Capítulo 3

Redes inalámbricas

Está previsto que las comunicaciones inalámbricas sean ampliamente utilizadas en un futuro cercano para dos tipos de comunicación:

- comunicaciones en el interior del vehículo
- comunicaciones entre el vehículo y otras entidades localizadas a lo largo de la carretera o en el interior de otros vehículos

Comunicaciones en el interior del vehículo

Los automóviles modernos contienen un número cada vez mayor de unidades de control electrónico (ECU, *Electronic Control Unit*) y sus sensores y actuadores asociados. Por ejemplo, más de 50 sensores se pueden encontrar actualmente en vehículos de gama media. Es evidente que el cableado necesario para tales dispositivos puede acarrear diversos problemas y dificultar la instalación. Además, con las actuales redes basadas en CAN, el sistema debe ser rediseñado con cada cambio importante. La integración de sensores inalámbricos pude aportar una mayor flexibilidad, formando en el vehículo una red de sensores, actuadores y sistemas de información y entretenimiento. Estas redes no son un tipo cualquiera de redes de sensores, se diferencian por un diseño más específico guiado por los requisitos de bajas latencias y fiabilidad ya comentados en el capítulo anterior.

Este tipo de redes de sensores se diferencian de otras redes inalámbricas como 802.11 en varios aspectos clave. Por ejemplo, en cuanto a la topología, los sensores y actuadores de un vehículo siguen una topología en estrella con la ECU asociada sirviendo de nodo central. Esta topología es diferente a las tradicionales configuraciones ad-hoc.

Las tasas de transmisión requeridas también suelen ser diferentes; también los protocolos y los requisitos de fiabilidad de datos. La mayoría de redes inalámbricas para comunicación de datos utilizan la familía de protocolos TCP/IP. Sin embargo, una red basada en el protocolo IP es probablemente inapropiada para una red de sensores en el automóvil. La principal razón es que la carga asociada con la manipulación del protocolo es demasiado costosa para la mayoría de aplicaciones de control. Además, los requisitos de fiabilidad/integridad en los datos han de ser iguales o mayores a los de la red cableada. Habitualmente, en redes ad-hoc, las aplicaciones tratan de enmascarar la hetereogeneidad de la red a través de protocolos como TCP/IP o algún otro basado en el modelo OSI. Estos esquemas generalizados son inapropiados en automovilismo, donde habitualmente los datos lanzados por un sensor son de unos pocos bytes.

Los vehículos actuales cuentan con sensores que pueden requerir latencias de menos de 1 ms y

tasas de transmisión de 12 kbps hasta otros que requieren latencias de 50 ms y tasas de 5 bps. Por tanto, los requisitos cubren un amplio espectro. A la hora de escoger un protocolo es necesario alcanzar un compromiso entre soluciones a medida, que serían complejas de implementar y más costosas; y soluciones estándar como TCP/IP, que podrían añadir una sobrecarga no necesaria.

A nivel físico, estudios de propagación de ondas en el interior de un vehículo deben llevarse a cabo. Actualmente se cuenta con algunos resultados preliminares [1], [2], [3]. A nivel MAC (acceso al medio) se debe optar por soluciones que garanticen unas latencias máximas, preferiblemente evitando métodos de acceso por contienda.

Comunicaciones con el entorno

Este tipo de comunicaciones tiene lugar entre el vehículo y las distintas infraestructuras o bien otros vehículos. Aunque en este caso se puede intercambiar información de entretenimiento, está claro que el aspecto más importante es el relacionado con la seguridad.

Para implementar una red inalámbrica que conecte al vehículo con la infraestructura (V2I, *Vehicle To Infrastructure*), es necesario instalar un conjunto de estaciones base distribuidas a lo largo de las carreteras que se pondrá en contacto con los vehículos que pasen por sus cercanías.

Diversos tipos de información podrían ser intercambiados con un sistema así. Además de las condiciones del trafico y las condiciones de la carretera, que podrían ser mas frecuentes que aquellas que se reciben a través de radio o paneles informativos, es posible alertar a los conductores de posibles situaciones peligrosas en tiempo real. Además, un vehículo envuelto en un accidente puede emitir rápidamente información con dos importantes objetivos:

- La solicitud de ayuda podría comenzar inmediatamente.
- El resto de vehículos cercanos podrían quedar advertidos sobre el accidente.

La comunicación con el resto de vehículos (V2V, *Vehicle To Vehicle*) hace posible lo que se podría llamar un "viaje cooperativo", lo que permite intercambiar gran cantidad de información útil, en particular en aspectos de seguridad. Por ejemplo, un vehículo podría ser informado de la velocidad de los vehículos que circulan por delante, con las consecuentes indicaciones para regular la velocidad. Incluso un sistema de seguridad activo podría procesar la información de los automóviles cercanos y, en caso de que se prevea un accidente inminente que tendrá lugar en pocos segundos, pre-tensar los cinturones y preparar el airbag. Se puede hacer un resumen de las posibles aplicaciones de las comunicaciones V2V y V2I:

- Seguridad: avisos en llegadas a cruces, avisos de obstáculos, avisos de paradas repentinas, reporte de accidentes, avisos de cambio de carril, prevención de colisiones.
- Gestión del tráfico: límites de velocidad variables, semáforos adaptables, prioridades para cierto tipo de vehículos (por ejemplo, ambulancias).
- Asistencia: ayuda para aparcar el vehículo, control de velocidad, reconocimiento de señales.
- Control: avisos de límites de velocidad, accesos restringidos, vigilancia.
- Tarificación: pago de peajes, pago de parkings.

Un sistema externo de comunicaciones inalámbricas, especialmente cuando se usa con propósitos de seguridad, debe satisfacer estrictos requisitos temporales. Parece razonable que la entrega de los

mensajes no se retrase más de 100 ms, lo que puede dar lugar a tiempos de reacción totales en torno a 1 s, teniendo en cuenta las latencias de los componentes implicados. El área geográfica cubierta puede ser considerada extensa: en torno a los cientos de metros. Actualmente no existe ninguna tecnología inalámbrica capaz de satisfacer por sí sola los requerimientos de este tipo de comunicaciones, aunque hay en estudio algunas propuestas, como 802.11p que se trata más extensamente en uno de los siguientes apartados.

En este caso, el mayor reto lo supone no sólo superar el comportamiento de un canal inalámbrico impredecible, sino también el soportar rápidos cambios en la topología de la red junto con estrictos requisitos de tiempo y fiabilidad. Obviamente, sólo tiene sentido informar de una determinada situación antes de que sea un hecho y se pueda evitar algún peligro. Por tanto se requiere que los retrasos en este tipo de comunicaciones estén acotados. No se requieren altas tasas de transmisión, simplemente un sistema predecible que sea capaz de entregar los mensajes dentro de un plazo determinado.

En este sentido un aspecto crucial lo supone la implementación de la capa de acceso al medio, el cual debe ser dividido de una manera justa y predecible entre todos los participantes. En los sistemas de comunicación entre vehículos se ha prestado mucha atención a mejorar el método MAC introduciendo diferentes calidades de servicio (QoS, *Quality of Service*) para datos con diferentes prioridades. Probablemente no se necesitan muchas clases de servicio o tasas de transferencia diferentes, pero sí que es necesario que el método de acceso proporcione un tiempo de acceso finito para el peor caso. La información entregada fuera de plazo, no es solamente inútil, sino que también implica consecuencias graves para el sistema de seguridad de tráfico [4].

En la siguiente sección se muestran las principales características de varios protocolos de comunicación inalámbricos que podrían ser utilizados en redes de sensores. Se ha decidido optar por estándares internacionales para asegurar la compatibilidad con otros dispositivos. Partiendo de que los dispositivos no estarán físicamente muy alejados unos de otros, la búsqueda se ha enfocado fundamentalmente en redes inalámbricas de área personal o WPAN (*Wireless Personal Area Network*) y redes inalámbricas de área local o WLAN (*Wireless Local Area Network*), destacándose las siguientes:

- Wi-Fi (IEEE 802.11)
- IEEE 802.11p
- Bluetooth (IEEE 802.15.1)
- Ultra Wide Band (IEEE 802.15.3a)
- ZigBee (IEEE 802.15.4)
- WiMAX (IEEE 802.16)

3.1 Algunas tecnologías radio

3.1.1 IEEE 802.11

Se trata de un conjunto de normas [5] que implementan los niveles inferiores del modelo OSI (*Open System Interconnection*), en concreto, el nivel físico y el de enlace, sobre un canal inalámbrico. En su concepción se pensó para sustituir a Ethernet (estándar IEEE 802.3) en aquellas zonas o puntos donde difícilmente se podría llegar con un cable. El estándar base 802.11 fue inicialmente aprobado por el IEEE en 1997. Incluía una capa física de infrarojos y dos de espectro ensanchado (DSSS y FHSS). Desde entonces una serie de modificaciones a este estándar han sido propuestas y adoptadas:

La capa MAC de 802.11 proporciona dos métodos distintos de ganar acceso al medio; por contienda, conocido como *Distributed Coordination Function* (DCF) y libre de contienda, conocido como *Point Coordination Function*. PCF sólo puede ser usado cuando la red contiene un punto de acceso que mantiene un controlador de acceso. En este modo, todos los dispositivos deben recibir permiso de este controlador de acceso para empezar a transmitir. El procedimiento empieza cuando el dispositivo móvil envía una solicitud al punto de acceso indicando que desea transmitir. Este modo es opcional en el estándar, mientras que DCF es obligatorio, pudiendo el punto de acceso alternar entre ambos.

DCF se bada en la técnica CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) y todos los terminales deben competir por el acceso al canal. Cuando un dispositivo desea transmitir un paquete, empieza a escuchar el canal. Si está libre durante un tiempo, conocido como *Distributed Interframe Spacing* (DIFS), empezará a transmitir. También se implementa un mecanismo virtual denominado *Network Allocation Vector* (NAV), el cual sirve para indicar si el medio está ocupado incluso cuando no se detecta como tal. Cuando el canal está ocupado, el dispositivo espera un tiempo aleatorio antes de intentar la transmisión cuando vuelve a estar libre, ya que las mayores probabilidades de colisión ocurren tras la liberación del canal.

IEEE 802.11a: Se trata de una enmienda del estándar IEEE 802.11-1999 que se corresponde con la tercera generación de redes inalámbricas debido a que su aparición en el mercado fue posterior a la de las redes IEEE 802.11 y IEEE 802.11b. Sin embargo, su desarrollo se había iniciado antes que el del estándar IEEE 802.11b. A pesar de ello, se retrasó debido a los requisitos tecnológicos necesarios para poder llevarlo a cabo. La enmienda ha sido incorporada dentro del nuevo IEEE 802.11-2007 [5]. En concreto, las redes inalámbricas IEEE 802.11a se caracterizan por operar a una frecuencia de 5 GHz, en la banda de frecuencia conocida como UNII (*Universal Networking Information Infraestructure*). Esta forma de comunicación inalámbrica no está autorizada para su utilización en Europa porque la banda que usa para operar se encuentra ocupada por el estándar HiperLAN2. Se pueden citar las siguientes características:

- La tasa de transmisión es de 54 Mbps.
- Al trabajar en la banda UNII, posee mayor inmunidad frente a las interferencias por solapamiento, ya que dicha banda contempla el uso de 4 canales para este fin.
- Utiliza la banda libre de 5 GHz.

802.11a utiliza OFDM (*Orthogonal Frequency Division Multiplexing*). OFMD es una técnica de transmisión multiportadora que data los años sesenta. La idea básica es dividir el espectro disponible en varios subcanales. El flujo de datos se divide en varios flujos de datos más lentos que se transmiten simultaneamente en estos subcanales. OFDM tolera mejor problemas como la atenuación selectiva en frecuencia, propagación multitrayecto e interferencias.

Este estándar soporta diferentes tasas de transmisión, las cuales se pueden ver en la Tabla 3.1. Nótese que la tasa de código no tiene por qué ser la misma en cada caso, aunque no se ha especificado. El esquema de adaptación del enlace depende de la condición del canal y no se especifica en el estándar. La cabecera de un paquete es siempre enviada a la tasa de transmisión más baja. El número total de portadoras para datos es 48.

