An Overview of the Bluetooth Wireless Technology

Chatschik Bisdikian, IBM Corporation

ABSTRACT

The Bluetooth™[1] wireless technology is designed as a short-range connectivity solution for personal, portable, and handheld electronic devices. Since May 1998 the Bluetooth SIG has steered the development of the technology through the development of an open industry specification, including both protocols and application scenarios, and a qualification program designed to assure end-user value for Bluetooth products. This article highlights the Bluetooth wireless technology.[2]

INTRODUCTION

For the last few years the wireless world has been bombarded daily with information about a new generation of radio frequency (RF) technologies that would profoundly impact, if not revolutionize, the way we live and contact our businesses. This new generation of technologies spans the full spectrum of wireless communications coverage. Third generation (3G) wireless technologies are being developed to enable personal, high-speed interactive connectivity to wide area networks (WANs). The IEEE 802.11b wireless local area network (LAN) technology finds itself with an increasing presence in corporate and academic office spaces, buildings, and campuses. Furthermore, with slow but steady growth, the 802.11b technology is making inroads into public areas such as airports and coffee bars.

WAN and LAN technologies enable device connectivity to infrastructure-based services, either through a wireless carrier provider or through a campus or corporate backbone intranet. The other end of the coverage spectrum is occupied by the short-range personal wireless connectivity technologies that allow personal devices to communicate with each other directly without the need for an established infrastructure. At this end of the coverage spectrum the Bluetooth wireless technology offers to the personal connectivity space the benefits of omni-directionality and the elimination of the line of sight requirement of RF-based connectivity. The personal connectivity space resembles a communications bubble that follows people around and empowers them to connect their personal devices with other devices that enter the bubble. Connectivity in this bubble is spontaneous and ephemeral and can involve several devices of diverse computing capabilities, unlike wireless LAN solutions that are designed for communication between devices of sufficient computing power and battery capabilities.

The Bluetooth wireless technology[3] will serve primarily as a replacement of the interconnect cables between a variety of personal devices, including notebook computers, cellular phones, personal digital assistants (PDAs), digital cameras, etc. The Bluetooth wireless technology aims to serve as the universal low cost, user friendly, air interface that will replace the plethora of proprietary cables that people need to carry and use to connect their personal devices. While personal devices typically communicate based on the RS-232 serial port protocol, proprietary connectors and pin arrangements make it impossible to use the same set of cables to interconnect devices from different manufactures, and sometimes even from the same manufacturer. The primary focus of the Bluetooth wireless technology is to provide a flexible cable connector with reconfigurable pin arrangements permitting several personal devices to interconnect with each other.

Another focus of the technology is to enable a uniform interface for accessing data services. A user using any number of data-capable devices will be able to connect to a LAN access point that provides access to, for example, the corporate intranet infrastructure and services. Likewise, the user will be able to connect to her cellular phone and access WAN data services. Applications can then be written that could provide the user with a similar connectivity experience connecting to data service in either manner. Connecting to data services through one's cellular phone gives rise to the concept of a *personal gateway*. People will carry their personal gateways wherever they go. The personal gateway will serve as a facilitator in accessing remote data services, with the added convenience that it can be kept hidden away from the line-of-sight of its communicating Bluetooth partner. The Bluetooth wireless technology enables the unobtrusive separation of the functionality of connecting to a data service from viewing and interacting with the information provided by the

[1] Bluetooth is a trademark owned by the Bluetooth SIG, Inc., USA.

[2] Any opinions expressed in this article represent only the personal opinions of the author and do not reflect a position of the author's employer or anybody else's.

[3] According to the Bluetooth brand requirements document, the term "Bluetooth" must always be used as an adjective. Furthermore, when the term "Bluetooth" is used to denote the corresponding technology, the term "wireless" must be inserted between Bluetooth and technology. The author recognizes that the above rules are not always followed and the term "Bluetooth" has grown to represent both the technology and the whole industry behind it.

0163-6804/01/$10.00 © 2001 IEEE

data service. Thus a PDA can be used as a more convenient I/O device for entering and receiving data, while using the personal gateway purely for communicating with the wireless data carrier.

Yet another focus item for the Bluetooth wireless technology is to enable ad hoc connectivity among personal devices. This will permit individuals to form collaborative groups, for example, during a conference meeting, to exchange data without the need to rely on an infrastructure to support their communication.

In this article, we present an overview of the Bluetooth wireless technology. This article is organized as follows. We present a history of the Bluetooth wireless technology, followed by a discussion of the Bluetooth specification, including the core and the profile portions of the specification. We conclude with a summary of the article.

The History of the Bluetooth Wireless Technology

The development of the Bluetooth industry standard started late in the winter of 1998 when Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Industry Group (SIG) to develop and promote a global solution for short-range wireless communication operating in the unlicensed 2.4 GHz ISM (industrial, scientific, medical) band.

The name Bluetooth comes from the Danish king *Harald Blåtand* (Bluetooth). King Bluetooth is credited with uniting the Scandinavian people during the 10th century. Similarly, the Bluetooth wireless technology aims to unite personal computing devices. The name was chosen temporarily to describe the yet unannounced development project. However, the search for a new name never came to a successful fruition and the temporary name became permanent. In retrospect, the selection of this joyful name can be credited highly for the recognition and acceptance the technology has received so far.

To facilitate the wide acceptance of this new technology, the SIG decided to offer all the intellectual property explicitly included in the Bluetooth specification royalty-free to adopter members of the technology when it is used to introduce Bluetooth products in the market. The SIG announced its existence and intentions to the public in May 1998, joined at the time by approximately 70 adopter members. As of this writing there are approximately 3000 adopter members. A little over a year later, in the summer of 1999, the over 1600-page Bluetooth specification version 1.0A became publicly available. Due to the Bluetooth SIG license agreement, the development of the specification is not made available to the general public until it is finished and approved by the Bluetooth SIG. Adopter members have the privilege to look at the specification prior to its public availability.

