CHAPTER 13

AD HOC NETWORKING AND WPAN

13.1 Introduction

13.2 What is IEEE 802.15 WPAN?

13.3 What is HomeRF?

13.4 What is Bluetooth?

13.4.1 Overall Architecture
13.4.2 Protocol Stack
13.4.3 Physical Connection
13.4.4 MAC Mechanism
13.4.5 Frame Formats
13.4.6 Connection Management
13.4.7 Security

13.5 Interference between Bluetooth and 802.11

13.5.1 Interference Range
13.5.2 Probability of Interference
13.5.3 Empirical Results

Questions

Problems

13.1 INTRODUCTION

In the last three chapters, we provided an overview of the wideband wireless local access techniques. We divided these activities into WLANs and WPANs and provided the details of WLAN standards. In this chapter we provide an overview of the WPAN activities. At the time of this writing, WPANs are differentiated from the WLANs with their smaller area of coverage, ad hoc only topology, plug and play architecture, support of voice and data devices, and low-power consumption. WPANs started as BodyLANs which connect sensors and information devices attached to the body to the neighbors for the military application and as personal networks to connect personal equipment such as the laptops, notepads, and cell phones of a person in commercial applications.

The very first personal area network to be announced was the BodyLAN which emerged from a DARPA project in the mid-1990s. This was a low-power, small-size, inexpensive WPAN with modest bandwidth that could connect personal devices within a range of around five feet [DEN96]. Motivated by the BodyLAN project, a WPAN group originally started in June 1997 as a part of the IEEE 802.11 standardization activity. In January 1998, the WPAN group published the original functionality requirement. In May 1998, the study group invited participation from the WATM, Bluetooth, HomeRF, BRAN (HIPERLAN), IrDA (IR short-range access), IETF (Internet standardization), and WLANA (a marketing alliance for WLAN companies in the United States). Only the HomeRF and Bluetooth groups responded to the invitations. In March 1998, the Home RF group was formed. In May 1998, the Bluetooth development was announced, and a Bluetooth special group was formed within the WPAN group [SIE00]. In March 1999, the IEEE 802.15 was approved as a separate group in the 802 community to handle WPAN standardization. At the time of this writing, IEEE 802.15 WPAN has four subcommittees on Bluetooth, coexistence, high data rate, and low data rate. Bluetooth has been selected as the base specification for IEEE 802.15. In the rest of this chapter, we provide an overview of the WPAN, HomeRF, and Bluetooth activities.

13.2 WHAT IS IEEE 802.15 WPAN?

The 802.15 WPAN group is focused on development of standards for short distance wireless networks used for networking of portable and mobile computing devices such as PCs, PDAs, cell phones, printers, speakers, microphones, and other consumer electronics. The WPAN group intends to publish standards that allow these devices to coexist and interoperate with one another and other wireless and wired networks in an internationally acceptable frequency of operation.

The original functional requirement published in January 22, 1998, was based on the BodyLAN project and specified devices with [HEI98]:

- Power management: low current consumption
- Range: 0–10 meters

- Speed: 19.2–100 kbps
- Small size: .5 cubic inches without antenna
- Low cost relative to target device
- Should allow overlap of multiple networks in the same area
- Networking support for a minimum of 16 devices

As we will see later on in this chapter, these specifications fit the Bluetooth specification that was announced after this premier announcement. The initial activities in the WPAN group included HomeRF and Bluetooth group. Today HomeRF maintains its own Web site at [HomeRFweb] and IEEE 802.15 WPAN has four task groups. Task group one is based on Bluetooth and defines PHY and MAC specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS). A POS is the space about a person or object that typically extends up to 10 meters in all directions and envelops the person whether stationary or in motion. The proposed project will address QoS to support a variety of traffic classes [IEE00].

Task group two is focused on coexistence of WPAN and 802.11 WLANs. This group is developing a coexistence model to quantify the mutual interference and a coexistence mechanism to facilitate coexistence of an IEEE 802.11 WLAN and an IEEE 802.15 WPAN device. A goal of the WPAN Group will be to achieve a level of interoperability that could allow the transfer of data between a WPAN device and an 802.11 device.

Task group three of the IEEE P802.15 works on PHY and MAC layers for high-rate WPANs that operate at data rates higher than 20 Mbps. This standard will provide for low-power, low-cost solutions addressing the needs of portable consumer digital imaging and multimedia applications. This standard aims at providing compatibility with the Bluetooth specification of the task group one and expects to be completed by early 2002.

Task group four is chartered to investigate an ultralow complexity, ultralow power consuming, ultralow cost PHY and MAC layer for data rates of up to 200 kbps. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation. The project may also address the location tracking capabilities required to support uses of smart tags and badges.

13.3 WHAT IS HomeRF?

According to [HOM00] the mission of the HomeRF working group is to provide the foundation for a broad range of interoperable consumer devices by establishing an open industry specification for wireless digital communication between PCs and consumer electronic devices anywhere in and around the home. Figure 13.1 represents the overall vision of the HomeRF working group. Like the general architecture of home networks described in Chapter 10, the HomeRF working group architecture supports both ad hoc and infrastructure networks. In the more popular infrastructure network, the home Internet and PSTN access arrives at a control HomeRF distribu-

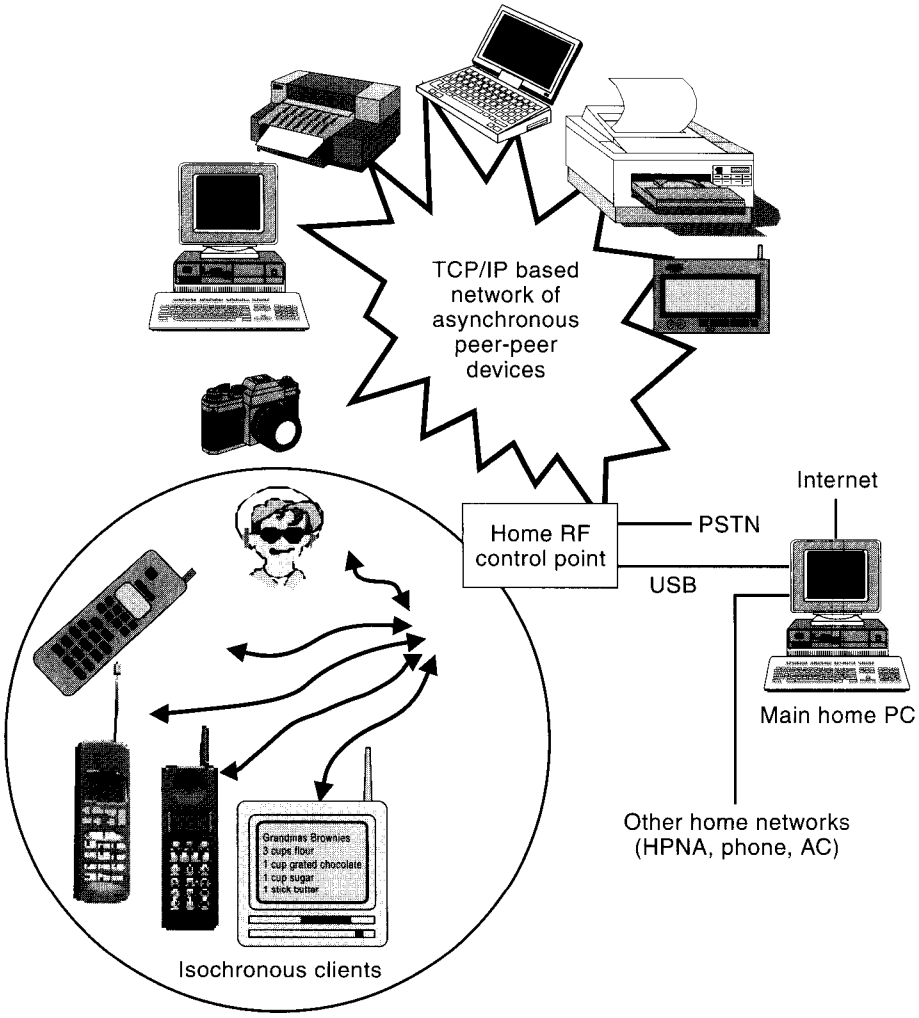


Figure 13.1 The overall architecture of the HomeRF System [HomeRFweb].