IEEE 802.11b

El estándar 802.11b es una extensión de la capa física original DSSS (*espectro ensanchado por secuencia directa*) en la banda de los 2.4 Ghz y permite tasas de transmisión de hasta 11 Mbps. La principal

Mbps	Modulación	Bits/Subportadora	Bits/Símbolo OFDM
6	BPSK	1	48
9	BPSK	1	48
12	QPSK	2	96
18	QPSK	2	96
24	16-QAM	4	192
36	16-QAM	4	192
48	64-QAM	6	288
54	64-QAM	6	288

Tabla 3.1: Diferentes tasas de transmisión en IEEE 802.11a

ventaja de este estándar es que ha sido ampliamente usado en todo el mundo para establecer redes inalámbricas, siendo el primero en salir de forma comercial. En 2007 también fue incorporada al nuevo IEEE 802.11-2007. Presenta una serie de inconvenientes que en revisiones posteriores se han intentado corregir. Entre éstas se pueden citar:

- Problemas de interferencias debido a que el rango de frecuencias en el que opera se encuentra saturado al tratarse de una banda libre.
- La capacidad de transmisión es reducida.
- Requiere de modulaciones que contrarresten los efectos de trayectorias múltiples.
- Es sensible a la distancia de tal forma que a una distancia a más de 75 metros la capacidad del enlace se ve disminuida a 2 Mbps.

IEEE 802.11g

Esta enmienda surgió como una extensión del IEEE 802.11b con el que se pretendía mejorar la capacidad de transmisión del enlace usando el mismo rango de frecuencias, es decir, la banda de 2,4 GHz. Para ello, lo que se hizo fue introducir un segundo modo de acceso basado en OFDM usado ya en las redes IEEE 802.11a, que permitió aumentar la capacidad del enlace hasta los 54 Mbps. De esta forma, al disponer de las dos técnicas de modulación, las usadas en IEEE 802.11b y la usada en IEEE 802.11a, este estándar podía dar servicio a dispositivos que cumpliesen la normativa IEEE 802.11b y a la vez a los nuevos dispositivos compatibles con el estándar IEEE 802.11g. Por tanto, la principal ventaja de las redes IEEE 802.11g es el aumento considerable de la tasa de transmisión hasta 54 Mbps. No obstante, al compartir la misma banda que IEEE 802.11b presenta las mismas desventajas.

IEEE 802.11n

Se corresponde con una norma recientemente aprobada [6]. Se caracteriza principalmente por conseguir un aumento de la capacidad de transmisión muy superior a la proporcionada por IEEE 802.11a/-b/g. Se podrían alcanzar hasta 600 Mbps. Para poderlo conseguir ha sido necesario emplear dos conceptos claves en la definición de la capa física: el uso de sistemas MIMO (Multiple In Multiple Out) y un ancho de banda de 40 MHz para los diversos canales existentes. La unión de estas dos decisiones de diseño ha originado ese aumento de la capacidad de transmisión.

Durante la formulación de este estándar se ha mantenido siempre el carácter compatible del mismo con las revisiones anteriores de IEEE 802.11, por lo que permite el uso de modulaciones OFDM

para poder usar dispositivos compatibles con IEEE 802.11a/g y las técnicas vistas en 802.11b. Esta característica supone una gran ventaja comercial puesto que el usar un nuevo estándar de comunicaciones inalámbricas no supone tener que cambiar los dispositivos que el usuario pueda ya haber adquirido. Entre otras de las principales ventajas de IEEE 802.11n se encuentran las siguientes:

- mayor capacidad de transmisión, hasta 600 Mbps
- compatibilidad hacia atrás con los dispositivos IEEE 802.11a/b/g
- uso de modos para reducir el consumo

Aunque todos estos protocolos (802.11a/b/g/n) se diseñaron para sustituir a redes cableadas ethernet, se pueden encontrar estudios de su rendimiento en comunicaciones V2V y V2I.

3.1.2 IEEE 802.11e

Esta enmienda [7] añade QoS a la capa MAC de IEEE 802.11, y es independiente de la capa física en uso. Define un nuevo procedimiento de acceso al medio denominado *Hybrid Coordination Function* (HCF). También introduce un nuevo espacio intertrama llamado *Arbitration Interframe Space* (AIFS). Se incorporó también al estándar IEEE 802.11-2007 [5].

La HCF proporciona dos nuevos métodos de acceso: EDCA (*Enhanced Distributed Channel Access*) y HCCA (*HCF Controlled Channel Access*). EDCA es una versión mejorada de DFC. En lugar de usar un DIFS para todos los tipos de paquetes, utiliza el llamado AIFS. Diferentes paquetes tienen longitudes diferentes de AIFS, con lo que los paquetes de mayor prioridad pueden tener un espacio intertrama más pequeño.

HCCA es un nuevo procedimiento centralizado de acceso al medio libre de contienda y debe ser usado junto con un punto de acceso. Cuando se usa HCCA, el tiempo se divide en periodos de contienda y periodos libres de contienda. Los equipos que quieren acceder al periodo libre de contienda solicitan recursos durante el periodo de contienda usando EDCA.

3.1.3 IEEE 802.11p

IEEE 802.11p [8], que se se puede encuadrar dentro de las tecnologías *Dedicated Short-Range Communications* (DSRC), es un futuro estándar WLAN dirigido a los sistemas de seguridad de tráfico. El término DSRC es ambiguo, pudiendo hacer referencia a diferentes estándares. Los estándares originales DSRC, que se pueden encontrar en Europa, Japón y Corea, son estándares más específicos que contienen la pila completa de protocolos y están diseñados para aplicaciones tales como pago automático de peajes.

El actual borrador de 802.11p está pensado exclusivamente para aplicaciones en entornos de vehículos, como servicios de seguridad y emergencia a lo largo de las carreteras, los cuales requieren una alta fiabilidad y baja latencia (varios cientos de milisegundos como mucho). Usará la misma capa física que 802.11a e introduce cambios a parámetros como la tolerancia a la frecuencia del reloj de símbolos, tolerancia a la frecuencia de transmisión, temperaturas de operacíon, etc. Utilizará canales de 10 MHz, en lugar de los de 20 MHz utilizados en 802.11a, por tanto son posibles tasas de transmisión de 3, 4.5, 6, 8, 12, 18, 24 y 27 Mbps.

802.11p usará la banda de 5,850-5,925 Ghz (ITS-RS, *Intelligent Transportation Systems Radio Service*) que se ha reservado en EEUU por la FCC para aplicaciones DSRC. Recientemente, también se

han reservado en Europa 30 Mhz en la banda de 5.9 Ghz para este tipo de aplicaciones. La decisión se basa es que estas frecuencias son especialmente apropiadas para entornos de vehículos.

La capa MAC de 802.11p usará el mecanismo EDCA (*Enhanced Distributed Channel Access*) derivado de 802.11e. Esto proporciona un acceso priorizado al canal gracias al uso de colas con diferentes espacios de arbitraje entre tramas (AIFS). La cola con la mayor prioridad tendrá que esperar el menor tiempo (menor AIFS) antes de que su transmisión pueda comenzar. Si hay estaciones con tráfico de menor prioridad, perderán la batalla por el canal frente a las estaciones con el tráfico de mayor prioridad.

IEEE 802.11p tiene una gran importancia dentro de la familia de estándares llamada *IEEE 1609 Family of Standards for Wireless Access Vehicular Environments* (WAVE) desarrollada por el IEEE. La pila de protocolos IEEE 1609 tiene soporte para TCP/IP, pero también incluye su propio protocolo de nivel de red y transporte, denominado *WAVE short message protocol* (WSMP). Esta pila soporta tanto comunicaciones de vehículo a vehículo como comunicaciones entre vehículos e infraestructuras. La pila consiste en los protocolos IEEE 1609.1, IEEE 1609.2, IEEE 1609.3 y IEEE 1609.4, tal como se puede ver en la Figura 3.1.

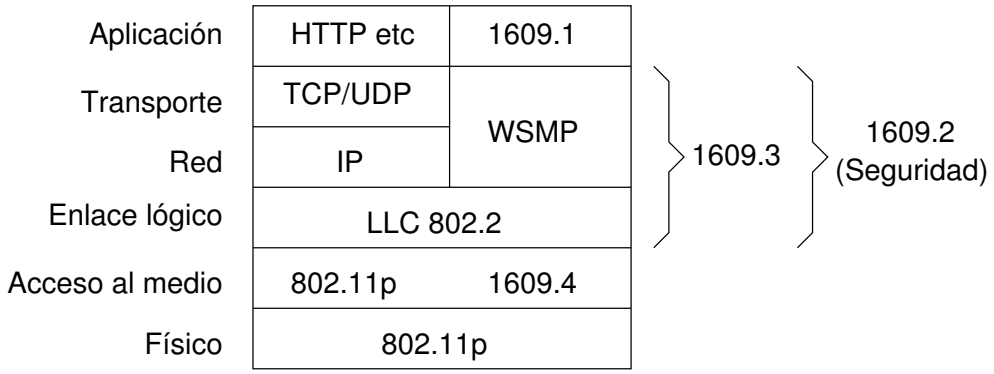

Figura 3.1: Conjunto de protocolos IEEE 1809

En un sistema IEEE 1609 hay dos tipos de dispositivos: unidades de a bordo (OBU, *On-Board Units*) y unidades distribuidas a lo largo de la carretera (RSU, *RoadSide Units*), sin que sea necesario ningún tipo de autenticación o procedimiento de asociación para unirse a la red.

IEEE 1609.1 es un gestor de recursos situado en la capa de aplicación, multiplexando comunicaciones entre un transmisor y múltiples receptores [9]. El escenario típico es que un RSU proporciona un servicio y un OBU lo usa. Un gestor de recursos (RM) hospedado en la RSU es responsable de retransmitir comandos desde la aplicación del RM (RMA). En el OBU debe situarse un procesador de comandos de recurso (RCP, *Resource Command Processor*). Los RMAs se comunican con los RCPs a través del RM.

IEEE 1609.3 implemente el protocolo WSMP, incluyendo labores de transporte y red [10]. El WSMP ofrece a las aplicaciones la capacidad de determinar características del canal físico como la potencia de transmisión. IEEE 1609.2 añade mecanismos de seguridad [11]. Una estación compatible con WAVE debe soportar un canal de control (CCH) y múltiples canales de servicio (SCH) tal como se define en IEEE 1609.4 [12]. La manera en que dichos canales se usan es decidido por 802.11p. Un dispositivo escucha en el canal CCH hasta que un anuncio de servicio (WSA, *WAVE Service Advertisement*) se recibe. Este WSA contiene información sobre un servicio en uno de los SCHs. El CCH está orientado a la transmisión de mensajes cortos y no permite tráfico IP.

3.1.4 Bluetooth

Es un estándar de comunicaciones inalámbricas basado en radiofrecuencia, de bajo coste y bajo consumo energético. Las características y versatilidad que presenta Bluetooth han hecho que se pueda utilizar en una gran cantidad de situaciones, como pueden ser el establecimiento de conexiones entre dos terminales móviles inteligentes (PDAs, teléfonos móviles), conexionado de periféricos, dispositivos de audio, ordenadores, etc.

El trabajo conjunto de los diferentes miembros del Bluetooth SIG (*Special Interest Group*) permitió una rápida aceptación por parte de los fabricantes, así como la compatibilidad entre dispositivos de diferentes fabricantes. Este hecho, provocó que las redes WPAN (*Wireless Personal Area Network*) basadas en Bluetooth estuviesen reguladas por el IEEE bajo la denominación IEEE 802.15.

Las principales características de esta forma de comunicación son:

- Opera en la banda libre de los 2,4 GHz.
- Tiene una capacidad máxima de transmisión de hasta 3 Mbps.
- Implementa diversos mecanismos de ahorro energético.
- Posee un precio económico que permite implementarlo en casi cualquier dispositivo sin encarecerlo desmesuradamente. Un sistema Bluetooth empotrado tiene un precio cercano a 20 € y un adaptador USB (Universal Serial Bus) típico para ordenador, no más de 10 €.
- Alcance de hasta 100 metros en función de la potencia de emisión que posea el transmisor Bluetooth.

La red Bluetooth más pequeña, denominada *piconet*, puede incluir hasta 8 dispositivos, controlando el acceso al canal a través de un esquema de sondeo. La operación de esta red se basa en un esquema maestro-esclavo. Cada estación puede actuar de maestro, pero sólo una puede hacer este papel en cada momento. Debido a los saltos de frecuencia, la transmisión entre maestro y esclavo estará basada en *slots* de 625 µs. Por tanto, si no hay retransmisiones, el sondeo de un nodo esclavo requiere 1250 µs. En una situación ideal, el ciclo de sondeo de mayor duración es de 8.75 ms (esto es, 7 dispositivos), lo que satisface el requisito de mantener los tiempos de comunicación en varios cientos de milisegundos de algunas aplicaciones.