The Bluetooth specification, currently at version 1.1, comprised the following two parts, which we discuss later in the article:

- The core specification defining the radio characteristics and the communication protocols for exchanging data between devices over Bluetooth radio links.
- The profile specification that defines how the Bluetooth protocols are to be used to realize a number of selected applications.

To make free use of the intellectual property in the Bluetooth specification, adopter members need to qualify any Bluetooth products they intent to bring to market through the Bluetooth qualification program (BQP). The BQP includes radio and protocol conformance testing and profile conformance testing (when applicable) as well as interoperability testing.

In December 1999 the promoter group increased from five to nine with the addition of 3Com, Lucent, Microsoft, and Motorola. As of early 2001, Agere, a Lucent spinoff comprising its former microelectronics division, has taken the place of Lucent in the promoters group.

In March 1999 the IEEE 802.15 standards working group was created to develop a family of communications standards for wireless personal area networks (WPANs).[4] In the first meeting of the new working group in July 1999, the Bluetooth SIG submitted the just created Bluetooth specification as a candidate for an IEEE 802.15 standard. The Bluetooth proposal was chosen to serve as the baseline of the 802.15.1 standard. As of this writing, the development of the draft standard is in its final stages, having successfully completed two sponsor ballots. In addition to the IEEE 802.15.1 activity, the IEEE 802.15.2 task group studies coexistence issues between 802 wireless technologies. The 802.15.3 task group is developing standards for high-rate radios (>20 Mb/s). Finally, the 802.15.4 task group is developing standards for low-rate radios (<200 kb/s).

The Bluetooth Specification

The Bluetooth specification has been written primarily as an implementation manual rather than a formal communications standard document. This aspect of the specification reflects its development process by a group of engineers that actually developed the technology in parallel with the development of the specification. These engineers wrote in a prose style, describing in the specification their experiences gained in implementations. This is in contrast to the formal language commonly used in a formally developed standard. This approach has its pros and cons. On the upside, the specification is easier to read than a formal standards document. On the downside, using prose, which is naturally imprecise, the specification is sometimes open to conflicting interpretation. The latter issue is being addressed through an errata resolution process.

Figure 1 depicts the Bluetooth protocol stack, which also shows the application and profiles "layer" for completeness. (We discuss the latter later in this section.) The protocols in the stack have been grouped in two categories: the *transport* and the *middleware* protocols. The transport protocols comprise protocols developed exclusively for the Bluetooth wireless technology. These protocols are involved in all data communications between two Bluetooth devices. The middleware protocols comprise both Bluetooth-specific protocols and other adopted protocols. These protocols are used selectively to enable

The search for a new name never came to a successful fruition and the temporary name became permanent. In retrospect, the selection of this joyful name can be credited highly for the recognition and acceptance the technology has received so far.

[4] *WPAN is a trademark of IEEE.*

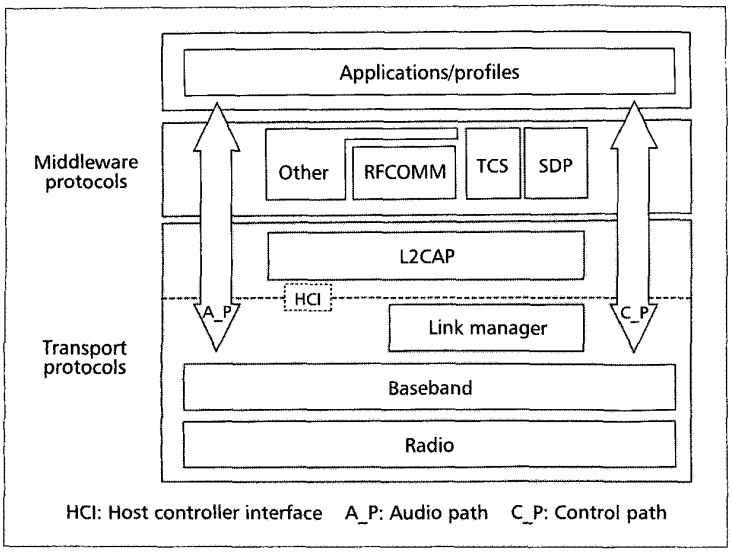


Figure 1. *The Bluetooth protocol stack.*

different applications, including both legacy and new applications, to exchange data using the Bluetooth wireless technology. Whenever desired, the middleware protocols shield these applications from the specifics of the Bluetooth transport protocols.

This grouping of the protocols in the Bluetooth protocol stack is not part of the specification. Rather, it is used here as a natural grouping of the protocols for ease of presentation.

The Transport Protocols

The Radio — The radio layer defines the technical characteristics of the Bluetooth radios. A Bluetooth radio operates on the license-free 2.4 GHz ISM band and is compliant with FCC part 15 regulations for intentional radiators in this band. It employs a fast (1,600 hops/sec), frequency-hopping, spread-spectrum (FHSS) technique. The radio hops in a pseudo-random fashion on 79 one-MHz channels.[5] The frequencies are located at $(2{,}402 + k)$ MHz, $k = 0, 1, \ldots, 78$.

The modulation technique is a binary Gaussian frequency shift-keying (GFSK) and the baud rate is 1 Msymbol/s. Hence, the bit time is 1 ms and the raw transmission speed is 1 Mb/s. The Bluetooth radios come in three power classes, depending on their transmit power. Class 1 radios have transmit power of 20 dBm (100 mW); class 2 radios have transmit power of 4 dBm (2.5 mW); class 3 radios have transmit power of only 0 dBm (1 mW). Due to the power and cost constraints of the various personal devices that use Bluetooth radios, class 3 and class 2 radios are expected to be the ones mostly used in these devices.