tion box that supports wireless as well as HPNA networks. The wireless part supports an isochronous network interconnecting up to six cordless telephone devices and an asynchronous network interconnecting a number of data devices. The two major competitors of this technology are HIPERLAN-2 and Bluetooth. Compared with HIPERLAN-2, the HomeRF solution provides a narrower bandwidth (up to 2 Mbps against 54 Mbps in HIPERLAN-2) that cannot support video for TV and VCR applications. HomeRF has a higher data rate than Bluetooth, but the latter was introduced as an inexpensive chip set that soon attracted a large alliance.

The HomeRF working group has developed a specification for wireless communications in the home called shared wireless access protocol (SWAP). The SWAP specification defines a new common interface that supports wireless voice and data networking in the home. The SWAP specification is an extension of

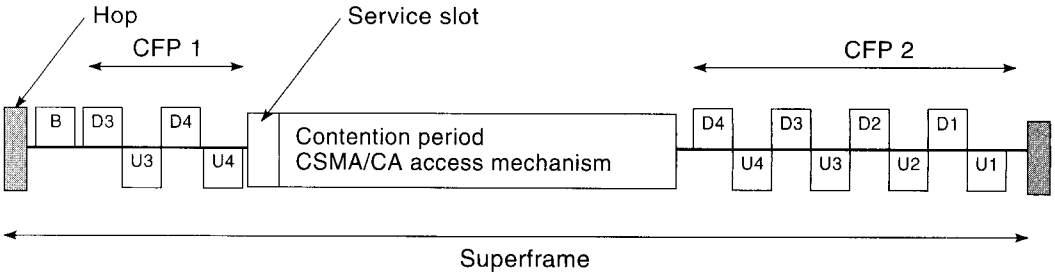


Figure 13.2 SWAP frame specification.

DECT (using TDMA) for voice and a relaxed 802.11 (CSMA/CA) for high-speed data applications. Figure 13.2 shows the MAC frame structure of the SWAP. Each superframe packet has a length of 20 ms and is transmitted in one hop (50 hops per second) of the FHSS system that supports 1 and 2 Mbps using two- and four-level FSK like IEEE 802.11. The superframe has a beacon period for control functions, two contention-free periods (CFPs) for voice traffic, and a contention period (CP) for data traffic. The second CFP is shared by four 2-way (TDD) voice users. The first CFP is used for two 2-way voice channels that can also be used for retransmission of the lost voice packets in the first two channels. The TDMA/TDD access mechanism used in this part is the same as that of the DECT. After completion of the first CFP, the channel will be available through CSMA/CA protocol for data access. Then it is left for the CFP voice transmission. The reader interested in more details on HomeRF can refer to [NEG00], [HOM00].

13.4 WHAT IS BLUETOOTH?

Bluetooth is an open specification for short range wireless voice and data communications that was originally developed for cable replacement in personal area networking to operate all over the world. In 1994 the initial study for development of this technology started at Ericsson, Sweden. In 1998, Ericsson, Nokia, IBM, Toshiba, and Intel formed a special interest group (SIG) to expand the concept and develop a standard under IEEE 802.15 WPAN. In 1999, the first specification was released and then accepted as the IEEE 802.15 WPAN standard for 1 Mbps networks. At the time of this writing, over 1,000 companies have participated as members in the Bluetooth SIG, and a number of companies all over the world are developing Bluetooth chip sets. Marketing forecasts indicate penetration of Bluetooth in more than 100 million cellular phones and several millions of other consumer devices. The IEEE 802.15 standard is also studying coexistence among and interference between Bluetooth and IEEE 802.11 products operating at 2.4 GHz.

The story of the origin of the name Bluetooth is interesting and worth mentioning. "Bluetooth" was the nickname of Harald Blaatand (A.D. 940–981), king of Denmark and Norway. When the Bluetooth specification was introduced to the public, a stone carving, shown in Figure 13.3, erected from Harald Blaatand's capital

Figure 13.3 Picture of Bluetooth on the stone [BLUweb].

city Jelling, was also presented [BLU00]. This strange carving was interpreted as Bluetooth connecting a cellular phone and a wireless notepad in his hands. The picture was used to symbolize the vision in using Bluetooth to connect personal computing and communication devices. Bluetooth, the king, was also known as a peacemaker and a person who brought Christianity to Scandinavians to harmonize their beliefs with the rest of Europe. That fact is used to symbolize the need for "religious" harmony among manufacturers of WPANs around the world to support the growth of WPAN industry.

Bluetooth is the first popular technology for short-range, ad hoc networking that is designed for an integrated voice and data applications. Unlike WLANs, Bluetooth has a lower data rate, but it has an embedded mechanism to support voice applications. Unlike 3G cellular systems, Bluetooth is an inexpensive personal area ad hoc network operating in unlicensed bands and owned by the user.

The Bluetooth SIG considers three application basic scenarios that are shown in Figure 13.4 [BLU00]. The first scenario, shown in Figure 13.4(a), is the wire replacement to connect a PC or laptop to its keyboard, mouse, microphone, and notepad. As the name of the scenario indicates, it avoids the multiple short-range wiring surrounding today's personal computing devices. The second scenario is ad hoc networking of several different users at very short range in an area such as a conference room. As we saw in the last three chapters, WLAN standards and products also commonly consider this scenario. The third scenario is to use Bluetooth as an AP to the wide area voice and data services provided by the cellular networks, wired connection, or satellite links. The 802.11 community also considers this over-