Este protocolo de comunicaciones queda restringido para enlaces punto a punto, puesto que el sistema de establecimiento de conexiones hace difícil la realización redes punto-multipunto, debido principalmente a que desde un principio estaba destinado a sustituir a los enlaces establecidos mediante un cable físico.

Sus mayores problema a la hora de utilizarlo en sensores dentro de un automóvil son su coste, complejidad y consumo de energía.

3.1.5 Ultra Wide Band

Se corresponde con una tecnología de comunicación inalámbrica conocida hace muchos años en el mundo de la investigación y militar. La principal característica de las redes UWB (*Ultra Wide Band*) es que permite obtener enlaces con una gran capacidad de transmisión, consumiendo muy poca potencia. Esto se consigue transmitiendo señales en el dominio del tiempo de muy corta duración. El periodo de estas señales es del orden de unos pocos nanosegundos. Se pueden tener grandes anchos

de bandas en las señales transmitidas, lo que conlleva considerables beneficios en cuanto al consumo y a la capacidad de transmisión.

El despegue de esta tecnología se produjo en 2002 cuando el organismo estadounidense FCC (*Federal Communications Commission*) permitió el uso de la banda ubicada entre 3.6 GHz y 10.1 GHz. Este acontecimiento provocó que numerosos centros de investigación, gobiernos y la industria de las telecomunicaciones investigaran posibles aplicaciones. Entre ellas, cabe citar:

- acceso a Internet de banda ancha a muy alta velocidad
- localización con precisión de centímetros
- imágenes de radar de alta resolución
- obtención de imágenes a través de paredes
- navegación y seguimiento de objetos de forma precisa

El principal inconveniente de esta tecnología es que sólo se puede utilizar en un corto rango de espacio, cercano a los 10 metros de cobertura. Esto está motivado por los niveles tan bajos de potencia que la FCC estableció para UWB. En concreto, la máxima potencia de salida de un transmisor UWB es de 0.0001 mW/MHz lo que supone que para un ancho de banda típico de 500 MHz se tenga una potencia de salida de 0.05 mW, valor que se encuentra muy por debajo de la máxima potencia permitida, por ejemplo, en el caso de IEEE 802.11b (100 mW).

3.1.6 ZigBee

ZigBee se corresponde con una especificación global creada por un consorcio de múltiples marcas (*ZigBee Alliance*) destinadas a la venta de sistemas de control inalámbrico. Dicha especificación se basa en el estándar IEEE 802.15.4 [13] definido por IEEE donde se especifica la capa física y de enlace del protocolo. En cuanto a los niveles superiores, *ZigBee Alliance* se encarga de establecer el conjunto de reglas que deben cumplir las capas de red, aplicación, el framework de aplicación, los perfiles y los mecanismos de seguridad.

La idea principal sobre la que se ha desarrollado ZigBee ha sido la facilidad a la hora de implementarlo en un sistema de control, o lo que es lo mismo, se busca que de una manera sencilla y rápida se pueda desarrollar un sistema robusto y duradero, fácilmente integrable en una red inalámbrica destinada a la supervisión y el control. Por este motivo, ZigBee pretende cumplir los siguientes objetivos:

- alta fiabilidad
- bajo coste
- muy bajo consumo
- alta seguridad
- apertura del estándar

En consecuencia, para poder satisfacer todos estos puntos, el estándar ZigBee se caracterizar por:

- Baja capacidad de transmisión, en torno a 250 Kbps, lo que permite desarrollar sistemas de muy bajo coste.

- Protocolo sencillo, pudiendo ser implementado sin ningún tipo de limitación en sistemas microcontroladores de 8 bits.
- Muy bajo consumo energético que permite que la fuente de alimentación del sistema pueda durar años.

Como gran desventaja, se puede mencionar la baja capacidad de transmisión adoptada, lo que restringe el uso de esta especificación para usos muy concretos y actividades que requieran poco intercambio de datos, como accionar un interruptor de la luz o monitorizar un sensor de temperatura o luminosidad. En cualquier caso, se puede decir que es una de las soluciones más prometedoras para cualquier tipo de sensores inalámbricos.

3.1.7 WiMAX

Se trata de una estándar de comunicaciones cuyo principal objetivo consiste en dar servicios de banda ancha de una forma inalámbrica a áreas metropolitanas, es decir, está pensado para ser usados en redes MAN. Por este motivo, se desarrolló para cubrir distancias de hasta 50 Km y permitir una capacidad de transmisión de hasta 100 Mbps. Con estas características, esta tecnología podría hacer frente a otras como DSL y las líneas T1 tendidas en el bucle de abonado. WiMAX se corresponde con el nombre con el que se comercializa a tecnología basada en el estándar IEEE 802.16 [14].

La idea fundamental de WiMAX se centra en poder dar una gran variedad de servicios, motivado por el bajo coste de los enlaces, que pueden ir desde actuar como backbone para redes IEEE 802.11, dar servicios de conexión a dispositivos móviles sin hacer uso del estándar IEEE 802.11, como red de respaldo de las redes cableadas.

Entre las principales características de WiMAX se encuentran las siguientes:

- Dos rangos de frecuencias para operar:
  - 10GHz-66 GHz: se corresponde con la banda asignada en la primera versión del estándar. El principal problema de este rango es que requiere visión directa entre las distintas estaciones para poder llevar a cabo la comunicación, provocando el encarecimiento de la instalación al tener que aumentar el número de estaciones que se coloque.
  - 2GHz-11 GHz: en esta banda se establecen dos rangos, uno en los 3,5 GHz que requiere de licencia para poder transmitir y otro en los 5,8 GHz que se encuentra en la banda libre y, por tanto, no se necesitaría ningún tipo de licencia.
- Uso de selección dinámica de la frecuencia de utilización. Esta técnica permite seleccionar la frecuencia de transmisión en base a las interferencias generadas por otros sistemas en la banda usada y por la interferencia con canales adyacentes, permitiendo ajustar la potencia de transmisión en base a estos parámetros. De esta forma, consigue mejorar el rendimiento de la comunicación.
- Es útil en redes punto-multipunto.
- Asignación de una determinada calidad de servicio a cada conexión, lo que permite poder transportar sobre la capa de enlace de WiMAX protocolos como ATM, IPv4, IPv6.

Finalmente, cabe mencionar que en 2005, el IEEE aprobó el estándar IEEE 802.16e en el que se definen redes de banda ancha móviles usando WiMAX como capa física y de enlace.

A continuación se compararán las distintas tecnologías vistas, mostrando sus principales características en la Tabla 2.1.

Tecnología	Velocidad (Mbps)	Alcance (m)	Potencia (mW)	Ancho de banda (MHz)
ZigBee	0,03	10-100	30	0,6
Bluetooth	1-3	1-100	100	1
IEEE 802.11a	54	100	1500	20
IEEE 802.11b	11	100	750	22
IEEE 802.11g	54	100	1000	20
IEEE 802.11n	200	100	2000	40
IEEE 802.11p	27	100	1500	10
UWB	200	10	400	500

Tabla 3.2: Comparativa entre tecnologías inalámbricas

3.2 El estándar Bluetooth

El estándar Bluetooth [15] nació en 1994 cuando la empresa Ericsson se interesó en conectar sus teléfonos móviles y otros dispositivos (por ejemplo, PDAs) sin necesidad de cables. Posteriormente formó con otras empresas (Intel, IBM, Toshiba y Nokia) el SIG (*Bluetooth Special Interest Group*), que se encargó de formalizar las especificaciones. Al proyecto se le asignó el nombre Bluetooth, en honor al rey vikingo Harald Blåtand (940 – 981 DC) quien unificó distintas tribus danesas en un mismo reino. La analogía es que Bluetooth hace lo mismo con los protocolos de comunicación, uniéndolos en un mismo estándar. Las primeras versiones (1.0 y 1.0b) tenían muchos problemas de interoperabilidad, dificultando la creación de conexiones entre dispositivos. Estos problemas fueron resueltos en versiones siguientes de la especificación (1.1 y 1.2). La versión 2.0, entre otras cosas, introdujo soporte para una tasa de transmisión mejorada, y la 3.0 para una capa MAC/física alternativa (802.11). Actualmente, la especificación actual ha alcanzado la versión 4.0 (*Bluetooth Low Energy*), dirigido a dispositivos con baja capacidad de batería.

Actualmente se tiene una gran cantidad de dispositivos personales que soportan la tecnología Bluetooth, tales como ordenadores, teléfonos celulares, auriculares, PDAs, etc. Normalmente, en estos dispositivos se utiliza para la sincronización de datos, intercambio de archivos, mensajes y juegos. Es en los teléfonos celulares y ordenadores portátiles donde se ve especialmente la aceptación e integración del estándar Bluetooth.

3.2.1 La pila de protocolos Bluetooth

Hay tres modelos de implementación de la pila de protocolos, atendiendo a la funcionalidad o los recursos que el dispositivo posee, estas son: *hosted* (anfitrión), *embedded* (empotrado) y *fully embedded* (totalmente empotrado). Estos modelos se diferencian por el lugar donde se implementan las diferentes capas, que corresponden a la pila que se puede observar en la Figura 3.2.

En el modelo *hosted*, las capas más bajas residen en el dispositivo Bluetooth mientras que las capas superiores se encuentran en el dispositivo anfitrión, que puede ser un PC o un microcontrolador si el dispositivo es independiente (*standalone*). Éstos se comunican mediante la interfaz HCI (*Host Controller Interface*), situada entre las capas superiores e inferiores de la pila de protocolos formando un puente. Este modelo es óptimo cuando se tiene un procesador potente y se dispone de mucha memoria.

En el modelo embedded, toda la pila reside en el dispositivo Bluetooth pero la aplicación del usuario se ejecuta fuera, en el anfitrión (*host*). Este modelo es ideal para los teléfonos móviles, máquinas expendedoras de tickets o periféricos de computadoras con limitaciones de procesador y memoria.

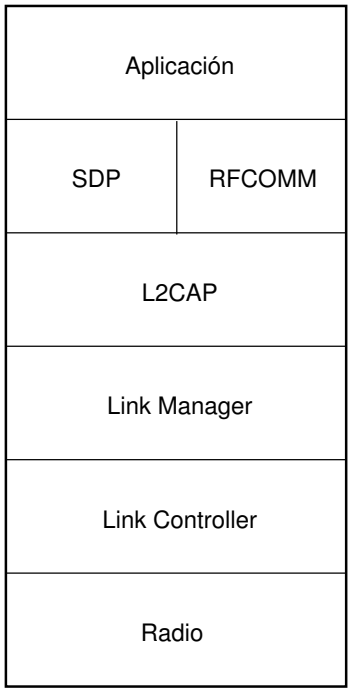

Figura 3.2: Pila de protocolos Bluetooth

El modelo fully embedded, la pila y la aplicación del usuario se encuentra en el dispositivo Bluetooth. Generalmente los dispositivos de este tipo tienen recursos de memoria limitada, lo que implica que las aplicaciones deben ser simples. El mejor ejemplo de un dispositivo completamente empotrado es un auricular Bluetooth.

A continuación se describirán las diferentes capas del protocolo y se analizará con detalle el funcionamiento de las comunicaciones Bluetooth.

3.2.2 Radio Bluetooth

Los sistemas Bluetooth operan en la banda ISM (*Industrial, Scientific and Medical*) de los 2.4 Ghz, específicamente entre 2400 y 2483.5 MHz, siendo libre en la mayoría de los países del mundo y como son de uso no comercial, no requieren de licencia. El sistema de radio hace uso de una técnica denominada espectro ensanchado por salto de frecuencia (FHSS), que consiste en dividir toda la banda de frecuencia en diversos canales y saltar de uno a otro durante la conexión. En el caso de Bluetooth estas frecuencias vienen dadas por:

$$f = (2402 + n)\text{MHz}, n = 0, 1, ..., 78$$

La secuencia básica de salto consiste en un ordenamiento pseudoaleatorio de estas 79 frecuencias, además se utiliza una banda de guarda en los extremos inferior y superior de la gama de frecuencias, de 2 MHz y 3,5 MHz respectivamente. La secuencia de salto puede adaptarse para excluir una sección de frecuencias utilizadas por los dispositivos que están causando interferencias. La técnica de salto adaptable mejora la coexistencia de la tecnología Bluetooth con los sistemas ISM estáticos (es decir, sin salto) cuando éstos se encuentran localizados.