The Baseband — The baseband defines the key procedures that enable devices to communicate with each other using the Bluetooth wireless technology. The baseband defines the Bluetooth piconets and how they are created, and the Bluetooth links. It also defines how the transmit resources are to be shared among several devices in a piconent, as well as the low-level packet types.

The Bluetooth Address and Clock — Each Bluetooth device has two parameters that are involved in practically all aspects of Bluetooth communications. The first one is a unique IEEE-type 48-bit address assigned to each Bluetooth radio at manufacture time. The *Bluetooth device address (BD_ADDR)* is engraved on the Bluetooth hardware and it cannot be modified. The second parameter is a free-running 28-bit clock that ticks once every 312.5 μs, which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/sec.

Bluetooth devices can communicate with each other by acquiring each other's Bluetooth addresses and clocks, as will be further described later.

The Bluetooth Piconet — A piconet is a collection of Bluetooth devices that can communicate with each other. A piconet is formed in an ad hoc manner without any infrastructure assistance, and it lasts for as long as the creator of it needs and is available to communicate with other devices. A piconet contains at least one device identified as the *master* of the piconet and at most seven other devices identified as *slaves* with which the master is *actively* involved in communications. The terms master and slave are relative to a particular existing piconet. The terms are not assigned to the radio units at manufacture time. A Bluetooth radio may serve either as a master or slave at different times.

To identify each slave, the master of a piconet assigns a locally unique *active member address (AM_ADDR)* to the slaves participating in active communications in the piconet. The master regulates and controls who transmits and when. While up to seven slaves may be actively communicating in a piconet at one time, additional devices may be registered with the master and be invited to become active whenever necessary. These additional devices are called *parked*. Bluetooth devices not associated with any piconet are in *stand-by* mode. Figure 2 shows two piconets with a number of slaves and parked devices associated with them, and a few standby devices. Bluetooth piconets can coexist in time and space independently of each other. Furthermore, a single device may be a member of several piconets, a case referred to as *scatternet* in Bluetooth parlance.

The communications channel in a piconet is defined as the sequence of the frequency hops followed by the piconet members in a synchronized manner. The transmit and receive time axis are slotted, with each slot lasting the duration of a nominal frequency hop, 625 μs. Each baseband transmission resides fully within the boundaries of a slot. However, multi-slot packets occupying three or five slots instead are also allowed. During the transmission of a multi-slot packet, the transmit frequency does not change. When frequency hopping resumes, it resumes with the frequency whose turn it would have been if the devices were to use only single-slot transmissions.

To maintain time synchronization for the hops, slaves utilize the Bluetooth clock of the master and the fact that hops occur in multiples of 625 μs; slaves actually maintain the offset time between their Bluetooth clock and that of

[5] *The specification permits a reduced channel hop over only 23 channels for countries that have restrictions in their corresponding ISM band.*

their master. Slots in a piconet are identified as even or odd according to the value of the second least significant bit of the Bluetooth clock of the master; recall that the Bluetooth clock ticks at a rate twice that of the slot rate. To recreate the frequency hop sequence in a piconet, a slave utilizes the Bluetooth address of the master of the piconet. Furthermore, the Bluetooth clock of the master identifies the particular frequency to be used at a particular slot. Therefore, the communications channel in a piconet is fully identified by the master. As a result, in the case of scatternets a device can serve as a master for only one piconet, otherwise the two piconets cannot be distinguished from each other.

The master and the slaves alternate transmit opportunities in a *time-division duplex* (TDD) fashion. In particular, the master transmits on even numbered slots, as defined by the master's Bluetooth clock, while the slaves transmit on odd numbered slots (recall that each slot lasts 625 μs). A slave can transmit only if the master has just transmitted to this slave. A transmission may last one, three, or five slots; however, the specification requires that only the one-slot transmissions be mandatory. In the case of scatternets, a device cannot receive or transmit data simultaneously in two or more piconets. However, such a device may time-share its participation in each piconet over non-overlapping time intervals.

To engage in communications in a piconet, the slaves in the piconet need to know the *BD_ADDR* and Bluetooth clock of the master. Likewise the master needs to know the identities of the slaves. This information is acquired in two phases: the inquiry phase, for locating devices, and the the paging phase, for inviting specific devices to join a piconet. A good overview of these phases is given in J. Haartsen's "The Bluetooth Radio System" in [1].

The *inquiry* process is a device discovery process during which the master of a future piconet discovers other devices in its vicinity. The master makes its presence known by transmitting inquiry messages. Devices that perform inquiry scan, that is, search actively for inquiry messages, respond with inquiry response messages that, among other things, contain the *BD_ADDR* of the device.

Armed with the knowledge of the identity of devices in its vicinity, the master of a piconet may explicitly *page* devices to join its piconet. A master with prior knowledge of the identity of a device may skip the inquiry process and go directly to paging the device. If the device does not respond, it may mean that it is not in the transmit range of the paging device.

With the information sent by the paging device to the paged device, the paged device can now join as a slave the piconet whose master is the paging device. After joining the piconet, the master and the slave may negotiate reversal of roles, in which case the (original) master becomes a slave in the piconet whose master will be the (original) slave.

Next we present how masters and slaves exchange data.

The Bluetooth Links and Baseband Packets — There are two types of links supported in the Bluetooth piconet. Between a master and a slave there is a single *asynchronous connectionless* (ACL) link supported. Optionally, a piconet may support *synchronous connection-oriented* (SCO) links. Up to three SCO links may be supported in a piconet.