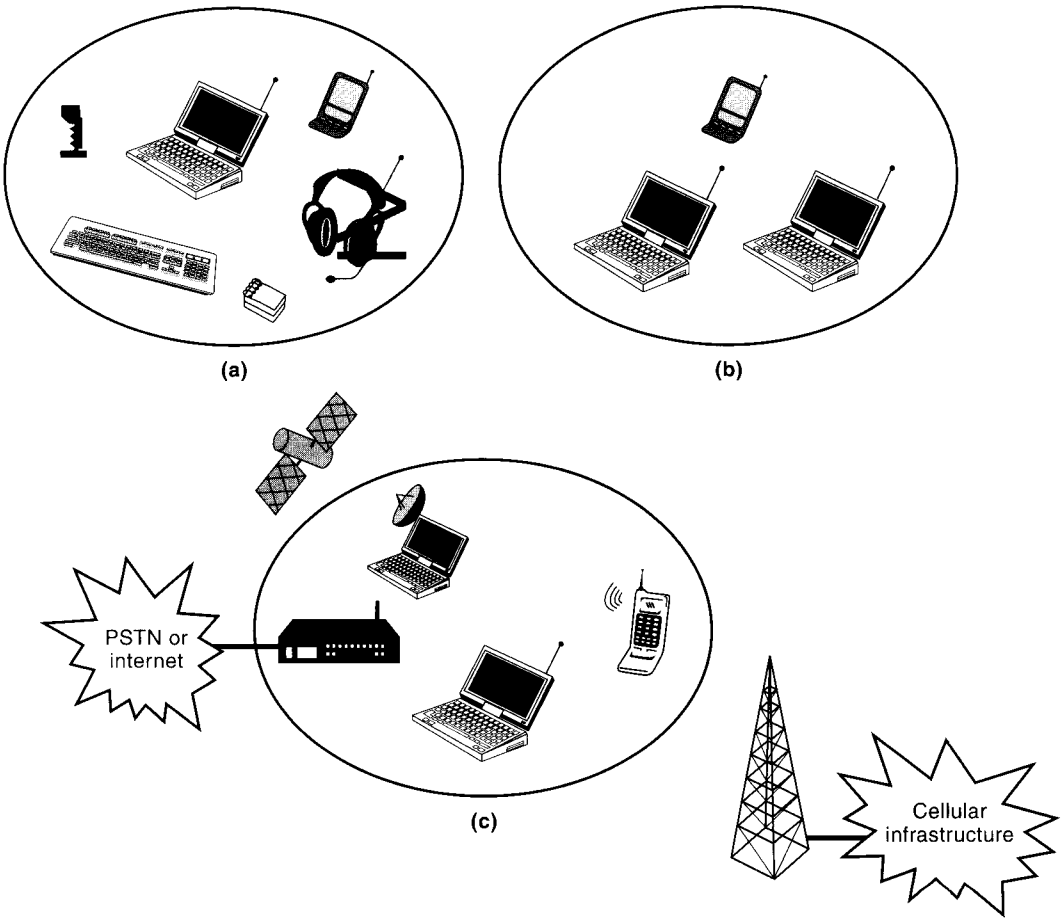


Figure 13.4 Bluetooth application scenarios: (a) cable replacement, (b) ad hoc personal network, and (c) integrated AP.

all concept of the AP. However, the Bluetooth AP is used in an integrated manner to connect to both voice and data backbone infrastructures. The HIPERLAN-2 standard is expected to provide a more comprehensive version of similar connections that supports a larger number of users and wider bandwidths.

13.4.1 Overall Architecture

The topology of the Bluetooth is referred to as *scattered ad hoc topology* that is illustrated in Figure 13.5. In a scattered ad hoc environment, a number of small networks support a few terminals to coexist or possibly interoperate with one another. To implement such a network, we need a plug-and-play environment. The network should be self-configurable, providing an easy mechanism to form a new small network and a procedure for participation in an existing one. To implement that environment, the system should be capable of providing different states for connecting

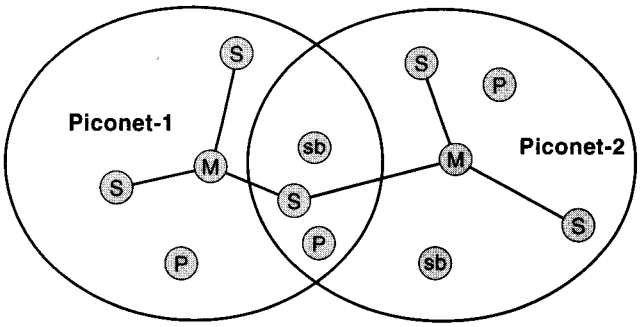


Figure 13.5 Bluetooth's scattered ad hoc topology.

to the network. The terminals should have options to associate with multiple networks at the same time. The access method should allow formation of small, independent ad hoc cells, as well as the possibility of interacting with large voice and data networks considered by Bluetooth.

To accommodate these features, the Bluetooth specification defines a small cell as a *piconet* and identifies four states, Master "M," Slave "S," Stand By "SB," and Parked/Hold "P" for a terminal. Like other ad hoc topologies, such as the one supported by IEEE 802.11, each terminal can be an "M" or an "S." As shown in Figure 13.5, the Bluetooth topology, however, allows "S" terminals to participate in more than one piconet. An "M" terminal in the Bluetooth can handle seven simultaneous and up to 200 active slaves in a piconet. If access is not available, a terminal can enter the "SB" mode waiting to join the piconet later. A radio can also be in a parked/hold, "P," in a low power connection. In the parked mode, the terminal releases its MAC address, while in the "SB" state it keeps its MAC address. Up to 10 piconets can operate in one area [BLU00]. Bluetooth specifications have selected the unlicensed ISM bands at 2.4 GHz for operation. The advantage is the worldwide availability of the bands and the disadvantage is the existence of other users, in particular IEEE 802.11 and 802.11b products in the same band. At the time of this writing, a subcommittee of the IEEE 802.15 is working on the interference issues related to the Bluetooth and IEEE 802.11.

13.4.2 Protocol Stack

One of the distinct features of the Bluetooth is that it provides a complete protocol stack that allows different applications to communicate over a variety of devices. Other wireless local networks, such as IEEE 802.11, specify the three lower layers for communications. The protocol stack for voice, data, and control signaling in Bluetooth is shown in Figure 13.6 [HAA00]. The *RF layer* specifies the radio modem used for transmission and reception of the information. The *baseband layer* specifies the link control at bit and packet level. It specifies coding and encryption for packet assembly and frequency hopping operation. The *link management protocol* (LMP) configures the links to other devices by providing for authentication and encryption, state of units in the piconet, power modes, traffic scheduling, and packet format. The *logical link control and adaptation protocol* (L2CAP) provides

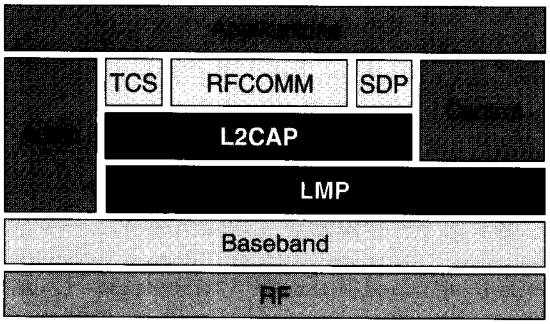


Figure 13.6 Protocol stack for Bluetooth.

connection-oriented and connectionless data services to the upper layer protocols. These services include protocol multiplexing, segmentation and reassembly, and group abstractions for data packets up to 64 kB in length. The audio signal is directly transferred from the application to the Baseband. Also LMP and the application exchange control messages interact to prepare the physical transport to the application.

Different applications may use different protocol stacks but nevertheless all of them share the same physical and data link control mechanisms. There are three other protocols above the L2CAP. The *service discovery protocol* (SDP) finds the characteristics of the services and connects two or more Bluetooth devices to support a service such as faxing, printing, teleconferencing, or e-commerce facilities. The *telephony control protocol* (TCP) defines the call control signaling and mobility management for the establishment of speech for cordless telephone application. Using these protocols legacy telecommunication applications can be developed.