Se definen dos modos de modulación; un modo obligatorio, llamado modo de transferencia básica, que usa una modulación GFSK (un par de frecuencias diferentes para 1 y 0, con un filtrado previo

de la información en banda base por un filtro gaussiano) para reducir al mínimo la complejidad del transmisor/receptor. Y otro modo opcional (desde la versión 2.0), llamado de transferencia de datos mejorada (EDR, *Enhanced Data Rate*), que usa modulación PSK y cuenta con dos variantes: π/4-DQPSK y 8DPSK. La tasa de transferencia de símbolos de todas las secuencias de modulación es de 1 M muestras/s. La velocidad de transmisión total es de 1 Mbps con el modo de transferencia básica; 2 Mbps con la transferencia de datos mejorada y π/4-DQPSK; y 3 Mbps con la transferencia de datos mejorada y 8DPSK.

Los dispositivos se clasifican según su potencia de transmisión en tres tipos. Los dispositivos de clase 1 disponen de control de potencia obligatorio. Dicho control de potencia se usa para limitar la potencia transmitida por encima de los 4 dBm. Por debajo de 4 dBm, la capacidad para controlar la potencia es opcional, y puede emplearse para controlar el consumo energético y el nivel global de interferencias. Los dispositivos con capacidad para controlar la potencia usan comandos LMP (*Link Manager Protocol*) para optimizar la potencia de salida en un enlace físico. Esto se consigue midiendo la RSSI (*Received Signal Strength Indication*) y comunicando si la potencia de transmisión debe aumentarse o reducirse según ese valor.

En la Tabla 3.3 se muestran las características de los tres tipos de dispositivos Bluetooth según la potencia.

Clase	Potencia de salida máxima	Potencia de salida nominal	Potencia de salida mínima	Control de potencia
1	100 mW (20 dBm)	No especifica	1 mW (0 dBm)	4dBm < Ptx < Pmax Opcional:Pmin < Ptx < Pmax
2	2,5 mW (4 dBm)	1 mW (0 dBm)	0,25 mW (-6 dBm)	Opcional: Pmin < Ptx < Pmax
3	1 mW (0 dBm)	No especifica	No especifica	Opcional: Pmin < Ptx < Pmax

Tabla 3.3: Clases de dispositivos Bluetooth

3.2.3 Gestor de enlaces

El gestor de enlaces se ocupa de la creación, modificación y liberación de enlaces lógicos (y, en caso de ser necesario, de la comunicación lógica asociada), así como de la actualización de los parámetros relacionados con los enlaces físicos entre dispositivos. Para ello, se comunica con el gestor de enlaces del dispositivo Bluetooth remoto mediante el protocolo de gestión de enlace (LMP).

Este protocolo permite la creación de nuevos enlaces y comunicaciones lógicos entre los dispositivos cuando resulta necesario, así como un control general de las características de los enlaces y la comunicación, tales como la activación del cifrado de la comunicación lógica, la adaptación de la potencia de transmisión en el enlace físico o el ajuste de los parámetros QoS para enlaces lógicos.

3.2.4 Controlador de enlaces

El controlador de enlaces se ocupa del cifrado y decodificación de los paquetes Bluetooth de la carga útil de datos y los parámetros relacionados con el canal físico, la comunicación lógica y los enlaces lógicos.

Sincronizado con el gestor de recurso, el controlador de enlaces lleva a cabo la señalización del protocolo de control de enlace, que se utiliza para las comunicaciones del control de flujo y confirmación, así como para la retransmisión de señales solicitadas. La interpretación de estas señales es

una característica de la comunicación lógica asociada al paquete de banda base. La interpretación y supervisión de la señalización de control de los enlaces se suele asociar al programador del gestor de recursos.

3.2.5 Definición de canales

El canal físico se subdivide en unidades de tiempo denominadas ranuras (*slots*) de 625 µs de duración. Los datos intercambiados entre los dispositivos Bluetooth se transmiten en forma de paquetes que se emplazan en estos *slots*. Cuando la situación lo permite, se pueden asignar varias ranuras consecutivas a un único paquete. Para cada uno de estos *slots* se hace un salto de frecuencia, lo que conlleva una tasa de 1600 saltos/s. Transmisión y recepción se alternan en estos *slots*, lo que da lugar en conjunto a una técnica de acceso múltiple y dúplex por división en el tiempo (TDD y TDMA). Este mecanismo de transmisión se puede observar en la Figura 3.3.

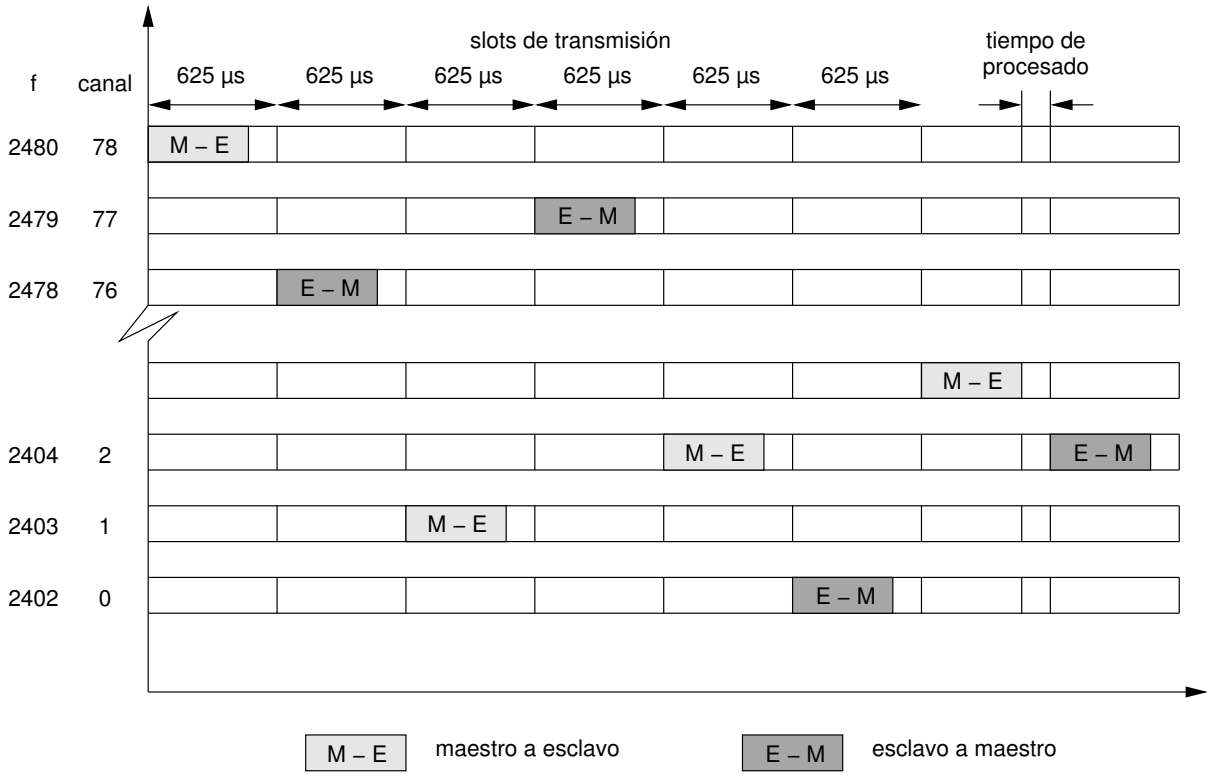

Figura 3.3: Duplex por división en el tiempo y saltos de frecuencia en Bluetooth

Un canal físico Bluetooth se entiende como una secuencia de saltos en frecuencia y una fase dentro de esta secuencia, que sirven para determinar la frecuencia a utilizar en cada *slot*. Dos o más unidades utilizando un mismo canal forman una *piconet*. Una unidad actúa como maestro, controlando todo el tráfico de esta red, siendo el resto de unidades esclavos. La secuencia de saltos se calcula a partir de la identidad del maestro y la fase se calcula a través del reloj del maestro. Para recrear el reloj del maestro, los esclavos pueden añadir un desfase a su propio reloj (Figura 3.4). Si todos los participantes de un determinado canal usan la misma identidad y reloj como entrada al sistema de selección de frecuencia, se mantendrán sincronizados.

El maestro sólo puede transmitir en determinados *slots*, y la respuesta de un esclavo sólo puede emplazarse en el *slot* inmediatamente posterior. Un esclavo sólo puede transmitir si fue direccionado por el maestro en el *slot* anterior.

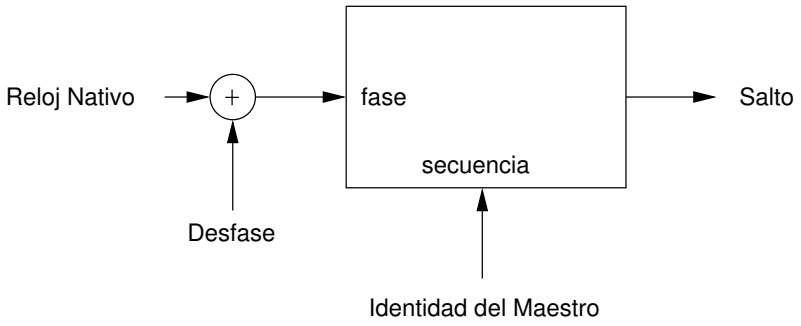

Figura 3.4: Mecanismo de selección de saltos en Bluetooth

3.2.6 Paquetes

En las Figuras 3.5 y 3.6 se muestran los paquetes en cada unos de los modos de modulación: el básico y el mejorado, respectivamente, los cuales se emplazan en los diferentes *slots*. En el modo de transferencia básico cada paquete contiene tres partes: el código de acceso, la cabecera y la carga útil.

Figura 3.5: Formato del paquete básico

El paquete de transferencia de datos mejorada consta de seis entidades: el código de acceso, la cabecera, el periodo de guarda, la secuencia de sincronización, la carga útil de la transferencia de datos mejorada y la cola o *trailer*. El código de acceso y el encabezamiento usan la misma secuencia de modulación que los paquetes del modo de transferencia básico, en tanto que la secuencia de sincronización, la carga útil de la transferencia de datos mejorada y la cola usan la secuencia de modulación de la transferencia de datos mejorada

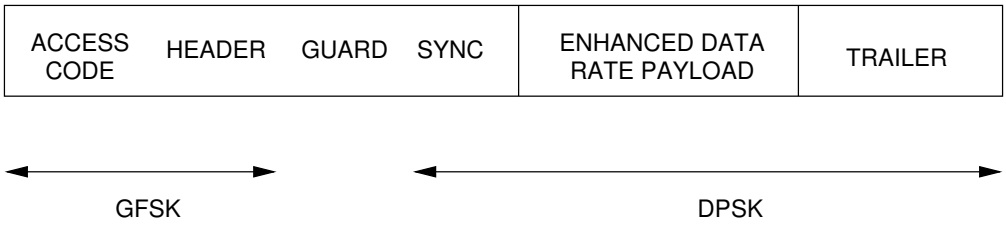

Figura 3.6: Formato del paquete de datos mejorado

El código de acceso se deriva de la identidad del maestro y es único para cada canal. Cada paquete que se intercambia en una *piconet* está precedido por este código de acceso, que además se utiliza para sincronización y compensación del desplazamiento en frecuencia. Los receptores de cada *piconet* comparan el código de acceso del código recibido con el de su canal, rechazándolo si no coincide. Se definen tres códigos diferentes:

- código de acceso del dispositivo (DAC)
- código de acceso del canal (CAC)
- código de acceso de consulta (IAC)

Todos los códigos de acceso se derivan del campo LAP de la dirección de dispositivo o de una dirección de búsqueda. El código de acceso del dispositivo se utiliza en el estado *Page* (paginación). El código de acceso al canal se utiliza en el estado *Connection* (conexión) y constituye el comienzo de todos los paquetes intercambiados en el canal físico de una *piconet*, como ya se ha comentado. El código de acceso del canal será es derivado de la dirección Bluetooth del dispositivo maestro. Por último, el código de acceso de búsqueda será utilizado en el estado *Inquiry* (búsqueda). Hay un IAC general (GIAC) para las operaciones de búsquedas de carácter general y hay 63 IACs dedicados (DIACs) para las operaciones de búsqueda dedicada. Estos diferentes estados se explican en una de las siguientes secciones junto con el establecimiento de conexiones.