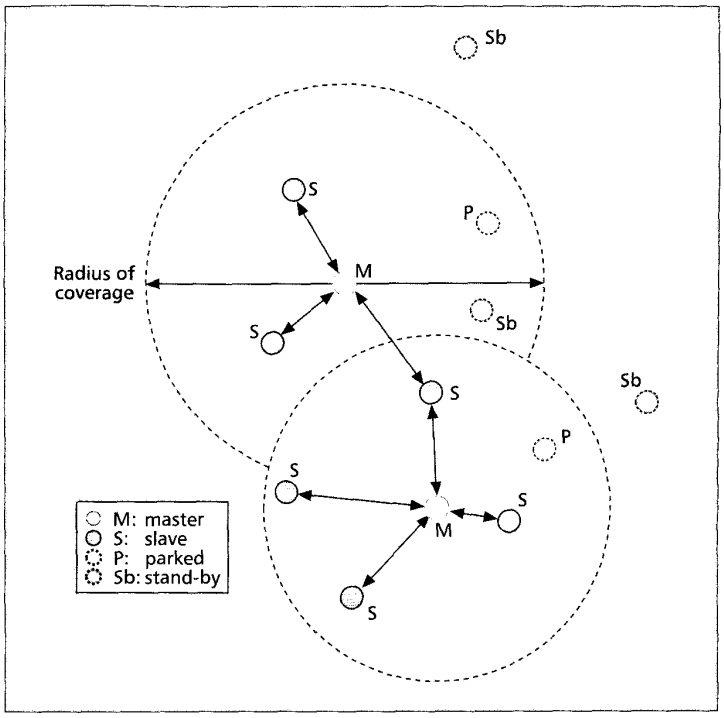


Figure 2. *Bluetooth piconets.*

The ACL link is a best-effort link appropriate for asynchronous data transmissions. It maintains integrity by using retransmissions and sequence members, as well as forward error correction (FEC) if necessary. The SCO link supports periodic audio transmissions at 64 Kb/s in each direction. SCO traffic is not retransmitted, but it can use FEC mechanisms to recover from transmission errors when they occur.

Figure 3 shows the various baseband packet types. They all contain an *access code* (AC) field, which is used to distinguish transmissions in different piconets. With the exception of the ID packet, all other packets also have a header portion. With the further exception of the poll and null packets, all other packets also have a payload section.

The ID packet is used during inquiry searches and to obtain time synchronization during pages. The poll packet is used by the master to explicitly poll a slave when no payload information needs to be sent to the slave. The *null* packet is used to acknowledge a transmission when no payload information needs to be sent.

The *frequency-hopping sequence* (FHS) packet is used during the creation of a piconet and it is used to pass address (*BD_ADDR* and *AM_ADDR*) and clock information between future masters and slaves. The payload of an FHS packet is encoded with a shortened Hamming code with rate 2/3. The number of bits shown in the figure is after the application of the FEC.

The ACL or SCO packets carry asynchronous

The link manager protocol is a transactional protocol between two link management entities in communicating Bluetooth devices whose responsibility is to set-up the properties of the Bluetooth link.

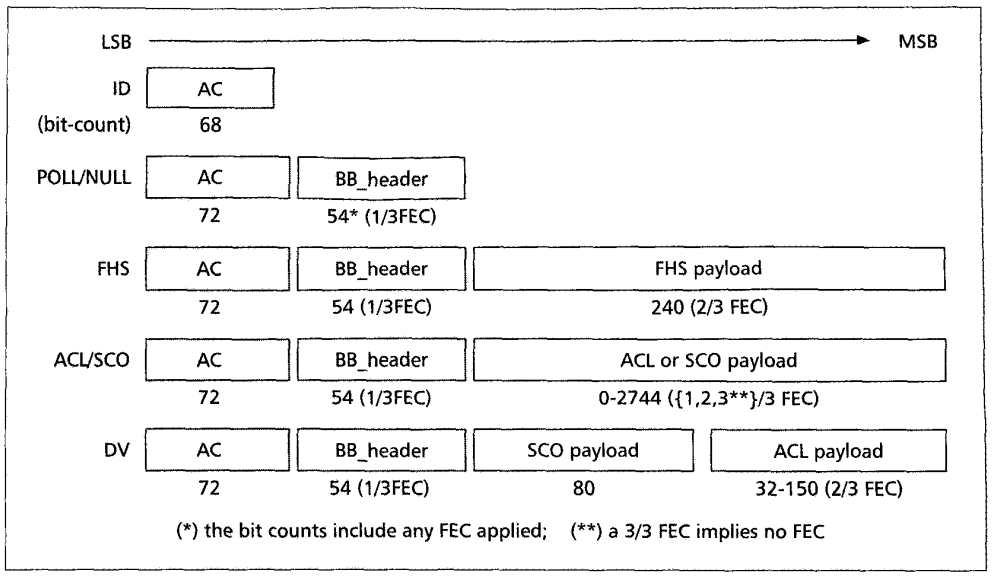


Figure 3. *The baseband packet types.*

and synchronous data in their payload, respectively. The payload of ACL packets may be encoded with an FEC with rate 2/3, or not encoded at all. The payload of SCO packets may be encoded with an FEC with rate 2/3 or 1/3, or not encoded at all. When the FEC with rate 1/3 is used, each bit is simply repeated three times. The *data voice* (DV) packet is a packet that contains both ACL and SCO data and is transmitted at the periodic instances of a regular SCO packet, whenever there is a need to send ACL data to the recipient device of the SCO transmission.

Figure 4 depicts the fields in the header and the payload of a baseband packet. The *AM_ADDR* field identifies the destination slave of a master transmission or the source slave of a slave transmission. The *PDU_type* field identifies the type of baseband packet as shown in Fig. 3. The flags are used for controlling the transmission and retransmission of ACL packets. In particular, ACL packets use a stop-and-go ARQ scheme and a 1-bit sequence number. Furthermore, the ACL link is flow-controlled. The header is protected by an 8-bit header error check (HEC) code. The ACL payload has its own header and body portion (see also Fig. 5) and it is protected with a 16-bit cyclic redundancy check (CRC).