Example 13.1: Telephony Control Protocol in Bluetooth

Figure 13.7 shows the protocol stack for implementation of the cordless telephone application. The audio signal is directly transferred to the Baseband layer while SDC and TCP protocols operating over L2CAP and LMP handle signaling and connection management.

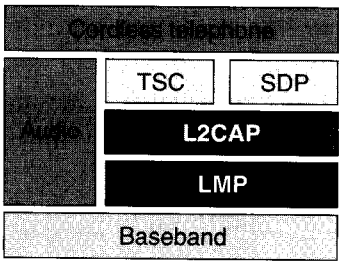


Figure 13.7 Protocol stack for implementation of cordless telephone over Bluetooth.

The *RFCOMM* is a "cable replacement" protocol that emulates the standard RS-232 control and data signals over Bluetooth baseband. Using RFCOMM a number of non-Bluetooth specific protocols can be implemented on the Bluetooth devices to support legacy applications.

Example 13.2: Lightweight Applications in Bluetooth

Figure 13.8 shows the implementation of a vCard application for credit card verification. This application protocol runs over object exchange protocol (OBEX) that is accommodated by the RFCOMM protocol in the Bluetooth protocol stack. Therefore, the sequence of protocols for implementation of credit card verification over Bluetooth is vCard–OBEX–RFCOMM–L2CAP–Baseband–RF. This protocol stack implementation contains both internal object representation convention of vCard and over-the-air transport protocols of the Bluetooth.

Example 13.3: WAP over Bluetooth

Figure 13.9 shows the implementation of a wireless application environment (WAE) protocol that defines applications over the wireless access protocol (WAP). The WAP packets use the TCP/UDP protocols for Internet access on top of the point-to-point protocol (PPP) that runs over the RFCOMM.

The overall Bluetooth protocols can be divided into three classes. The Bluetooth SIG developed the core exclusively Bluetooth-specific protocols for Baseband, LMP, L2CAP, and SDP. The protocols that are also developed by the Bluetooth SIG but based on existing protocols include RFCOMM and TCP. The third group consists of existing protocols that are adopted by Bluetooth SIG. At the time of this writing, these protocols include PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC-1, and WAE. Bluetooth specification is open, and other legacy protocols such as HTTP and FTP can be accommodated on top of the existing protocol stack.

Example 13.4: FTP over Bluetooth

Figure 13.10 provides a protocol stack for implementation of the FTP application. OBEX and RFCOMM manage the data transfer, whereas SDP provides for the establishment of the link.

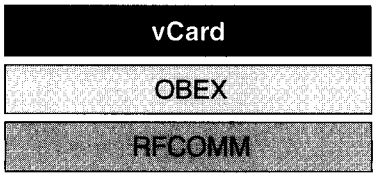


Figure 13.8 Protocol stack for implementation of vCard over Bluetooth.

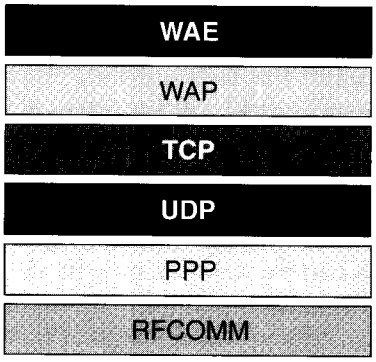


Figure 13.9 Protocol stack for implementation of WAE over Bluetooth.

The overall structure of the protocol stack in the Bluetooth does not clearly follow the OSI model and its acronyms. Therefore, the division of the following section may appear somehow different from other wireless local networks described in the last two chapters. However, we make our every effort to make them as close as what we had in the previous chapters to provide a fluency that comforts the reader in understanding the details and relating them to other details for similar systems.

13.4.3 Physical Connection

The OSI equivalent PHY layer of the Bluetooth is embedded in the RF and Baseband layers of the Bluetooth protocol stack. The physical connection of Bluetooth uses a FHSS modem with a nominal antenna power of 0 dBm (10 m coverage) that has an option to operate at 20 dBm (100 meter coverage). Like the 1 Mbps option of the IEEE 802.11 FHSS standard, the Bluetooth specification uses a two-level GFSK modem with a transmission rate of 1 Mbps that hops over 79 channels in the ISM bands starting at 2.402 GHz and stopping at 2.480 GHz. The hopping rate and pattern and number of hops used in Bluetooth, however, are different from IEEE 802.11. The Bluetooth hopping rate is 1,600 hops per second (625 μs dwell time) as

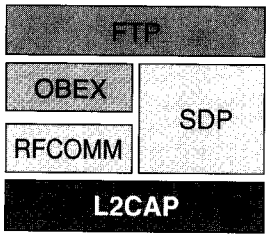


Figure 13.10 Protocol stack for implementation of FTP over Bluetooth.

compared with the 2.5 hops per second (400 ms dwell time) system adopted by the 802.11. The two-level GFSK modem allows simple noncoherent detection implementation using simple FM demodulators. The 0 dBm modem with the Bluetooth hopping pattern complies with the FCC rules in the United States, and due to local regulations, the bandwidth is reduced in Japan, France, and Spain. An internal software switch (which allows an environment for implementation of a system that works universally) handles this transition.

The Bluetooth specification assigns a specific frequency-hopping pattern for each piconet. This pattern is determined by the piconet identity and master clock phase residing in the master terminal in the piconet. Figure 13.11 illustrates the element of frequency hopping strategy in the Bluetooth. The overall hopping pattern is divided into 32 hop segments. The 32-hop pseudorandom hopping pattern segment is generated based on the master identity and clock phase. The 79 frequency hops at the ISM bands are arranged in odd and even classes. Each 32-hop sequence starts at a point in the spectrum and hops over the pattern that covers 64 MHz because it hops either on odd or even frequencies. After completion of each segment, the sequence is altered, and the segment is shifted 16 frequencies to the forward direction. The 32 hops are concatenated, and the random selection of the index is changed for each new segment. This way segments slide through the carrier list to maintain the average time each frequency is used at an equal probability. Change of the clock or identity of the piconets will change the sequence and segment mapping, allowing different piconets to operate with different set of random codes. These codes are not orthogonal to one another, but they are randomized against each other. With 79 hops it is difficult to find a large number of orthogonal codes anyway [HAA00].

To protect the integrity of the transmitted data Bluetooth uses two error-correction schemes in the baseband controllers. An FEC code is always applied to the header information, and if needed it is extended to the payload data for the voice-oriented synchronous packets. The FEC code generally reduces the number of retransmissions. It is always applied to the header because header information is short and important. The flexibility of using FEC for payload provides an option to avoid overhead in favor of increased throughput when the channel is good and error free. An unnumbered ARQ scheme is also applied by the baseband layer for

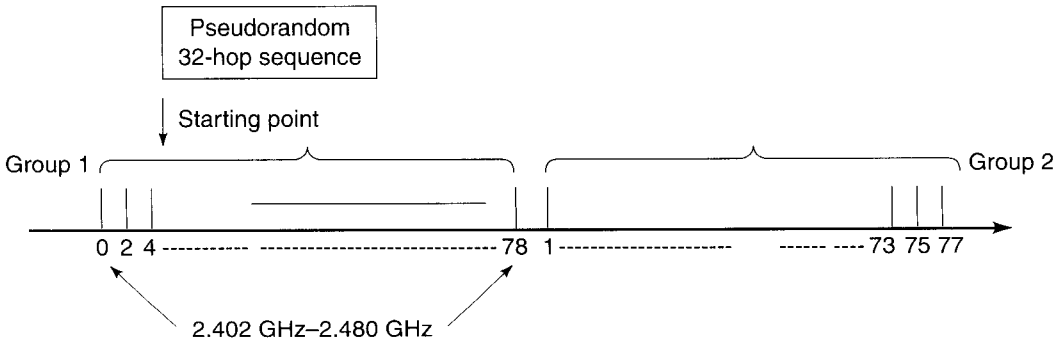


Figure 13.11 The hopping sequence mechanism in Bluetooth.

the asynchronous data-oriented information in which the recipient acknowledges data transmitted. For data transmission to be acknowledged, both the header error check and the payload check, if applied, must indicate no error condition. These functionalities implemented in the Baseband layer of the Bluetooth protocol stack are often implemented in the data link layer of the OSI reference model for networks complying with that model.