La cabecera que sigue al código de acceso contiene informaciones importantes de control, como una dirección de 3 bits que identifica a cada esclavo dentro de la *piconet*, denominado LT_ADDR (esta identificación es diferente a la dirección del dispositivo, la cual sólo se usa con el propósito de coordinar o formar una *piconet*); bits de control de flujo, y bits para la implementación del esquema de retransmisión automática. El éxito en la transmisión de un paquete se indica en la cabecera del paquete de retorno. Esta cabecera también sirve para definir paquetes *multislot* (1, 3 o 5 *slots*). Durante la transmisión de un paquete multi*slot* se mantiene la misma frecuencia, haciendo el salto al final del último *slot*.

3.2.7 Dirección de dispositivos Bluetooth

A cada dispositivo Bluetooth se le asigna una dirección de dispositivo Bluetooth única de 48-bit proporcionada por la autoridad reguladora de IEEE. Ésta se divide en tres campos que se muestran en la Figura 3.7 y que son los siguientes:

- LAP (*Lower Address Part*): parte baja de la dirección Bluetooth de 24 bits.
- UAP (*Upper Address Part*): parte alta de la dirección Bluetooth de 8 bits.
- NAP (*Non-significant Address Part*): parte no significativa de la dirección Bluetooth de 16 bits.

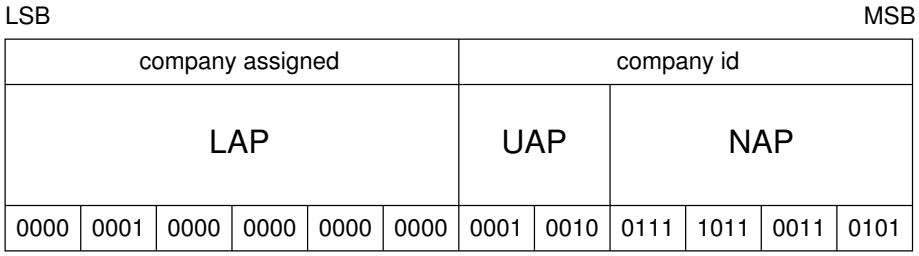

Figura 3.7: Formato de direcciones Bluetooth

Hay un grupo contiguo de sesenta y cuatro LAPs reservadas para operaciones de descubrimiento, un LAP común para todos los dispositivos reservada para la búsqueda general y 63 reservada para la búsqueda dedicada para clases de dispositivos específicos. Las direcciones LAP reservadas van desde 0x9E8B00 hasta la 0x9E8B3F y para la búsqueda general el LAP es 0x9E8B33.

3.2.8 Definición de enlaces

Se definen cinco tipos de enlaces para soportar aplicaciones multimedia en las que se mezclan voz y datos:

- enlaces síncronos orientados a conexión del usuario (SCO-S, *Synchronous Connection-Oriented*)
- enlaces síncronos ampliados (eSCO-S)
- enlaces asíncronos del usuaruo (ACL-U, *Asynchronous Connectionless Link*)
- control del enlace (LC)
- control ACL (ACL-C)

Además de estos enlaces lógicos, se definen enlaces físicos, que no son más que una conexión entre dispositivos dentro de un mismo canal físico con características comunes de aspectos como el cifrado o el control de energía. También se definen cinco tipos de comunicaciones lógicas para servir de transporte a los enlaces lógicos:

- por conexión síncrona (SCO)
- por conexión síncrona ampliada (eSCO)
- por conexión asíncrona (ACL)
- por difusión del dispositivo esclavo activo (ASB)
- por difusión del dispositivo esclavo en espera (PSB)

Los enlaces lógicos de control LC y ACL-C se usan al nivel del control de enlaces y del gestor de enlaces, respectivamente. El enlace lógico ACL-U se utiliza para transmitir información síncrona o asíncrona del usuario. Los enlaces lógicos SCO-S y eSCO-S se usan para transmitir información síncrona del usuario. El enlace lógico LC se transmite en la cabecera del paquete, todos los demás enlaces lógicos se transmiten en la carga útil del paquete. Los enlaces lógicos ACL-C y ACL-U están indicados en el campo de la ID del enlace lógico (LLID) en la cabecera de la carga útil. Los enlaces lógicos SCO-S y eSCO-S son transmitidos exclusivamente por las comunicaciones lógicas síncronas; el enlace ACL-U se transmite normalmente por la comunicación lógica ACL; sin embargo, también puede ser transmitido por los datos del paquete DV de la comunicación lógica SCO. El enlace ACL-C puede transmitirse por cualquiera de las dos comunicaciones lógicas SCO o ACL.

Las comunicaciones SCO soportan transmisiones simétricas punto a punto, de forma muy similar a una red de conmutación de circuitos. En la práctica se implementa a través de la reserva de determinados *slots* para esta comunicación. Las comunicaciones ACL soportan comunicaciones simétricas o asimétricas basadas en conmutación de paquetes. Todo el tráfico ACL y SCO es planificado por el maestro. Una comunicación ACL (y por tanto enlaces de control y datos) está presente durante todo el tiempo de existencia de la *piconet*, ya que se crea una predeterminada cuando un dispositivo se conecta (para utilizarla simplemente hay que transmitir datos en el *slot* adecuado cada vez que el maestro se comunique con el dispositivo). Las comunicaciones (enlaces) SCO deben ser configuradas previamente.

La especificación Bluetooth 1.1 define los enlaces ACL y SCO como enlaces físicos. No obstante, con la incorporación del enlace SCO ampliado (eSCO) y puestos a considerar futuras ampliaciones, resulta más conveniente tratar estos enlaces como lógicos ya que este tipo obedece mejor a su finalidad. A través de estos enlaces lógicos, además de los datos del usuario se transporta el protocolo de control de la banda base y las capas físicas: se trata del protocolo de gestión de enlace (LMP). Los dispositivos que están activos dentro de la *piconet* tienen una comunicación lógica asíncrona predeterminada para el transporte de la señalización del protocolo LMP. Esta comunicación es la que se

establece cuando un dispositivo se une a una *piconet*. Se pueden crear comunicaciones lógicas adicionales si resulta necesario para transportar el flujo de datos síncronos.

El gestor de enlaces se sirve del protocolo LMP para controlar el funcionamiento de los dispositivos en la *piconet* y proporcionar servicios de gestión en las capas inferiores de la arquitectura: capa de radio y de banda base. El protocolo LMP sólo se transporta a través de la comunicación lógica ACL y la comunicación lógica de difusión predeterminadas.

La denominación de los enlaces lógicos se realiza añadiendo a la comunicación lógica asociada un sufijo que indica el tipo de datos que se están transfiriendo: C para enlaces de control que transportan mensajes LMP, U para enlaces L2CAP que transfieren datos del usuario (unidades PDU de la capa L2CAP) y S para enlaces de flujo que transmiten datos síncronos o isócronos sin formato. Resulta habitual eliminar el sufijo del enlace lógico sin que se induzca a error. Puede entenderse que una referencia al enlace lógico ACL significa un enlace lógico ACL-C cuando se trate del protocolo LMP, o un enlace lógico ACL-U cuando se esté en el contexto de la capa L2CAP.

El enlace lógico ACL-C se diferencia del ACL-U (que transporta datos L2CAP y de usuario) mediante el campo identificador de enlace lógico (LLID) que se transmite junto antes de la carga. En ACL-C tiene mayor prioridad que el resto del tráfico. Una forma más simple de ver todo esto es considerar que el maestro simplemente identifica a un esclavo al que quiere transmitir datos asíncronos a través del campo LT_ADDR (*Logical Transport ADDRess*) y el campo LLID indica si se trata de datos de la capa L2CAP o datos de control LMP.

La comunicación lógica SCO reserva ranuras en el canal físico, por lo que puede considerarse una conexión de conmutación entre el maestro y el esclavo. Este tipo de comunicación transfiere información sincronizada con el reloj de la *piconet* a una velocidad de 64 Kbps. (por lo general, un flujo de datos de voz codificado) Existen tres configuraciones SCO para nivelar los parámetros de fiabilidad de la señal, demora y consumo de ancho de banda.

Cada enlace lógico SCO-S se transmite por una comunicación lógica SCO simple, a la que se asignará el mismo campo LT_ADDR que el designado para la comunicación lógica ACL entre los dispositivos. Por ello, para identificar el destino de un paquete recibido no basta el campo LT_ADDR. Puesto que los enlaces SCO se sirven de ranuras reservadas, el dispositivo debe emplear las direcciones LT_ADDR, los números de ranura (propiedad del canal físico) y los tipos de paquetes para identificar las transmisiones realizadas en estos enlaces.

3.2.9 Establecimiento de conexiones

Esta sección describe cómo se establece una *piconet* y cómo los dispositivos pueden ser añadidos y liberado de la *piconet*. Se definen los estados de funcionamiento de los dispositivos para admitir estas funciones.

Hay tres estados principales: *STANDBY* (espera), *CONNECTION* (conexión) y *PARK* (aparcar), y siete subestados: *Page* (paginación), *Page Scan* (detección de paginación), *Inquiry* (búsqueda), *Inquiry Scan* (detección de búsqueda), *Master Response* (respuesta del maestro), *Slave Response* (respuesta del esclavo) y *Inquiry Response* (respuesta de la búsqueda). Los subestados son estados internos, que se utilizan para el establecimiento de 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 (como la señal desencadenante del correlador y las señales de expiración del tiempo de espera).

La formación de una *piconet* desde cero consta de tres fases:

1. *Inquiry* (búsqueda): durante esta fase el dispositivo inicia la búsqueda de dispositivos Bluetooth

en su entorno. Como resultado, las direcciones hardware de los dispositivos a los que es posible conectarse son descubiertas.

2. *Paging* (paginación): en esta fase se negocia la conexión. Principalmente comprende la información al esclavo del canal Bluetooth a utilizar y sincronizar su reloj.

3. *Connection* (conexión): una vez que la conexión ha sido establecida, los datos se pueden transmitir entre los distintos dispositivos.

Teniendo en cuenta que los saltos en frecuencia de los transceptores de radio Bluetooth dificultan la coicidencia en un mismo canal de dos dispositivos que todavía no se han coordinado, el procedimiento para que un nodo A descubra a otro nodo B no es completamente trivial.

Para que B pueda ser descubierto, éste entra regularmente en un estado denominado *inquiry scan* durante 10.625 ms. Durante este estado el dispositivo permanece a la escucha buscando paquetes con el código de acceso definido para este procedimiento, el cual no se corresponde con el de ninguna *piconet*. Los saltos en frecuencia se obtienen también a partir de este código de acceso específico y los últimos 4 bits del reloj del dispositivo, con lo cual únicamente se utilizan 32 en este caso. Cada vez que se entra al estado *inquiry scan*, lo cual se hace en un intervalo que va desde los 0 a los 2.56s (normalmente 1.28s), se produce un salto de frecuencia. Puesto que los saltos de frecuencia y un reloj determinan un canal, se suele hablar de un canal físico de búsqueda en este caso.

Para descubrir al dispositivo, A entra en el estado *inquiry*. En este estado A envía paquetes de búsqueda a diferentes frecuencias (por grupos de 16). Lo hace a una tasa de saltos que es el doble de la usual, esto es, colocando un par de paquetes en cada *slot* de 625 µs y escuchando posibles respuestas en los 625 µs siguientes. Esto implica un tiempo de 10 ms. Ambos dispositivos usan la misma secuencia de saltos, pero difieren en su fase. Ya que A debe permanecer varios segundos en estado inquiry enviando trenes de paquetes de búsqueda (normalmente 10.24 s), los dos dispositivos coincidirán en algún momento.

Una vez que B ha recibido el paquete de búsqueda, esperará un número aleatorio de *slots*. Este retraso aleatorio sirve para evitar colisiones con otros dispositivos que también pueden responder a la búsqueda. Tras ello, buscará el momento oportuno para transmitir, entrando en el estado *inquiry response* y volviendo a escuchar paquetes de búsqueda. Cuando se se alcanza sincronización de frecuencias (esto es, se recibe un nuevo paquete), se transmitirá una respuesta en el *slot* inmediatamente posterior que contendrá su dirección hardware y su reloj nativo, entre otras informaciones. La respuesta se envia a una frecuencia derivada de la frecuencia de recepción.

Usando la información recibida de B (dirección hardware y reloj), A iniciará un procedimiento de paginación para establecer una conexión. El procedimiento es similar al de búsqueda, salvo que en este caso se utiliza un código de acceso derivado de la dirección hardware de B. También se puede hablar de un canal de paginación en este caso. Cuando B entra en estado *page scan* (lo cual debe hacer también regularmente) y detecta uno de estos paquetes con su código de acceso, envía una respuesta a A, que contiene únicamente el código de acceso.