When *AM_ADDR* = b'000', then the packet is a broadcast packet from the master to all the slaves. Broadcast packets are not acknowledged and are not retransmitted.

The *L_CH* field in Fig. 5 is used to identify the logical channel for this baseband transmission. When *L_CH* = b'11', then the body of the ACL packet payload is passed to the link manager and is used for the configuration of the Bluetooth link. When *L_CH* = b'01' or b'01', then the body is passed to L2CAP for further processing (discussed later).

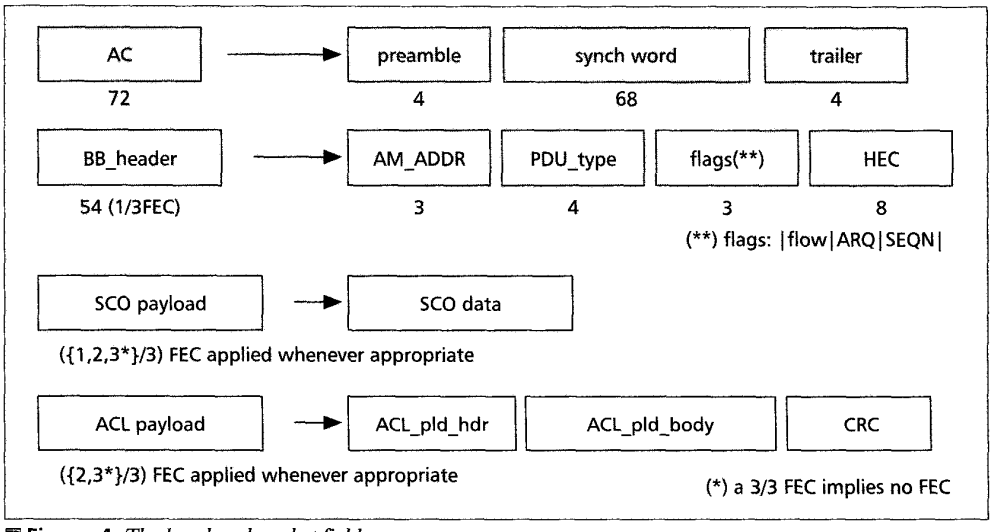
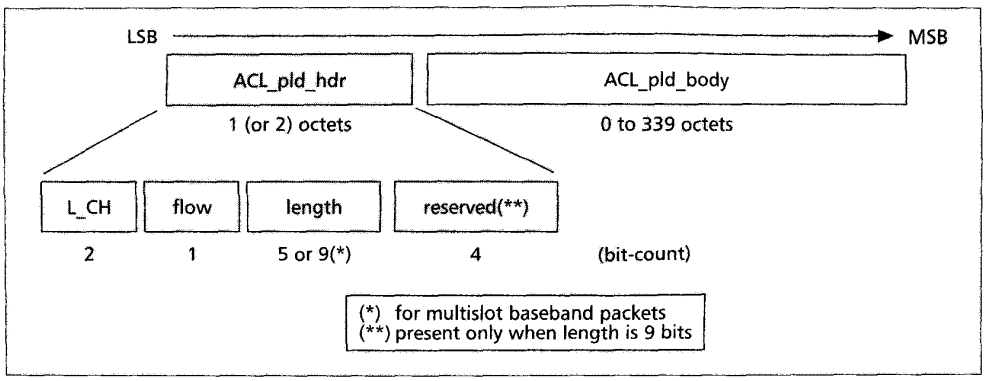


Figure 4. *The baseband packet fields.*



■ **Figure 5.** *The ACL packet payload format.*

The Link Manager Protocol — The Link Manager Protocol (LMP) is a transactional protocol between two link management entities in communicating Bluetooth devices whose responsibility is to set-up the properties of the Bluetooth link. For LMP packets, the *L_CH* field in Fig. 5 is set to the binary value b'11'.

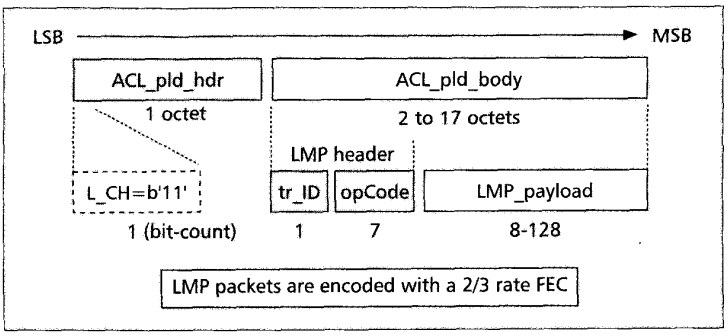
Through LMP transactions one device may authenticate another device through a challenge response mechanism. For authenticated devices, the link may be further encrypted. Two link managers may learn each other's features, for example whether the devices support SCO links, what size of packet transmission do they support, or whether they support any of the low power consumption modes. SCO connections are established using LMP transactions; polling intervals and agreed upon packet sizes are also set up through LMP transactions.

Figure 6 shows the format of an LMP packet. The LMP packets are carried in the payload of one-slot ACL packets with logical channel *L_CH* = b'11'; optionally, when supported, DV packets may also be used. The header of an LMP packet is just one octet. The *tr_ID* (for transaction ID) simply signifies the initiator of an LMP transaction, which could be either the master (*tr_ID* = b'0') or the slave (*tr_ID* = b'1').

