dos condiciones.

```
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$ ./busqueda_entrelazada
./busqueda_entrelazada <dir_bt> <iac> <lap> <type> <mode>
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$ sudo ./busqueda_entrelazada  00:02:5B:0A:6E:52 1 9e8b01 1 1
iac = 1
lap = 9e 8b 33
Inquiry:
        Tipo:   0x00
        Modo:   0x01
iac = 1
lap = 9e 8b 1
Inquiry:
        Tipo:   0x01
        Modo:   0x01
esteban@esteban-desktop:~/Escritorio/busqueda de dispositivos$
```

Figura 3. Captura de pantalla de los resultados de la búsqueda de dispositivos con código de acceso dedicado.

El cambio de los parámetros de búsqueda de dispositivos (Fig. 3), antes y después del cambio de los valores. La aplicación desarrollada debe ejecutarse con cinco parámetros, que son: la dirección Bluetooth del dispositivo local, el código de búsqueda, el código de acceso, el tipo y el modo de

respuesta del proceso de búsqueda.

Pruebas de calidad de enlace. Se pretende que los alumnos obtengan los parámetros que hacen referencia a la calidad del enlace y a la potencia recibida y transmitida por los dispositivos a fin de establecer métricas y poder comparar los estados de los enlaces. Las variables analizadas son:

- Transmit Power Level (TPL), que especifica el nivel de potencia transmitida (en dBm) por el módulo Bluetooth. En la mayoría de los casos un emisor responderá con el nivel de potencia configurado por defecto para iniciar o responder a las preguntas, aunque la variable TPL puede variar durante la conexión, debido al control de potencia, mediante comandos de regulación de potencia. En la especificación Bluetooth el control de potencia es obligatorio en los dispositivos de clase 1 y opcional en los demás.
- Received Signal Strength Indicator (RSSI). Variable que indica si el nivel de potencia recibida está dentro, por encima o abajo del denominado Golden Receiver Power Range (GRPR), que es considerado como el rango ideal de potencia aplicable al transmisor para el establecimiento del enlace Bluetooth. Tal como se define en la especificación Bluetooth, un RSSI positivo o negativo (en dB) indica que el nivel de potencia está por encima o por debajo de la GPRP, respectivamente, mientras que cero es el valor ideal (el nivel de potencia recibida está dentro de GRPR).
- Link Quality (LQ). Evalúa la calidad del enlace que se percibe en el receptor. El índice varía desde 0 hasta 255. A mayor valor, mejor es el estado del enlace. Para la mayoría de los módulos de Bluetooth, que se deriva de la tasa media de error de bit (BER) visto en el receptor, y se actualiza constantemente en forma de paquetes que se reciban. Sin embargo, la asignación exacta de BER a LQ es específico del dispositivo. LQ se utiliza principalmente para adaptarse a los cambios en el estado del enlace, en particular, para apoyar al denominado CQDDR (Canal Driven Quality Data Rate).

Se muestra la aplicación desarrollada para evaluar las características del enlace (Fig. 4). A ésta se le pasa la dirección Bluetooth del dispositivo al que estamos conectados y nos devuelve la potencia actual del transmisor, el valor del RSSI y la calidad del enlace. Se ve como variando la posición y velocidad de los dispositivos, las características del enlace varían.

```
esteban@esteban-desktop:~/Escritorio/RSSI, TPL y LQ$ ./rssiytpl
mide-rssi <btaddr>
esteban@esteban-desktop:~/Escritorio/RSSI, TPL y LQ$ ./rssiytpl 00:1E:3B:D1:26:9A
Midiendo RSSI
Numero de conexiones: 1
Direccion de dispositivo remoto: 00:1E:3B:D1:26:9A
Valor de la potencia 4
Link quality: 255
Valor del rssi -4
Valor de la potencia 4
Link quality: 245
Valor del rssi -5
Valor de la potencia 4
Link quality: 251
Valor del rssi -6
Valor de la potencia 4
Link quality: 242
Valor del rssi -12
Valor de la potencia 4
Link quality: 211
Valor del rssi -13
Valor de la potencia 4
Link quality: 210
Valor del rssi -13
Valor de la potencia 4
Link quality: 211
Valor del rssi -14
Valor de la potencia 4
Link quality: 212
Valor del rssi -14
Valor de la potencia 4
Link quality: 211
Valor del rssi -13
Valor de la potencia 4
Link quality: 211
```

Figura 4. Captura de pantalla con los resultados de los parámetros de calidad de enlace.