Tras recibir esta respuesta de B, A entra en el estado *master response*, durante el cual transmite su propia dirección hardware y su reloj. Tras la confirmación de B, la conexión queda establecida. A partir de este momento, ambos dispositivos utilizan la misma frecuencia de saltos. Además, se crea la comunicación ACL predeterminada entre el maestro y el esclavo y se asigna una dirección LT_ADDR de 3 bits al dispositivo.

Hay que destacar que la incertidumbre del proceso de búsqueda recae en el dispositivo que la inicia (A en este caso), lo cual requiere tiempo y un mayor gato de energía. Que el resto de unidades sólo escuchen durante pequeños intervalos mientras se encuentran en *standby* y no envíen ningún

tipo de baliza, es preferible para reducir su consumo y evitar interferencias innecesarias.

A la vista del procedimiento de búsqueda explicado, queda claro que éste debe prolongarse durante varios segundos.

3.2.10 Piconets y Scatternets

Las unidades Bluetooth que se encuentran en un determinado espacio establecen conexiones ad hoc usando procedimientos como el explicado en el apartado anterior. Para regular el tráfico del canal, una de estas unidades se convierte en maestro, como ya se ha comentado. Cualquier unidad se puede convertir en maestro, pero por definición, la unidad que inicia la paginación se convierte en él, siendo todos los demás participantes esclavos. Si alguna unidad quiere hacerse cargo del papel de maestro, existen procedimientos de intercambio maestro-esclavo.

En cualquier momento, sólo puede haber un maestro dentro de una *piconet*, ya que su identidad y reloj especifican el canal. Cuando se libera la *piconet*, los papeles de maestro y esclavo se pierden. Cada vez que un esclavo recibe un paquete del maestro con un código de acceso válido, reajusta su desplazamiento de reloj; el reloj nativo nuca se reajusta. El maestro regula el tráfico se la red estableciendo canales SCO o bien utilizando el mecanismo de planificación para los canales ACL de acuerdo a las necesidades de cada momento. Como se ha comentado también anteriormente, un esclavo sólo puede transmitir en un *slot* cuando haya sido direccionado en el *slot* inmediatamente anterior por el maestro (exceptuando configuraciones multi*slot*).

Una *piconet* puede tener hasta siete dispositivos activos y hasta doscientos cincuenta y cinco dispositivos esclavos estacionados (modo de bajo consumo que será analizado más adelante).

Los usuarios de un mismo canal deben compartir la capacidad. Ya que ésta es de sólo 1 MHz, confome se añaden más dispositivos, puede caer rápidamente. El ancho de banda disponible es de 79 MHz, pero no puede ser utilizado efectivamente cuando todos los dispositivos deben utilizar uno de estos canales de 1 MHz debido al mecanismo de saltos. Para solucionar este problema, se permite que se puedan crear diversas *piconets* en un mismo área de cobertura. Estas *piconets* tienen secuencias de salto independientes y no están coordinadas. De esta forma, múltiples *piconets* tienen a su disposición todo el espectro de 79 MHz. En la Figura 3.8 se pueden apreciar las distintas configuraciones.

Una colección de varas *piconets* se denomina *scatternet*. La tasa de transmisión que ve cada dispositivo es superior a la que habría si todos los dispositivos participasen en la misma *piconet*. En cualquier caso, según aumenta el número de *piconets*, el rendimiento del sistema de saltos en frecuencia empieza a decaer notablemente.

La información que se intercambia en cada *piconet* es sólo compartida por sus participantes (gracias al mecanismo que establece el código de acceso que transporta cada paquete). En cualquier caso, se pueden establecer conexiones entre varias de ellas. Un dispositivo puede participar en diferentes *piconets*. Puede ser maestro en una de ellas y esclavo en otra (o varias), aunque sólo puede estar presente en un canal en cada instante. En este caso, se requiere una planificación muy cuidadosa.

3.2.11 Modos y procedimientos de operación

Modo conectado

Cuando el procedimiento de conexión se realiza correctamente, los dispositivos quedan físicamente conectados entre sí en una *piconet*. Esto significa que existe un canal físico de *piconet* al que están conectados, un enlace físico entre los dispositivos y enlaces lógicos ACL-C y ACL-U predetermi-

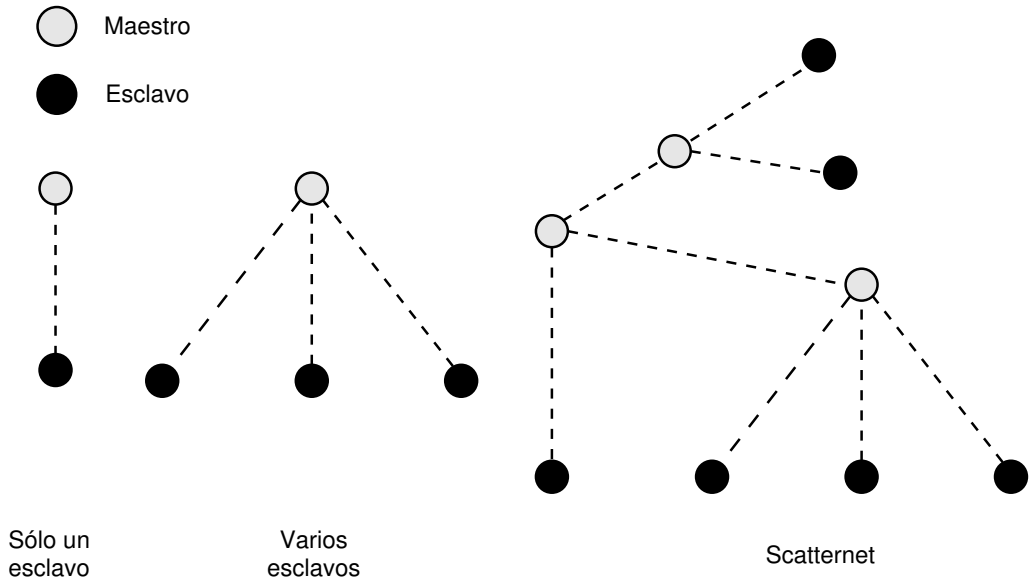

Figura 3.8: Diferentes configuraciones Bluetooth

nados. Una vez que la conexión está establecida, es posible crear y activar otros enlaces lógicos, así como cambiar los modos de los enlaces lógicos y físicos mientras los dispositivos siguen conectados al canal físico de la *piconet*. Además, se podrán realizar procedimientos de búsqueda, paginación o exploración, o bien conectarse a otras *piconet*s sin necesidad de abandonar la primera.

Los enlaces lógicos adicionales se crean mediante el gestor de enlaces, que intercambia los mensajes de su protocolo específico (LMP) con el dispositivo Bluetooth remoto a fin de negociar la creación y configuración de tales enlaces. Los enlaces lógicos ACL-C y ACL-U predeterminados se establecen siempre durante el proceso de conexión y se utilizan para los mensajes LMP y el canal de señalización L2CAP respectivamente.

Se ha advertido que cuando dos unidades se conectan a la vez, se crean dos enlaces lógicos predeterminados. Uno de estos enlaces (ACL-C) transporta el protocolo de control LMP, de forma que las capas superiores al gestor de enlaces no pueden detectarlo. El segundo enlace (ACL-U) se encarga del protocolo de señalización L2CAP y los canales de mejor esfuerzo L2CAP multiplexados. Resulta habitual remitirse a una comunicación lógica ACL predeterminada, y si bien puede resolverse en contexto, suele recurrirse al enlace lógico ACL-U predeterminado. Es necesario apuntar que estos dos enlaces lógicos comparten una comunicación lógica.

Mientras un dispositivo esclavo está conectado a una *piconet*, se produce una comunicación lógica ACL predeterminada entre el dispositivo maestro y esclavo. Existen dos métodos para eliminar esta comunicación. El primero consiste en desconectar el dispositivo del canal físico de la *piconet*, lo que ocasionará que desaparezca la jerarquía de los canales L2CAP, los enlaces lógicos y las comunicaciones lógicas que vinculan los dispositivos.

El segundo, en crear un enlace físico para que el dispositivo esclavo quede en modo park, es decir, a la espera; tras lo que se dará por concluida la comunicación lógica ACL predeterminada. Esto sólo es posible si se han dado por terminadas todas las comunicaciones lógicas, excepto la de difusión del dispositivo esclavo activo (comunicación ASB) que no puede crearse ni eliminarse directamente. Los dispositivos con comunicación lógica que no sean del tipo ACL ni ASB predeterminado no podrán quedarse en espera.

Cuando el enlace físico del dispositivo esclavo se deja en espera, se activa su comunicación lógica

ACL, y la comunicación lógica ASB se sustituye por una de difusión del dispositivo esclavo en espera (comunicación PSB). Los enlaces lógicos ACL-C y ACL-U multiplexados de la comunicación lógica ACL permanecen, pero no se pueden utilizar para la transferencia de datos. El gestor de enlaces del dispositivo maestro deja de utilizar mensajes LMP que puedan transmitirse por el enlace lógico PSB-C. El gestor de canales y el de recursos L2CAP comprueban que no se están enviando datos de unidifusión L2CAP al controlador mientras el dispositivo está en espera. El gestor de canales podrá actuar para dejar en espera o activar el dispositivo según resulte necesario para la transferencia de datos.

Modo hold o de retención

El modo de retención no suele ser habitual, aunque se aplica a las ranuras sin reservar el enlace físico. En este modo, el enlace físico sólo está activo cuando hay ranuras reservadas para el funcionamiento de los enlaces síncronos SCO y eSCO. Los enlaces asíncronos estarán inactivos. Los modos de retención funcionan una vez para cada llamada; terminada la llamada, se vuelve al modo anterior.

Modo sniff o de escucha reducida

El modo de escucha reducida no es genérico del dispositivo, sino que se aplica a las comunicaciones lógicas ACL predeterminadas, de forma que la disponibilidad de estas comunicaciones se puede modificar definiendo un ciclo de servicio compuesto por periodos de presencia y ausencia. Los dispositivos con comunicaciones lógicas ACL predeterminadas en modo de escucha reducida podrán utilizar los periodos de ausencia para conectarse a otro canal físico o para pasar al modo de ahorro de energía. Este modo sólo afecta a las comunicaciones lógicas ACL predeterminadas (comunicación lógica ACL compartida). Las comunicaciones lógicas SCO o eSCO activas no se verán afectadas. Las comunicaciones lógicas que se dan en el enlace físico del canal físico de la *piconet* propician periodos de presencia o ausencia para este enlace.

Las comunicaciones lógicas de difusión no tienen establecidos estados de presencia ni de ausencia. El dispositivo maestro debería programar las difusiones para que coincidan con los periodos de presencia del enlace físico dentro del canal físico de la *piconet*, aunque esto no siempre resulta posible ni práctico. La repetición de las difusiones se configura para mejorar las posibilidades de detección de varios esclavos sin solapar los periodos de presencia. No obstante, las comunicaciones lógicas de difusión no se pueden considerar fiables.

Modo de espera

Un dispositivo esclavo puede permanecer conectado a una *piconet* aun cuando su enlace físico se encuentre en estado de espera. En este estado, el dispositivo no puede admitir ningún enlace lógico que lo vincule al maestro, salvo por los enlaces lógicos PSB-C y PSB-U necesarios para la comunicación entre el maestro y el esclavo. Cuando el enlace físico dirigido a un dispositivo esclavo se aparta para quedar en espera, los parámetros de comunicación lógica PSB definen limitaciones para la comunicación entre maestro y esclavo. Cuando esta comunicación lógica está inactiva (o ausente), los dispositivos pueden conectarse a otros canales físicos o bien entrar en el modo de ahorro de energía.

3.2.12 Procedimiento de intercambio de funciones

El procedimiento de intercambio de funciones permite intercambiar las funciones de dos dispositivos conectados a una *piconet*. Para ello, es necesario pasar del canal físico definido por el dispositivo maestro original al canal físico que definirá el nuevo maestro. En este proceso de salto al nuevo canal, la jerarquía de enlaces físicos y comunicaciones lógicas se elimina para, a continuación, volverse a establecer; no así las comunicaciones lógicas ASB y PSB implícitas de la topología, que no se mantendrán. Tras el intercambio de funciones, el canal físico original de la *piconet* podrá dejar de existir o seguir activo, si hay dispositivos esclavos que siguen conectados al canal del maestro original.