Security Procedures — The algorithms for authentication and encryption are part of the baseband portion of the Bluetooth specification. However, the act of authentication, as well as the negotiation for encrypting the link between two devices, are part of the LMP specification. Thus, the discussion about the security procedure is included here.

Bluetooth devices may be authenticated and links may be encrypted. Due to the ad hoc nature of Bluetooth communications and the fact that Bluetooth devices do not depend on infrastructure services for communications, certificate and public key infrastructure (PKI) approaches for authentication do not apply directly to Bluetooth piconets. Instead, the authentication of Bluetooth devices is based on a challenge/response mechanism based on a commonly shared secret, a *link key* generated through a user-provided PIN.

Authentication of devices may happen at any time during the lifetime of a connection between two Bluetooth devices. The authentication starts



■ **Figure 6.** *The LMP packet format.*

with the transmission of an LMP challenge packet. The challenge packet contains a random number generated by the *challenger*, which is the device that attempts to authenticate the other device. The receiver device of the challenge, called the *claimant*, operates on the challenge using a 128-bit authentication key. The claimant returns the result of the operation to the challenger, who can then compare the result with the expected outcome of the operation and, thus, verify the identity of the claimant.

Following device authentication, the devices may further encrypt the link between them to protect against eavesdropping. Using the link key, the devices will generate a sequence of encryption keys to encrypt their transmissions. The encryption key changes with each packet transmission. Encryption is a mutual operation, and encryption encrypts the whole link, both the asynchronous and synchronous transmissions.

The encryption key can be up to 128 bits long. However, the size of the encryption keys is ultimately dictated by government regulations. The authentication and encryption keys are generated based on the SAFER+ algorithm [2].

The Low Power Modes — As with the security algorithms, the actual low power modes of operation are part of the baseband. However, these modes can be configured and activated via LMP transactions, and they are highlighted here.

In the *sniff* mode, a slave agrees with its master to listen for master transmissions periodically, where the period is configured through LMP transactions.

The algorithms for authentication and encryption are part of the baseband portion of the Bluetooth specification. However, the act of authentication, as well as the negotiation for encrypting the link between two devices, are part of the LMP specification.

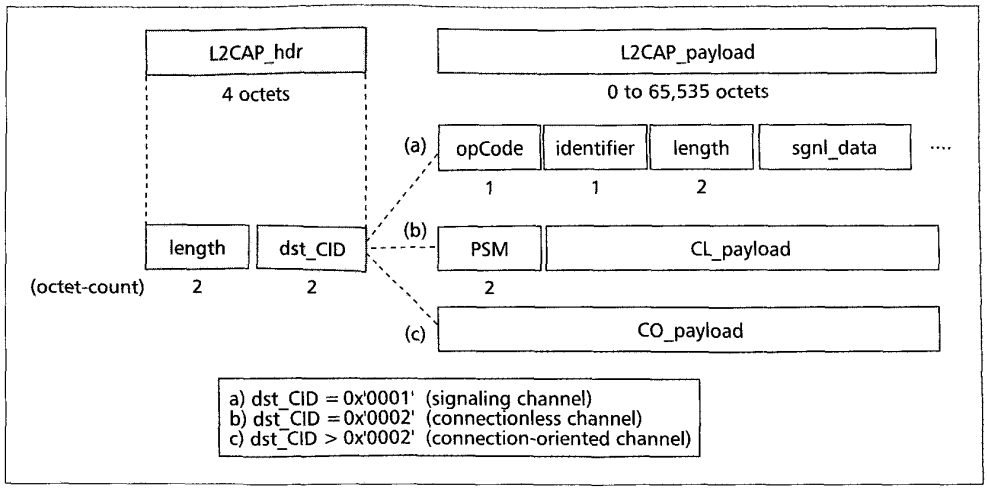


Figure 7. *The L2CAP packet format.*

In the *hold* mode, a device agrees with its communicating partner in a piconet to remain silent (in the particular piconet) for a given amount of time. A device that has gone into hold mode does not relinquish its temporary address, *AM_ADDR*.

Finally, in the *park* mode a slave device agrees with its master to park until further notice. As a device enters the park mode, the device relinquishes its active member address, *AM_ADDR*. While parked, a device will periodically listen to beacon transmissions from the master. A device may be invited back to active communications using a broadcast transmission during a beacon instant. When the slave wants to be unparked, it would send a message to the master in the slots following the beacon instant.

The above modes of operation are designed to reduce the power consumption of a device. However, they are optional features. While in any of these modes, a device may be involved in other tasks, such as entering inquiry scans, participating in active communications in another piconet, etc. Hence, the low power modes of operation, while designed for this purpose, enable additional modes of operation for a device.

The Host Controller Interface (HCI) — As the name states, this is not a protocol *per se*. Rather, it is an interface for host devices to access the lower layers of the Bluetooth stack through a standardized interface. Through the HCI, a host device passes and receives data destined to or coming from another Bluetooth device. Also through the HCI, a host may instruct its baseband to create a link to a specific Bluetooth device, execute inquiries, request authentication, pass a link key to the baseband, request activation of a low power mode, etc. The HCI will not be discussed further here; for more information see the Bluetooth specification.

The Logical Link Control & Adaptation Protocol — The Logical Link Control & Adaptation Protocol (L2CAP) layer shields the specifics of the Bluetooth lower layers and provides a packet interface to higher layers. At the L2CAP layer, the concepts of master and slave devices do not exist anymore. The L2CAP supports the multiplexing of several logical channels over the device's ACL links. Note that a slave has only one ACL link while a master has one for each slave that it actively communicates with.

L2CAP packets can be much larger than the baseband packets and they may need to be segmented prior to transmission over the air, and reassembled following their receipt. For L2CAP packets, the *L_CH* field in Fig. 5 is set to the binary value b'10' for the transmission of the first segment of an L2CAP packet, and b'01' for subsequent segments.