13.4.4 MAC Mechanism

Although the modulation technique and frequency of operation of the Bluetooth radio system closely follows that of the FHSS 802.11, the MAC mechanism in the Bluetooth is widely different from the 802.11. The Bluetooth access mechanism is a voice-oriented innovative system that is neither identical to the data-oriented CSMA/CA type nor voice-oriented CDMA or TDMA access methods and yet has elements that are somehow related to these access methods. The medium access mechanism of Bluetooth is a fast FH-CDMA/TDD system that employs polling to establish the link. The fast hopping of 1,600 hops per second allows short time slots of 625 μs (625 bits at 1 Mbps) for one packet transmission that allows a better performance in the presence of interference. Bluetooth is a CDMA system that is implemented using FHSS. In the Bluetooth CDMA, each piconet has its own spreading sequence, whereas in the DSSS/CDMA system used for digital cellular systems each user link is identified with a spreading code. The DSSS/CDMA is not selected for Bluetooth because DSSS/CDMA needs central power control that is not possible in the scattered ad hoc topology envisioned for Bluetooth applications. Without any need to centralized power control for CDMA operation, the FH/CDMA in Bluetooth allows tens of piconets to overlap in the same area providing an effective throughput that is much larger than 1 Mbps. As we discussed in Chapter 11, the FHSS 802.11 operates in the same 79 hops as Bluetooth with only three sets of hopping patterns. The throughput of the Bluetooth FH/CDMA system, however, is less than 79 Mbps which could be achieved in a coordinated FDM or OFDM system employed as in 802.11a and HIPERLAN-2 operating in 5.2 GHz U-NII bands. In Bluetooth, the FH/CDMA is selected over simple FDM or OFDM because ISM bands at 2.4 GHz only allow spread spectrum technology. The access method in each piconet of Bluetooth is TDMA/TDD. The TDMA format allows multiple voice and data terminals to participate in a piconet. The TDD eliminates cross talk between the transmitter and the receiver, allowing a single chip implementation in which a radio alternates between transmitter and receiver modes. To share the medium among a larger number of terminals, at each slot "M" decides and *polls* a "S." Polling is used rather than contention access methods because contention provides too much overhead for the short packets (625 bits) that were selected for the implementation of a fast FHSS system.

13.4.5 Frame Formats

The Bluetooth packet format is based on one packet per hop and a basic 1-slot packet of 625 μsec that can be extended to three slots (1,875 μsec) and five slots (3,125 μsec). This frame format and the FH/TDMA/TDD access mechanism allow

an "M" terminal to poll multiple "S" terminals at different data rates for voice and data applications to form a piconet.

Example 13.5: Operation of Piconets

Figure 13.12 illustrates several examples of Bluetooth operation in a piconet. In Figure 13.12(a), an "M" terminal is communicating with three "S" terminals. The TDMA/TDD format allows simultaneous operation of the three terminals assigning 625 μs (equivalent to 625 bits at 1 Mbps) for transmission and a time gap between the two packets in each direction. Terminals may run different applications (voice or data at different rates), but applications should run on one of the one-slot detailed packet formats that are specified by the Bluetooth SIG. The time gap is specified at 200 μs to allow a terminal to switch from transmitter to receiver mode for the TDD operation [HAA00]. Figure 13.12(b) shows an asymmetric communication in which the "M" uses a higher speed three-slot link, whereas the "S" operates at a lower rate with one-slot packets. Figure 13.12(c) represents a symmetric higher speed three-slot communication, and Figure 13.12(d) an asymmetric very high-speed five-slot with a return low speed one-slot link.

The overall packet structure of the Bluetooth is shown in Figure 13.13. There are 74 bits for the access code field, 54 bits for the header field and up to 2,744 bits for different payloads that can be as long as five slots. In IEEE 802.11 FHSS packets, the preamble and header of the PHY layer, shown in Figure 11.4, were 96 and 32 bits, respectively, whereas the payload could be as long as $4096 \times 8 = 32{,}768$ bits. The size of the overhead is more or less in the same range, but the maximum payload of 802.11 is at least an order of magnitude larger. Apparently Bluetooth uses more flexible shorter packets for ease of integration and better performance

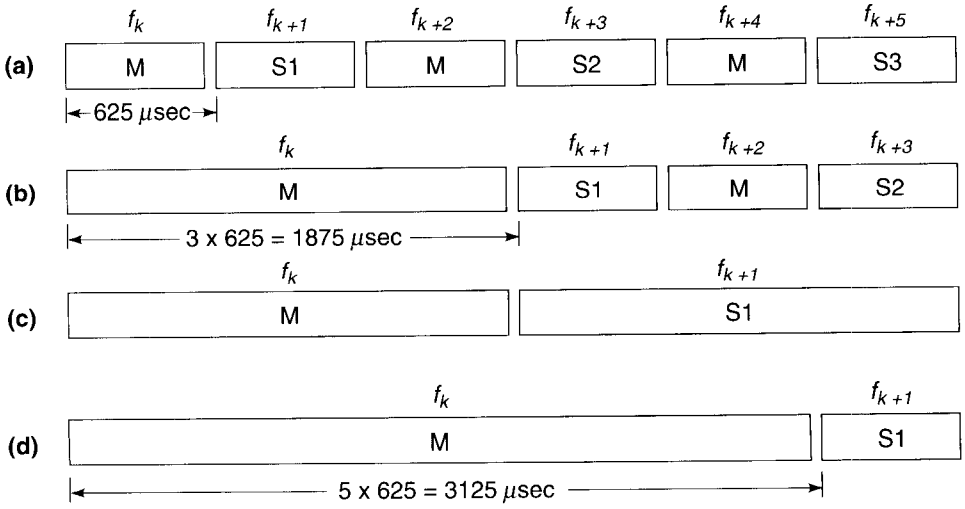


Figure 13.12 FH/TDMA/TDD multislot packet formats in Bluetooth: (a) 1-slot packets, (b) asymmetric 3-slots, (c) symmetric 3-slots (1,875 μsec), and (d) asymmetric 5-slots (3,125 μsec).