En el nuevo canal sólo se copian los enlaces lógicos ACL predeterminados y las capas compatibles. Si es necesario copiar otros enlaces lógicos de comunicación, deberá hacerse en capas superiores. Las direcciones de comunicación lógicas (LT_ADDR) de las comunicaciones afectadas podrían no conservarse si el nuevo canal físico utiliza estos valores.

Los valores de calidad de servicio (QoS) o los modos establecidos (como el de escucha reducida) en las comunicaciones lógicas originales se pierden tras el intercambio de funciones y tendrán que volver a negociarse una vez completada la operación.

3.2.13 Transferencia de datos mejorada (EDR)

La transferencia de datos mejorada (EDR) es un método que amplía la capacidad y los tipos de paquetes Bluetooth para aumentar el rendimiento máximo, ofrecer mayor compatibilidad para las conexiones múltiples y rebajar el consumo de energía, sin que se produzcan cambios en el resto de la arquitectura.

Se puede establecer para que funcione de forma independiente en cada comunicación lógica. Una vez activada, los bits del paquete de la cabecera se interpretan de modo distinto a cuando operan en el modo de transferencia básico. Este cambio de interpretación se aprecia en el campo de la dirección de comunicación lógica de la cabecera. Como resultado, la cabecera y la carga útil se reciben y demodulan según el tipo de paquete. La EDR sólo puede activarse para las comunicaciones lógicas ACL-U y eSCO-S. No así para las ACL-C, SCO-S ni las comunicaciones lógicas de difusión.

El amplio rango de posibles aplicaciones Bluetooth implica que debe haber diferentes capas software. En los apartados anteriores se han dado las características de las placas inferiores (Radio, Link Controller y Link Manager) y se han dado algunos detalles de su funcionamiento. Estas capas pueden proporcionar conexiones de voz y un sólo caudal de datos entre dos dispositivos Bluetooth. Para facilitar la integración de Bluetooth en las aplicaciones existentes, las capas intermedias intentan ocultar algunos detalles complejos de las comunicaciones inalámbricas. Combinadas, estas capas pueden tomar diversos tipos de datos, multiplexarlos, empaquetarlos y pasarlos a las capas inferiores. Las capas equivalentes en el dispositivo receptor se encargarán de realizar las operaciones inversas.

3.2.14 Bluetooth de bajo consumo

Esta reciente versión permitirá que los dispositivos que hagan uso de ella consuman una fracción de la energía de otros dispositivos Bluetooth. En muchos casos, podrán operar hasta un año con una pila de botón sin necesitar ninguna recarga. De esta forma, será posible que pequeños sensores operen continuamente. Se presenta como una pila de protocolos adicional, compatible con otras pilas Bluetooth ya existentes. Se puede decir que es comparable a otras soluciones como ZigBee.

3.2.15 Protocolos de capas superiores

En este apartado se comentan varios protocolos de importancia situados por encima del gestor de enlaces (*Link Manager*).

L2CAP

El denominado *Logical Link Control and Adaptation Protocol* multiplexa datos de las capas superiores en un solo enlace ACL, y lo dirige al esclavo apropiado en caso de que el dispositivo transmisor sea el maestro de la *piconet*. Se encarga de pasar paquetes al interfaz HCI (esto es, el llamado *Host Controller Interface*, que conecta las capas superiores con las inferiores en el caso de una implemetación Bluetooth de tipo *hosted*) o bien directamente a la capa *Link Manager*.

Localmente, cada canal lógico L2CAP consta de un identificador (CID, *Channel IDentifier*), que no debe coincidir necesariamente con el del dispositivo remoto. Las capas situadas por encima de L2CAP pueden ser identificadas por un valor PSM (*Protocol Service Multiplexor*). Puede haber varios canales abiertos transportando los mismos datos PSM; y cada capa definida sobre L2CAP tiene su propio PSM, por ejemplo:

- SDP - 0x0001
- RFCOMM 0x0003

L2cap sólo trata con tráfico de datos, no voz. Otras de sus funciones son:

- Segmentar paquetes.
- Proporcionar mecanismos multicast para dirigir datos a un grupo de dispositivos.
- Gestionar la calidad de servicio (QoS) para protocolos superiores.

En modo básico, L2CAP proporciona paquetes con una carga de hasta 65 kB, siendo 672 bytes la MTU por defecto. Opcionalmente puede configurarse para transmisiones fiables o isócronas a través de retransmisiones y chequeos de CRC, auque esta fiabilidad también está adicionalmente garantizada por capas inferiores.

EL2CAP añade el modo de transmisión mejorado a la especificación.

RFCOMM

RFCOMM emula una comunicación serie RS232 a través de un canal L2CAP. Se basa en el estándar TS 07.10 para emulación software del interfaz hardware RS232. TS 07.10 incluye la capacidad para multiplexar varias conexiones serie emuladas en una sola conexión de datos utilizando diferentes DLCIs (*Data Link Connection Identifier*) para cada puerto. Sin embargo, cada sesión TS 07.10 puede sólo conectar a traves de un único canal L2CAP y por tanto comunicarse con un solo dispositivo. Un maestro debe tener sesiones RFCOMM separadas para cada esclavo que requiera una conexión serie.

En la versión 1.1 del protocolo Bluetooth se añadieron capacidades de control de flujo, dirigida a dispositibos de baja capacidad que deben cortar el flujo de datos en determinado momento.

BNEP

BNEP se utiliza para entregar paquetes de red sobre L2CAP. El protocolo se utiliza por el perfil de red de área personal (PAN, *Personal Area Networking*).

SDP

Este protoclo (*Service Discovery Protocol*) difiere de todos los demás situados por encima de L2CAP en que su objetivo es solicitar información sobre el propio sistema Bluetooth. Esta información son los servicios que soporta un determinado dispositivo. La capa SDP actúa como una base de datos de servicio, siendo la aplicación local la encargada de registrar los servicios disponibles y mantenerlos actualizados. Los dispositivos remotos pueden dirigirse a esta base de datos para descubrir qué servicios están disponibles y cómo conectarse a ellos.

Por ejemplo, SDP podría ser utilizado para determinar qué perfiles Bluetooth están soportados por unos auriculares y las configuraciones del multiplexor de protocolos necesarias para conectarse a cada uno de ellos. Cada servicio se define por un identificador universal único (UUID, *Universally Unique Identifier*)

3.2.16 Uso de servicios Bluetooth

Diferentes etapas deben ser completadas antes de que se pueda utilizar un servicio Bluetooth:

1. Encontrar el dispositivo (*Inquire*).
2. Conectarse al dispositivo (*Page*).
3. Descubrir qué servicios soporta el dispositivo (SDP).
4. Decidir a qué servicio conectarse y descubrir cómo hacerlo (SDP).
5. Conectarse al servicio.

Las etapas 3 a 5 implican la actuación de las capas superiores de la torre de protocolos. Por ejemplo, la conexión de cualquier dispositivo (por ejemplo, un PC) a un sensor Bluetooth para la lectura de datos a través de RFCOMM se llevaría a cabo de la siguiente forma:

- Etapa 1: se realiza la búsqueda del dispositivo de acuerdo con los siguientes pasos.
    1. La aplicación del PC envía una solicitud de búsqueda (*inquiry*) a las capas inferiores.
    2. Estas capas envían la solicitud a su entorno a través del interfaz radio.
    3. Todos los dispositivos situados en este entorno responden a la solicitud.
    4. Las capas inferiores envían las respuestas a la aplicación.

    Nótese que la aplicación situada en el sensor no ha intervenido aún. Cuando ha configurado las capas inferiores para que accedan al modo *inquiry scan*, ignora completamente las respuestas que generan.

- Etapa 2: es el momento de realizar la conexión al dispositivo. Se asume que que el sensor se ha configurado para que acceda al estado *page scan* regularmente.
    1. La aplicación del PC envía una solicitud de paginación a las capas inferiores.

2. Estas capas inferiores inician el procedimiento de paginación con el sensor, utilizado su dirección hardware para generar paquetes que sólamente él escuchará. El procedimiento se lleva a cabo tal como se ha explicado en apartados anteriores.
3. Las capas inferiores del sensor envían un mensaje a la aplicación albergada en él indicando la solicitud de conexión. Esta notificación incluye la dirección hardware del PC.
4. La aplicación del sensor responde a las capas inferiores aceptando la conexión.
5. Las capas inferiores del sensor responden a las capas inferiores del PC.
6. Las capas inferiores del PC reenvían esta información a la aplicación, la cual sabe que a partir de ese momento dispone de un enlace ACL para transmitir datos.

- Etapa 3: se descubren los servicios soportados a través de SDP. Lo primero que se hace en este caso es establecer una conexión L2CAP utilizando el PSM correspondiente a este protocolo.

  1. La aplicación del PC solicita a su capa L2CAP una conexión al PSM de SDP en el sensor.
  2. La solicitud es reenviada a la capa L2CAP en el sensor, la cual pregunta a la aplicación si la quiere aceptar.
  3. La aplicación del sensor responde que aceptará la conexión a la capa SDP.
  4. La respuesta es reenviada a la capa L2CAP en el PC, que informa a su aplicación que la conexión L2CAP a la capa SDP está lista para ser usada.

- Etapa 4: se decide a qué servicio conectarse y cómo hacerlo. En este momento el PC puede enviar solicitudes SDP y puede recibir respuestas desde el sensor. Una vez que la aplicación del sensor ha registrado el servicio en la capa SDP, no necesita ocuparse en las transacciones SDP, ya que la propia capa lo hace de forma autónoma. El PC envía solicitudes para recibir el registro de servicios del dispositivo sensor. Esto comprueba cuáles están soportados y proporciona información sobre cómo conectarse a ellos.

- Etapa 5: se lleva a cabo conexión al servicio. Esta etapa comienza de la misma forma que la etapa 3. El procedimiento es el mismo que se utiliza para crear una conexión L2CAP a SDP, salvo que en este caso se utiliza el PSM de RFCOMM.

  Una vez que la conexión L2CAP a RFCOMM está establecida, puede ser utilizada para transmitir mensajes entre el PC y el sensor.

3.3 Sensores Bluetooth

Poco después de que Bluetooth empezara a incrementar su popularidad como una tecnología para la sustitución de las conexiones cableadas y proporcionase la base para las llamadas redes de área personal, surgió también interés entre las comunidad investigadora de redes de sensores. Tradicionalmente la mayoría de redes de sensores han sido redes de difusión, pero Bluetooth, con una topología orientada a conexión, está creciendo en popularidad para pequeños sensores situados en las cercanías de seres humanos (salud, domótica, etc.).

El mecanismo de saltos de frecuencia hace que Bluetooth sea relativamente inmune a las interferencias electromagnéticas, y el amplio número de dispositivos Bluetooth proporciona una infraestructura que puede ser aprovechada para mejorar la conectividad. Otro aspecto interesante de Bluetooth es que permite altas tasas de datos.

Por el contrario, se pueden encontrar las siguientes desventajas a la hora de su aplicación en redes de sensores:

- El descubrimiento de dispositivos es lento, pudiendo ser de varios segundos y conllevar un consumo considerable de energía.
- Mantener las conexiones abiertas es costoso en términos energéticos comparado con otras tecnologías radio. En cualquier caso, se han propuesto [16] políticas de gestión de energía que pueden hacer Bluetooth más adecuado para su aplicación en redes de sensores. También se debe tener en cuenta el reciente *Bluetooth Low Energy* adoptado como parte de la especificación.
- Una pila con varias capas complica un control preciso de la sincronización y restringe la posibilidad de realizar cierto tipo de optimizaciones.

Los sensores Bluetooth se pueden dividir en dos categorías: la primera sería aquella que sólo utiliza las capas inferiores de la torre de protocolos para configurar las conexiones. La comunicación de datos se lleva a cabo utilizando protocolos propietarios por encima de estos. Esta solución requiere sólo una parte de la especificaciń Bluetooth y permite un mejor ajuste de determinados parámetros. En esta categoría se pueden encontrar dispositivos como el BTnode de la ETH de Zúrich y el iMote de Intel.