L2CAP traffic flows over logical channels terminating at the L2CAP layer of communicating devices. Channels may either be connectionless or connection oriented. A channel end-point is identified by a two-octet *channel identifier* (CID); within each device, CIDs of various channels are unique. The connectionless CID has the reserved value 0x'0002'. The connection-oriented channels go through a setup process using L2CAP signaling. The CID of the signaling channel has the reserved value 0x'0001'.

Figure 7 summarizes the various types of L2CAP packets. They comprise a header, which is four octets long, and a payload portion, which could be up to 65,535 octets long. Devices with limited capabilities may be able to handle only much smaller packets. Learning the features supported from the other L2CAP entities is part of the L2CAP connection setup process.

As Fig. 7 shows, the payload of the L2CAP signaling packets (CID = 0x'0001') contains signaling information that is formatted with the following fields:

- A one-octet *opCode* field to identify the particular signaling data.
- A one-octet identifier field used to match responses to requests.
- A two-byte length field containing the length of the data field.
- The signaling data.

Figure 7 also shows the format of a connectionless L2CAP packet. Its payload carries asynchronous data and the *PSM* field used to support

protocol multiplexing in L2CAP channels. For connection-oriented channels the *PSM* field is included in the signaling data portion of a connection request signaling L2CAP packet. During an L2CAP connection establishment, a channel may be further configured for the *maximum transmit unit* allowed in each direction of the transmission. Also, a quality of service negotiation is possible; however, currently only best-effort traffic is fully supported over L2CAP channels.

The Middleware Protocols

While the transport protocols are involved in every communication of application data over Bluetooth links, not every middleware protocol participates in Bluetooth communications at all times.

The Service Discovery Protocol (SDP) — In order to support the rich application space envisioned for Bluetooth devices, a Service Discovery Protocol (SDP) was added to the basic Bluetooth protocols. Using this protocol a Bluetooth device can inquire about the services that another device across a Bluetooth link may have and learn about how to get access to it. The SDP only provides information about services, it does not provide access to them. A Bluetooth device may access the service via different means using the information learned through service discovery.

SDP is optimized for usage by devices of possibly limited capabilities over wireless links. Bandwidth is preserved by utilizing binary encoding of information over the air. Universally unique identifiers (UUIDs) are used to describe services and attributes of these services in a manner that may not require a central registration authority for registering services. Typically the UUIDs are 128 bits long; however, for known services 16-bit and 32-bit UUIDs may also be used.

The RFCOMM Protocol — The RFCOMM Protocol is an important layer that is used to expose a serial interface to the packet-based Bluetooth transport layers. In particular, the RFCOMM layer emulates the signals on the nine wires of an RS-232 interconnect cable. The RFCOMM is based on the ETSI 07.10 standard, which permits the emulation and multiplexing of several serial ports over a single transport.

RFCOMM enables legacy applications that have been written to operate over serial cables to run on top of a Bluetooth link without modification. Several of the applications developed for Bluetooth use the RFCOMM as part of their implementation stack.

The Telephony Control Signaling (TCS) Protocol — Telephony control can be performed using the AT command set. Since the AT commands have been designed to be passed over serial lines, Bluetooth devices use the RFCOMM to send and receive control signaling based on the AT command set. For example, using these commands a dialer application in a notebook computer may instruct a cellular phone to dial up an ISP location.

The AT command set is well established and can be used for supporting legacy applications such as the dialer application. In addition to this control protocol, referred to as TCS-AT, the Bluetooth technical groups developed an additional packet-based telephony control signaling protocol, called TCS-BIN (BIN stands for the binary encoding of information), that runs directly on top of L2CAP. The protocol supports normal telephony control functions such as placing and terminating a call, sensing ringing tones, accepting incoming calls, etc. Unlike TCS-AT, TCS-BIN supports point-to-multipoint communications as well, allowing, for example, a cordless base station to pass the ringing signal of an incoming call to several cordless headsets associated with the base station.

Other Protocols — To support various applications, a number of industry standards have been adopted. Such protocols include the Point-to-Point Protocol (PPP), which is an IETF standard for enabling communications, including IP communications, over serial lines; the Object Exchange (OBEX) Protocol, an IrDA standard for transporting objects between devices; and the Infrared Mobile Communications (IrMC) Protocol, another IrDA standard for describing and encoding information in business cards, calendar entries, and messages. All these protocols are run on top of RFCOMM.

The Bluetooth Profiles

As mentioned earlier, the Bluetooth specification comprises not only communications protocols but applications as well. This sets the Bluetooth wireless technology apart from many other communications technologies that focus primarily on the physical, data link, and possibly networking aspects of communications. Since the Bluetooth wireless technology is to be used primarily by consumers, the technology must require minimal technical expertise from its users. For this to be possible, a set of simple but useful applications had to be developed to allow Bluetooth devices to perform useful tasks with other Bluetooth devices right out of the box. This would provide added value to the users of the technology and aid in establishing this technology as the *de facto* means for short-range communications of personal devices. The specifications for building interoperable applications are called *profiles*.

All profiles depend on the *Generic Access Profile* (GAP) which defines the basic rules and conditions for connecting devices with each other and establishing Bluetooth links and L2CAP channels. It also defines security levels according to which devices may allow themselves to be discovered or allowed to be connected, be authenticated or authenticate other devices, etc. It also defines the conditions necessary to establish trust relationships between devices.

There are two protocol profiles, which depend on each other. The *serial port profile* defines how RFCOMM runs on top of the Bluetooth transport protocols, while the *generic object exchange profile* defines how objects can be exchanged using the OBEX protocol running on top RFCOMM as defined in the serial port profile. Depending on the previous profile, there

The RFCOMM protocol is an important layer that is used to expose a serial interface to the packet based Bluetooth transport layers. In particular, the RFCOMM layer emulates the signals on the nine wires of an RS-232 interconnect cable.