Pruebas de control de enlace. Se han desarrollado pruebas para analizar parámetros y estados muy importantes de entender a la hora de desarrollar aplicaciones para comunicaciones Bluetooth. Dentro de estos, destacar:

- Park mode. Cuando un dispositivo slave no necesita participar en una piconet, pero aún necesita estar sincronizado con el master, puede entrar en este modo, donde el slave tiene muy poca actividad pero se despierta a intervalos regulares de tiempo para mantenerse sincronizado con la piconet.
- Role switch. Un dispositivo necesita intercambiar las funciones cuando, por ejemplo, necesita ser master de más de una piconet.

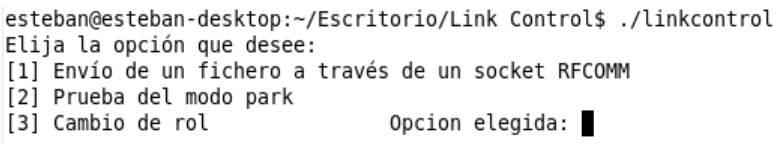

Figura 5. Captura de pantalla de la aplicación para cambiar los parámetros de control de enlace.

Se ven las opciones de la aplicación de control de enlace (Fig. 5), que nos permite enviar ficheros entre dispositivos Bluetooth (para realizar pruebas de control de velocidad o parámetros que necesiten de un enlace establecido), aparcar dispositivos y, por último, cambiar el rol master-slave de una piconet.

4. Conclusión

Este trabajo presenta el desarrollo de aplicaciones que permitirán a los alumnos de Laboratorio de Instrumentación acercarse de forma fácil y práctica a la norma Bluetooth, saltándose los detalles de programación de una pila de protocolos específica. Esto permitirá concentrarse en el significado y valor de una serie de parámetros referentes a la búsqueda y detección de dispositivos Bluetooth, así como las características del enlace establecido y la configuración topológica de una red Bluetooth. Además se intenta estimular el aprendizaje basado en prácticas, necesario en aplicaciones de este tipo.

Referencias

[1] Bluetooth Special Interest Group. *Bluetooth Specification Version 2.1 + EDR*, http://www.bluetooth.com/ (2007).

[2] G. Záruba y I. Chlamtac. *Accelerating Bluetooth Inquiry for Personal Area Networks.* Global Telecommunications Conference, 2003, vol. 2, pp.702-706, GLOBECOM '03, Diciembre 2003.

[3] B. Peterson, R. Baldwin y J. Kharoufeh. *Bluetooth Inquiry Time Characterization and Selection. Mobile Computing, IEEE transactions,* vol. 5, pp. 1173-1187, 2006.

[4] G. Záruba y V. Gupta. *Simplified Bluetooth Device Discovery – Analysis and Simulation. Systems Scineces*, 2004. Proceedings of 37th Annual Hawaii International Conference, pp. 9pp, 2004.

[5] S. Asthana y D. Kalofonos. *The problem of Bluetooth pullution and accelerating connectivity in Bluetooth Ad-Hoc networks. Pervasive Computing and Communications*, 2005. PerCom 2005. Third IEEE International Conference, pp. 8-12, 2005.

[6] X. Zhang y G. Riley. *Evaluatioin and accelerating Bluetooth device discovery. Radio and Wireless Symposium, pp.* 467-470, 2006.

[7] F. Bektas, B. Vondra, P. Veith, L. Faltin, A. Pohl y A. Scholtz. *Bluetooth communication employing antenna diversity*. *Computers and Communication*, 2003. Proceedings. Eighth IEEE International Symposium on, 2003, pp.652-657, vol 1, 2003.

[8] A. Mohammed y T. Hult. *Evaluation of the Bluetooth link and antennas performance for indoor office environments by measurement trials and FEMLAB simulations. Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st,* pp. 238-242, vol. 1, 2005.

[9] F. Forno, G. Malnati, G. Portelli. *Desing and implementation of a Bluetooth ad hoc network for indoor positioning*. Software, IEE Proceedings, pp. 223- 228, vol. 152, 2005.

[10] BlueZ, pila de protocolos Bluetooth oficial para Linux, http://bluez.org/