El BTnode (Figura 3.9) es una plataforma para la creación de redes ad-hoc. Se compone de un microcontrolador ATmega128 y dos módulos de radio. El primero de ellos es un Chipcon CC100 de difusión en la banda ISM. Esto permite al BTnode participar en redes multi-hop. El segundo sistema de radio es un módulo BLuetooth Zeevo ZV4002. El BTnode se ha usado en varios proyectos y también se usa en universidades con propósitos educacionales. El software se banda en Nut/OS o TinyOS y las comunicaciones se pueden realizar por los dos módulos de radio independientemente. El módulo de Chipcon opera en la bada de 433-915 MHz y usa protocolos propietarios. Por otro lado, el módulo Bluetooth soporta HCI, L2CAP y RFCOMM, permitiendo cierta interoperabilidad con otros dispositivos Bluetooth. Sin embargo, no soporta SDP. Se han creado scatternets con más de 70 dispositivos BTnode.

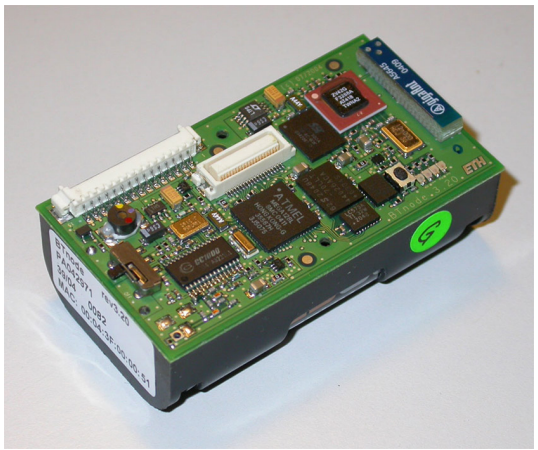

Figura 3.9: BTnode de la ETH de Zúrich

El iMote (Figura 3.10), desarrollado por Intel y la UCLA (Universidad de California, Los Ángeles) se basa en un microcontrolador Xscale y usa un módulo Bluetooth Zeevo TC2001. La plataforma soporta una multitud de diferentes sensores y fuentes de alimentación. A nivel de software, utiliza TinyOS junto con varias capas de protocolos desarrolladas para el dispositivo (no se soportan perfiles Bluetooth estándar), que premiten la creación de redes multi-hop.

La segunda categoría cumple con todas las capas de la pila de protocolos, lo que requiere una implementación más compleja. Sin embargo, esta complejidad permite comunicarse casi con cualquier dispositivo Bluetooth (ordenadores, teléfonos móviles, etc.). Además, el uso de TCP/IP puede

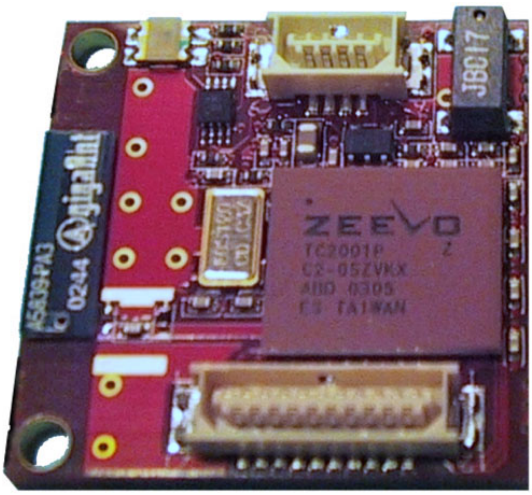

Figura 3.10: iMote de Intel

incrementar más aún las capacidades de comunicación, transmitiendo datos directamente a Internet. Utilizar TCP/IP lleva consigo varios beneficios tales como una mejora de la interoperabilidad y movilidad. Por contra, aumentar la complejidad del software puede suponer un problema en cierto tipo de microcontroladores; también se añade una carga extra a las comunicaciones debido a las cabeceras adicionales transmitidas en cada comunicación.

3.4 Bluetooth en vehículos

El uso potencial de la tecnología Bluetooth en vehículos se puede dividir en dos niveles: a nivel de sistema y a nivel de dispositivos de usuario.

3.4.1 Comunicaciones a nivel de sistema

Aunque inicialmente dirigida a aplicaciones de comunicación, es posible la utilización de sensores y actuadores Bluetooth en redes de control como las presentes en la mayoría de los automóviles modernos, pudiendo proporcionar la funcionalidad normalmente asociada con las redes cableadas como CAN. Su utilización depende de factores específicos a la industria automovilística y cualquier implementación debe cumplir rigurosos requisitos, referidos por ejemplo a las temperaturas de operación o la compatibilidad electromagnética.

También se debe considerar el número y cantidad de antenas necesarias para proporcionar la suficiente cobertura tanto en el interior como en el exterior del vehículo. Ya que el automóvil puede actuar como una jaula de Faraday, un diseño altamente especializado de estas antenas se hace necesario, además de un estudio de propagación de señales Buetooth en su interior [17]. Además existe el problema de que en determinados lugares como aparcamientos, donde varios cientos de dispositivos pueden estar activos y en proximidad, la calidad de las comunicaciones puede quedar comprometida. En caso de que se requiera que alguno de los sistemas Bluetooth queden activos mientras el vehículo está aparcado, lo que puede ser durante días o semanas, el consumo de energía puede ser difícil de gestionar, ya que los dispositivos Bluetooth en bajo consumo podrían ser despertados por otros en sus proximidades.

Una gran cantidad de cableado se encuentra presente en los vehículos modernos. Anteriormente

a la introducción de las redes de control ya comentadas (CAN, J1850, etc.), el incremento en la funcionalidad llevaba consigo un incremento en la cantidad de cableado. En cualquier caso, el problema continua existiendo, ya que los cables siguen siendo el componente electrónico más pesado y voluminoso en el interior del vehículo. Además presenta el MTBF (*Mean Time Between Failures*) más bajo de todos los componentes electrónicos. El conjunto de cableado puede contribuir hasta 50 kg a la masa del vehículo, afectando a su aceleración, diseño y eficiencia en el consumo de combustible. También se deben tener en cuenta factores medioambientales, ya que toda medida que implique la reducción en el consumo de combustible (menos peso implica menos consumo) debe ser seriamente considerada. Una arquitectura basada en tecnología Bluetooth tiene potencial para reducir el volumen de cableado.

No sería real pensar que los consumidores y los fabricantes aceptarían una solución inalámbrica para sistemas de control que requieren una seguridad crítica. Sin embargo, Bluetooth puede utilizarse para sistemas que no requieren una seguridad tan alta, como pueden ser módulos situados en las puertas, maletero, sensores de lluvia, movimiento de los asientos, etc. Ademas, reamplazar el cableado por conexiones inalámbricas en los interfaces móviles como aquellos situados entre las puertas y el vehículo, puede simplificar la labor de ensamblaje a los fabricantes e incluso llegar a ofrecer una mayor fiabilidad. Por otro lado, interfaces eléctricos complejos como el del panel de información del vehículo podrían ser eliminados, abriendo el camino para la instalación de diversos paneles personalizables.

En este contexto, una oportunidad interesante la presenta el desarrollo de pasarelas Bluetooth en el interior del vehículo, lo cual se ve facilitado por los mecanismos de sincronización global que proporcionan nuevos buses como TTP/C o FlexRay.

Probablemente la primera aplicación de Bluetooth a nivel de sistemas en un vehículo sea la de servir de interfaz a equipos de diagnóstico. Usando Bluetooth se podría acceder a toda la información de los sensores del vehículo sin necesidad de realizar ninguna conexión cableada. Por otro lado, en la fase de fabricación y ensamblaje, se podría interactuar con el vehículo para realizar labores de diagnóstico, calibración y configuración. Actualmente se pueden encontrar ejemplos de esta aplicación [18].

El software del vehículo podría ser descargado en sistemas de memoria flash, pudiendo hacer determinados elementos del automóvil reprogramables. Estas actualizaciones podrían realizarse a través de sistemas Bluetooth de forma sencilla.

Otro tipo de aplicaciones son algunas como la mejora de los sistemas de pago automático de peajes. Una amplia adopción estandarizada de este tipo de sistemas podría acelerar notablemente ese proceso. Casos parecidos se dan en aparcamientos (de pago o acceso privado).

3.4.2 Comunicaciones a nivel de dispositivos de usuario

La presencia de una red inalámbrica dentro de un automóvil introduce beneficios que podrían hacer la conducción más segura y confortable. En general, este tipo de comunicaciones pueden ser relevantes para información sobre el viaje (rutas, distancias, tráfico, etc.) o bien para propósitos de entretenimiento (música, televisión, etc.). Este tipo de comunicaciones no impone requisitos severos en la red de comunicaciones usada, debiendo cubrir distancias cortas y soportando tiempos de transmisión de hasta cientos de milisegundos. Un sistema de comunicación capaz de cumplir estos requisitos es Bluetooth. Además de sus ventajas técnicas, está previsto un uso cada vez mayor de este tipo de redes, lo que contribuirá a reducir aún más los precios de estos componentes electrónicos.

La aplicación más importante dentro de este campo será la conexión de teléfonos móviles o PDAs. En este entorno, un usuario podría entrar al vehículo con su teléfono móvil y empezar a usar el sistema de manos-libres sin hacer ningún tipo de conexión. También se podría realizar directamente una conexión a internet mostrando el contenido de páginas WEB o e-mails directamente en las pantallas

LCD del automóvil.

En la Tabla 3.4 se hace un resumen de todas las aplicaciones posibles durante las diferentes fases en la vida de un vehículo.

Fase de producción	Fase de operación	Fase de servicio
configuración	dispositivos multimedia	diagnósticos
calibración	teléfonos móviles	calibración
diagnósticos	PDAs	configuración
intercambio de información	pago de peajes	mejoras (software)
pre-ensamblaje y chequeos	sistemas de transporte inteligente	
mejora ensamblaje (automatización)	aparcamiento seguro	
	puertas, asientos, maletero	
	sistemas de alarma	

Tabla 3.4: Aplicaciones de Bluetooth en diferentes fases de la vida de un vehículo

Referencias

[1] J.A. Flint, A.R. Ruddle, and A.E. May. Coupling between Bluetooth modules inside a passenger car. In *Antennas and Propagation, 2003. (ICAP 2003). Twelfth International Conference on (Conf. Publ. No. 491)*, volume 1, pages 397--400 vol.1, March-3 April 2003.

[2] A.R. Moghimi, Hsin-Mu Tsai, C.U. Saraydar, and O.K. Tonguz. Characterizing Intra-Car Wireless Channels. *Vehicular Technology, IEEE Transactions on*, 58(9):5299--5305, Nov. 2009.

[3] Hsin-Mu Tsai, O.K. Tonguz, C. Saraydar, T. Talty, M. Ames, and A. Macdonald. Zigbee-based intra-car wireless sensor networks: a case study. *Wireless Communications, IEEE*, 14(6):67--77, December 2007.

[4] J.J. Blum, A. Eskandarian, and L.J. Hoffman. Challenges of intervehicle ad hoc networks. *Intelligent Transportation Systems, IEEE Transactions on*, 5(4):347--351, Dec. 2004.

[5] IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages C1--1184, 12 2007.

[6] IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, pages c1--502, 29 2009.

[7] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)*, pages 0_1--189, 2005.

[8] Draft Standard for Information Technology--Telecommunications and information exchange between systems--Local and metropolitan area networks --Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Wireless Access in Vehicular Environments. *IEEE Unapproved Draft Std P802.11p/D9.0, July 2009*, pages --, 2009.

[9] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager. *IEEE Std 1609.1-2006*, pages c1--63, 2006.

[10] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services. *IEEE Std 1609.3-2007*, pages c1--87, 20 2007.

[11] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. *IEEE Std 1609.2-2006*, pages 0_1--105, 2006.

[12] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation. *IEEE Std 1609.4-2006*, pages c1--74, 2006.

[13] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, pages 1--203, 2007.

[14] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems. *IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004)*, pages C1--2004, 29 2009.

[15] Bluetooth Special Interest Group. Bluetooth Core Specification v2.1. september 2007.

[16] L. Negri and D. Zanetti. Power/performance tradeoffs in bluetooth sensor networks. In *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 236b--236b, Jan. 2006.

[17] A. Schoof, T. Stadtler, and J.L. ter Haseborg. Simulation and measurement of the propagation of bluetooth signals in automobiles. In *Electromagnetic Compatibility, 2003. EMC '03. 2003 IEEE International Symposium on*, volume 2, pages 1297--1300 Vol.2, May 2003.

[18] Jianfeng Hua, Xinfan Lin, Liangfei Xu, Jianqiu Li, and Minggao Ouyang. Bluetooth wireless monitoring, diagnosis and calibration interface for control system of fuel cell bus in Olympic demonstration. *Journal of Power Sources*, 186(2):478 -- 484, 2009.