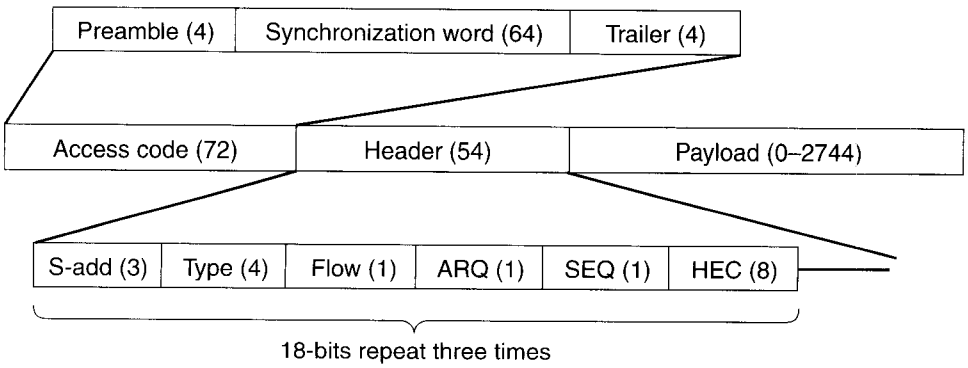


Figure 13.13 Overall frame format of the Bluetooth packets.

in fading, but these gains are at the expense of a higher percentage of overhead that reduces the throughput.

As shown in Figure 13.13, the access code field consists of a four-bit preamble and a four-bit trailer plus a 64-bit synchronization PN-sequence with a large number of codes with good autocorrelation and cross-correlation properties. The 48-bit IEEE MAC address unique to every Bluetooth device is used as the seed to derive the PN-sequence for hopping frequencies of the device. There are four different types of access codes. The first type identifies a "M" terminal and its piconet address. The second type of access code specifies an "S" identity that is used to page a specific "S." The third type is a fixed access code reserved for the inquiry process that is explained later. The fourth type is the dedicated access code that is reserved to identify specific set of devices such as fax machines, printers, or cellular phones.

As shown in Figure 13.13, the header field has 18 bits that are repeated three times with a 1/3 FEC code. The 18-bit starts with a 3-bit "S" address identifying, 4-bit packet type, 3-bit status reports, and an 8-bit error check parity for the header. The 3-bit S-ADD allows addressing the seven possible active "M"s in a piconet. The 4-bit packet type allows 16 choices for different grade voice services, data services at different rates, and four control packets. The 3-bit status reports are used to flag overflow of the terminal with information, acknowledgment of successful transmission of a packet, and sequencing to differentiate the sent and resent packets.

The Bluetooth SIG specifies different payloads and associated packet type codes that allow implementation of a number of voice and data services. Different master-slave pairs in a piconet can use different packet types, and the packet type may change arbitrarily during a communication session. The four-bit packet type identifies 16 different packet formats for the payloads of the Bluetooth packets. Six of these payload formats are asynchronous connectionless (ACL), primarily used for packet data communications. Three of the payload formats are synchronous connection oriented (SCO), primarily used for voice communications. One is an integrated voice (SCO) and data (ACL) packet, and four are control packets common for both SCO and ACL links.

The three SCO packets, shown in Figure 13.14, are high-quality voice (HV) packets numbered as HV1, 2, and 3 to designate the level of quality of the service.

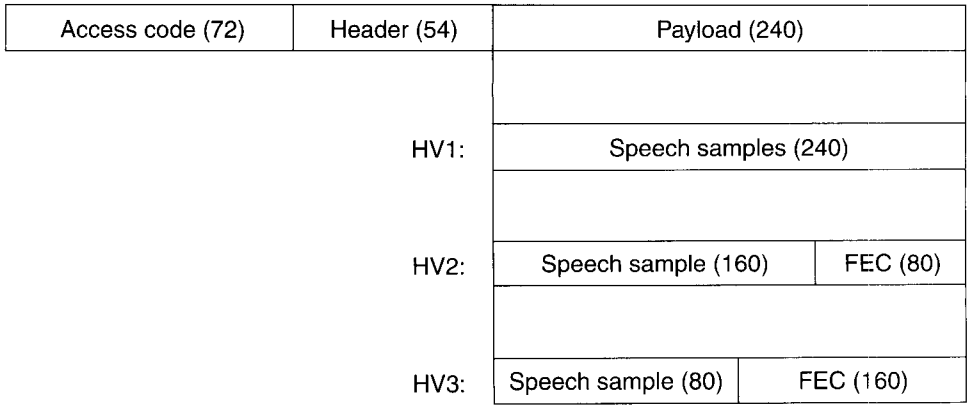


Figure 13.14 SCO 1-slot packet frame formats.

The SCO packets are all single slot packets, the length of the payload being fixed at 240 bits, and they do not use the status report bits, but they are transmitted over reserved periodic duplex intervals to support 64 kbps per voice user. HV1 uses all 240 bits for the user voice samples, HV2 uses 160 bits for user voice samples and 80 bits of parity for a ⅓ FEC code, and HV3 uses 80 bits of user voice samples and 160 bits of parity for a ⅔ FEC code. To keep the data rate for voice samples at 64 kbps, the HV1, HV2, and HV3 packets in each direction are sent every six, four, and two slots, respectively.

Example 13.6: Data Rate of High Quality Voice Packets

The HV1 packets are 240 bits long, and so they are sent every six slots. The packets are 1-slot packets sent at the rate of 1,600 slots/sec. Therefore, we have

$$\frac{1{,}600\ (slots/\text{sec})}{6(slots)} \times 240\ (bits) = 64\ \text{kbps}$$

The overall format of the payload for the six ACL packets is shown in Figure 13.15. The payload has its own 8- or 16-bit header, payload, and 16-bits CRC code. The header has information on the length and identity of the packet. If we want to compare the headers with those of 802.11, we may compare the overhead with the MAC overhead of the 802.11 shown in Figure 11.19. This time the overhead of Bluetooth is significantly lower than the 34 bytes (272 bits) overhead of the 802.11 MAC frames. Most of the saving in the overhead of Bluetooth occurs because 802.11 employs four addresses—source, destination of the device, and the intermediate APs. Bluetooth uses one 48-bit IEEE MAC address to identify a device that is embedded in the access code and is not needed in the payload.

The six ACL packets are data medium (DM) and data high (DH) rate packets numbered as DM or DH1, 3, or 5 according to the length of the slot they take. Figure 13.15 shows the overall frame format of all DM and DH data-oriented packets. DM packets use a rate of ⅔ FEC that improves the quality of the service. DH packets do not employ coding to achieve higher data rates. Using a different number of slots for a packet data payload size, exercising the coding option and changing