Beyond the current specification version 1.1, the SIG is working on a number of additional profiles including higher-rate radios, printing, imaging, cordless computers, support for IP communications without the need of RFCOMM and PPP in car applications, extended service discovery, and so on.

are profiles describing how to synchronize personal information management (PIM) data, how to push (and pull) objects, e.g., business cards, and how to transfer files. Based on the serial port profile there are also additional profiles related to the use of cellular phones as modems for dial-up networking, connecting to a wireless headset, sending faxes, or accessing LAN services through a LAN access point.

There are two profiles based on the TCS-BIN protocol which describe two aspects of the so called 3-in-1 usage scenario, where a cellular phone can be used as a headset in a cordless telephony system or as an intercom device to communicate directly with other cellular phones.

Finally, there is the service discovery application profile that shows how a service discovery application uses the service discovery protocol and, furthermore, how the latter protocol uses the Bluetooth transports for carrying the service discovery packets between a service discovery client and a server.

Beyond the current specification version 1.1, the SIG is working on a number of additional profiles including higher-rate radios, printing, imaging, cordless computers, support for IP communications without the need for RFCOMM and PPP, in-car applications, extended service discovery, and so on.

SUMMARY

The Bluetooth wireless technology is a specification for short-range, low-cost, and small form-factor that enables user-friendly connectivity among portable and handheld personal devices, and provides connectivity of these devices to the Internet. The technology supports both asynchronous data flows and synchronous audio streams over links with raw link speed of 1 Mb/s. It operates in the 2.4 GHz ISM band utilizing low transmit power radios, typically 0 dBm, using a frequency-hopping spread-spectrum technique. The Bluetooth specification is an ongoing process steered by the promoters of the Bluetooth SIG and developed by contributing SIG members.

The SIG recognized that the technology would be successful if it is widely available and if useful tasks can be done with it from the early days of its implementation. For this reason the Bluetooth specification comprises a protocol stack provided by a hardware and software description, and an application framework, called profiles, for building interoperable applications. Furthermore, the technology is provided license-free to the adopter members of the technology. The Bluetooth qualification program, which is applicable only on potential Bluetooth products by adopter members, has been designed to build, promote, and maintain a level of confidence to the users of the technology that they are using a product that was built in a manner compliant with the Bluetooth specification. Furthermore, it can interact with other devices and behave as expected when executing any application claimed to be conformant to the Bluetooth profiles.

The Bluetooth movement started in May 1998 and it has been followed very closely by the technical community, the business community, all sorts of market analysts and gurus, and the media. While we are witnessing the introduction of Bluetooth products into the market at an increasing rate, it appears that the deployment of the technology has been moved slower than originally anticipated. That is actually quite understandable and it is common with any new technology. For example, the development of the 802.11 technology started in the early 1990s, and it took a good portion of a decade before it started spreading.

The slower than anticipated pace of deployment of the Bluetooth wireless technology is understandably notable. However, the expectations for the potential of the technology have not seem to diminish, only shifted in time. The vision of a single technology that enables personal area networks that move as people move and brings worry-free, ad hoc connectivity to personal devices at home and in the workplace, in the car and in the mall, in the airport and in the ballpark, and so on, introduces too strong a paradigm to be ignored. It is true today, as it was in May 1998, that the only technology that still has the possibility to succeed in this space is the Bluetooth wireless technology.

IN MEMORY OF ...

Dr. Richard LaMaire, a dear friend and esteemed colleague, who passed away as the finishing touches of this article were being made.

REFERENCES

[1] C. Bisdikian, J. C. Haartsen, and P. Kermani, Eds., "Connectivity and Applications Enablers for Ubiquitous Computing and Communications," special issue of *IEEE Pers. Commun.*, vol. 7, no. 1, Feb. 2000.

[2] J. L. Massey, "On the Optimality of SAFER+ Diffusion," available at http://csrc.nist.gov/encryption/aes/round1/conf2/papers/massey.pdf

ADDITIONAL READING

[1] The Bluetooth specification is available at http://www.bluetooth.com

[2] B. A. Miller and C. Bisdikian, *Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications*, Prentice Hall, 2001.

[3] J. Bray and C. F. Sturman, *Bluetooth: Connect Without Cables*, Prentice Hall 2001.

[4] C. Bisdikian, P. Bhagwat, and N. Golmie, Eds., "Wireless Personal Area Networks," special issue of *IEEE Network*, vol. 15, no. 5, Sept./Oct. 2001.

[5] R. Schneiderman, "Bluetooth's Slow Dawn," IEEE Spec., vol. 37, no. 11, Nov. 2000.

BIOGRAPHY

CHATSCHIK BISDIKIAN (bisdik@us.ibm.com) [SM] is a research staff member and team leader for the Wireless Services (WISE) Platforms group at IBM's T.J. Watson Research Center, Hawthorne, NY. He received a Ph.D. degree in electrical engineering from the University of Connecticut in 1988 and he has been with IBM ever since. His research interests include short-range wireless networks, service discovery, spontaneous networking, content delivery, multimedia/broadband communications, and related areas. He has been involved with the development of the Bluetooth protocol specification from its early stages. He is participating in the standardization of the Bluetooth specification within IEEE 802.15 and serves as vice-chair of the IEEE 802.15.1 task group. He served on the editorial boards of several technical publications, authored over 85 technical, peer-reviewed papers, and holds five patents. He is a co-author of *Bluetooth Revealed*, published by Prentice-Hall PTR (2001). He is a 1995 Eta Kappa Nu Outstanding Young EE Award program finalist.