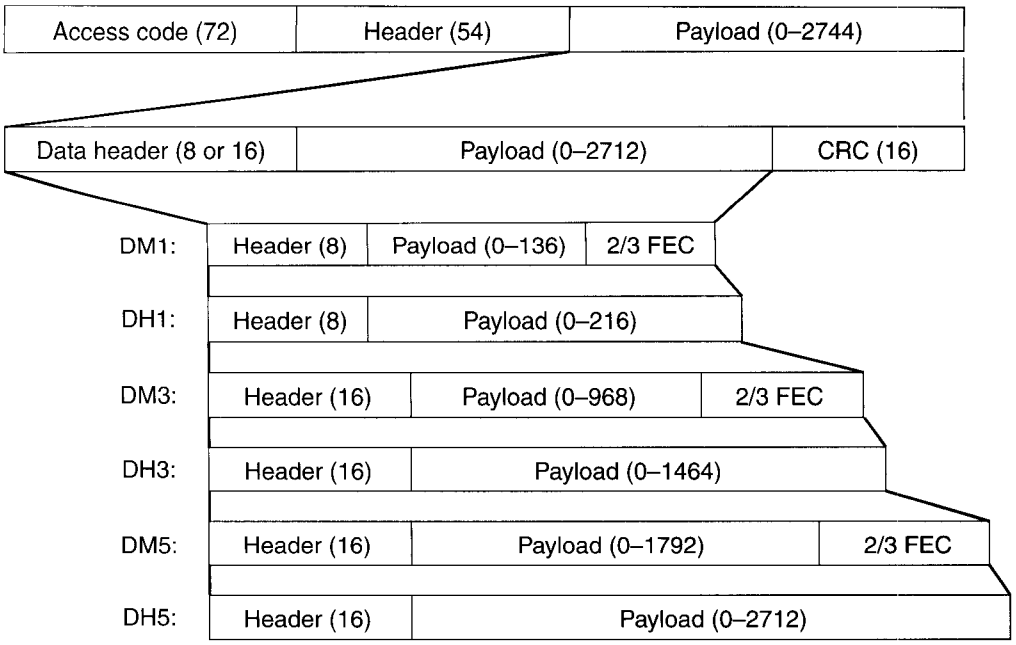


Figure 13.15 ACLs 1-, 3-, and 5-slot packet frame formats.

the symmetric nature of the transmitted packets in each direction, a number of packet data links can be implemented in the Bluetooth specification.

Example 13.7: High Data Rate in Bluetooth

A symmetric 1-slot DH1 link between an "M" and an "S" terminal carries 216 bits per slot at a rate of 800 slots per second (every other slot) in each direction. The associated data rate is 216 (*bits/slot*) × 800 (*slots*/sec) = 172.8 Kbps.

Example 13.8: Medium Data Rate in Bluetooth

The asymmetric DM5 link, shown in Figure 13.15(d) uses five-slot packets carrying 1,792 bits per packet by the "M" and 1-slot packet carrying 136 bits per packet by the "S" terminal. The number of packets per second in each direction is 1,600/6 packets per second. Therefore, the data rate from "M" is given by:

$$1{,}792\ (bits/packet) \times \frac{1{,}600}{6}\ (packets/\text{sec}) = 477.8\ \text{Kbps}$$

The data rate of the "S" terminal in this asymmetric connection is:

$$136\ (bits/packet) \times \frac{1{,}600}{6}\ (packets/\text{sec}) = 36.3\ \text{Kbps}$$

Table 13.1 shows all 12 symmetric and asymmetric data links that are supported with the frame format of the Bluetooth specification. The maximum data rate of 723.2 kbps is available in an asymmetric channel for a single user, with a

Table 13.1 ACL Packet Types and Associated Data Rates in Symmetric and Asymmetric Modes

Type	Symmetric	Asymmetric	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	256.0	384.0	54.4
DH3	384.0	576.0	86.4
DM5	286.7	477.8	36.3
DH5	432.6	~~721.0~~ 723.2	57.6

reverse channel carrying 57.6 kbps. The reader should remember that data applications operate in bursts, and therefore, even if an "M" node communicates with the maximum seven "S" data terminals still most of the time only one of the "S" terminals will communicate with the "M." When more than one "S" terminal simultaneously attempts to communicate with an "M" terminal, the QoS provided to the "S" terminals has to be compromised either by sharing the throughput or by providing additional delays. The decision-making process to reach a compromise in the voice-oriented access methods, such as the one used in Bluetooth, needs a complex algorithm to handle the QoS as negotiated at the start of a session. Comparing this situation with CSMA/CA used in 802.11, there is no negotiation at the starting point. When more than one terminal attempts to communicate with a single AP, the medium is shared, and the compromise is made automatically through the CSMA/CA access method described in Chapter 4. Apparently, for the data-only applications, CSMA/CA is more appropriate, and that is why it was developed by the data-oriented networking industry. However, when voice applications become dominant, the TDMA/TDD type access methods can guarantee QoS for the voice though CSMA/CA cannot do it easily.

The only remaining traffic packet in Bluetooth is a data voice (DV) packet that is a mixed SCO and ACL packet with the same access code and overall header that must be transmitted in regular intervals. The voice part carries 80 bits of voice payload without any coding, and the data part is a short packet of 0–72 bits with a 16-bit ⅔ CRC coding and an eight-bit data payload header. This packet also uses the three status report bits.

The Bluetooth specification also defines four control packets: ID, NULL, POLL, and FHS. The ID packet occupies only half of a slot, and it carries the access code with no data or even a packet type code. This packet is used before connection establishment to only pass an address. The NULL and POLL packet have the access code and the header, and so they have packet type codes and status report bits. The NULL packet is used for ACK signaling, and there is no ACK packet for it. The POLL packet is similar to the to the NULL packet, but it has an ACK. "M" terminals use the POLL packet to find the "S" terminals in their coverage area. The frequency hop synchronization (FHS) packet carries all the information necessary to synchronize two devices in terms of access code and hopping timing. This packet is used in the inquiry and paging process that is explained later.

13.4.6 Connection Management

The link manager (LM) layer and L2CAP layer of the Bluetooth perform the link setup, authentication, and link configuration. An important issue in a truly ad hoc network is how to establish and maintain all the connections in a network whose elements appear and disappear in an ad hoc manner, and there is no central unit transmitting signals to coordinate these terminals. In both digital cellular systems and WLANs, there is a common control or a beacon signal that allows a new terminal to lock to the network and exchange its identity with the networks identity. The Bluetooth specification achieves initiation of the network through a unique inquiry and page algorithm.

The overall state diagram of the Bluetooth is shown in Figure 13.16. In the beginning of the formation of a piconet, all devices are in SB mode, then one of the devices starts with an inquiry and becomes the "M" terminal. During the inquiry process, the "M" terminal registers all the SB terminals that then become "S" terminals. After the inquiry process, identification, and timing of all "S" terminals is

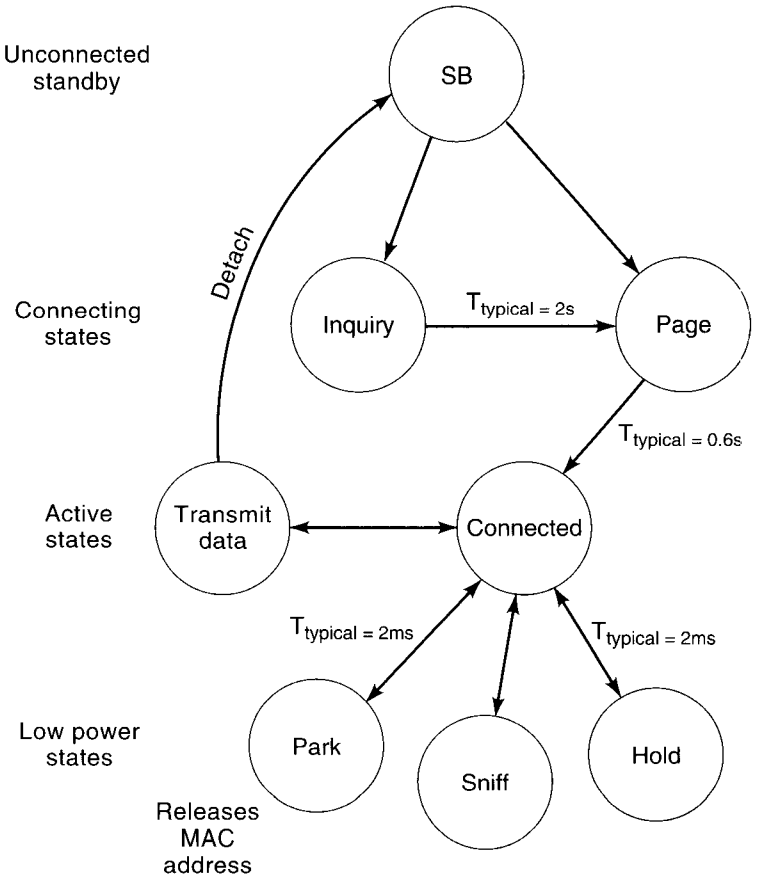


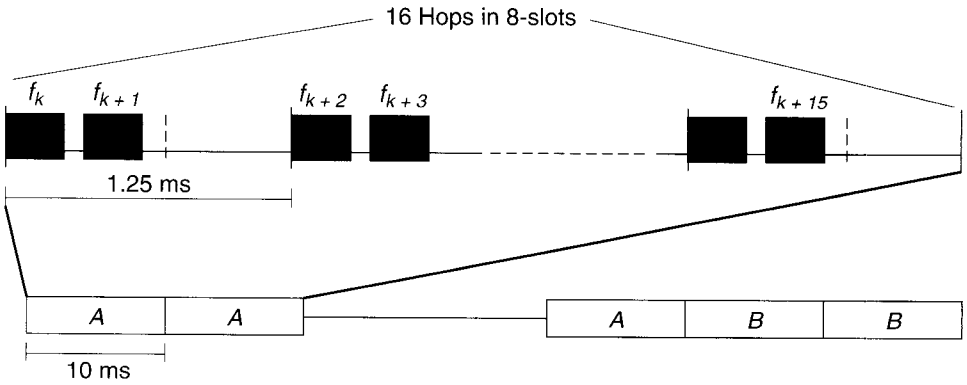
Figure 13.16 Functional overview of the Bluetooth specification.

sent to the "M" terminal using the FHS packets. A connection starts with a PAGE message with which the "M" terminal sends its timing and identification to the "S" terminal. When the connection is established, the communication session takes place, and at the end, the terminal can be sent back to the SB, Hold, Park, or Sniff states. Hold, Park, and Sniff are power-saving options. The Hold mode is used when connecting several piconets together or managing a low-power device. In the Hold mode, data transfer restarts as soon as the unit is out of this mode. In the Sniff mode, a slave device listens to the piconet at reduced and programmable intervals according to the application needs. In the Park mode, a device gives up its MAC address but remains synchronized to the piconet. A Parked device does not participate in the traffic but occasionally listens to the traffic of the "M" terminal to resynchronize and check on broadcast messages.

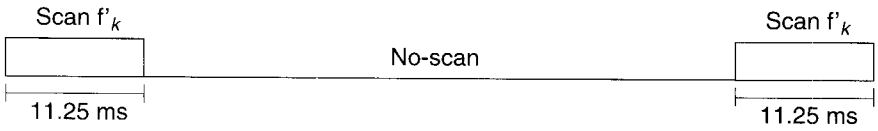
The main innovative part of the inquiry and paging algorithms in Bluetooth is a searching mechanism for two terminals that are not synchronized, but they both know a common address. The following example explains this algorithm.

Example 13.9: Search Algorithm for Synchronization

The two Bluetooth devices knowing a common 48-bit IEEE 802 address of an "M" terminal first use the common address to generate a common FH pattern of 32 hops and a common PN-sequence for the access code of all their packets. Then they start their operation as depicted in Figure 13.17. In the initial state, Terminal 1 sends two ID packets carrying the common access code every half slot on a dif-



(a) Terminal 1



(b) Terminal 2

Figure 13.17 Basic search for paging algorithm in the Bluetooth.

ferent hop frequency associated with the common frequency hopping pattern and listens to the response of the slave in the next slot. If there was no response, it continues broadcasting the ID packets on the two new frequencies in the common hop pattern and repeats this procedure eight times for a period of 10 ms (eight 2-slot times). During these 10 ms, the common ID is broadcast at 16 of the total 32 different hop frequencies. If there is no response, Terminal 1 assumes that Terminal 2 is in sleep mode and repeats the same broadcast again and again until the period of transmission becomes longer than the expected sleeping time of Terminal 2. At this time Terminal 1 assumes that Terminal 2 has scanned, but its scan frequency was not among the 16 hops, designated by A in Figure 13.17 and continues its broadcast with the second half of the 32 hop frequencies, designated by B in the figure. Terminal 2 is in sleeping mode; it wakes up periodically for a period of 11.25 ms to scan the channel at a given frequency for its desirable access code and sleeps again. In each scan period of 11.25 ms, the sliding correlator in Terminal 2 hears the desired address at 16 different frequencies. If one of these frequencies is the same as the scanning frequency, the correlator peaks and synchronization is signaled. Depending on the operation, Terminal 2 can scan the second time at the same frequency or at a new frequency for verification. In either case the objective is to maximize the probability of hitting the same frequency as the broadcast frequency.

The basic principle explained in Example 13.10 is used during the inquiry and paging processes. The following two examples explain these applications for the above mechanism.

Example 13.10: Paging

As in the previous example, the "M" terminal broadcasts repeating ID page trains carrying the access code of the paged terminal two per slot, waits for the response in the next slot, repeats at new hopping frequencies of the paged terminal to cover 16 frequencies every 10 ms, and repeats this for the estimated length of the sleeping time. The "S" terminal scans for 11.25 ms with one of the 32 frequencies of its hopping pattern, then sleeps and scans at the next hopping frequency. When frequencies are the same, a peak appears at the correlator output of the "S" terminal, and the slave responds by sending its own ID packet as an acknowledgment for detection of frequency hoping timing. The "M" terminal then stops broadcasting ID packets and sends an FHS packet containing its own ID and timing information. The "S" terminal responds with another ID packet at the timing of the "M" terminal and then connection is established, and the slave joins the piconet for information exchange. Usually, the "M" terminal knows the approximate timing of the hopping pattern, and 16 most probable hops are adequate to establish the connection. In case this estimate is not correct, like the previous example, the "M" terminal resorts to the second half of the 16 hops when there is no response after the estimated sleeping time.

Example 13.11: Inquiry

The Inquiry message is typically used for finding Bluetooth devices, including public printers, fax machines, and similar devices with an unknown address. The general format of the inquiry process is very similar to the paging mechanism. A

unique access code and FH pattern are reserved for inquiry. In other words, the inquiry process is universally identified with all attributes of a device. Like paging, inquiry starts with an "inquirer" broadcasting an ID packet every half slot at a different hop frequency, covering 16 frequencies every 10 ms, and repeats the same process until it receives responses. The "inquiree" scans with the sliding correlator for 11.25 ms. When the frequencies are the same, the sliding correlator peaks in all devices that are scanning. To avoid collision a device detecting the Inquiry ID runs a random number generator and waits for the length of the outcome before it scans the channel again. When the peak appears the second time after random waiting time, the inquiree terminal sends an FHS packet, allowing the inquirer to learn its ID and timing information. After process is completed, the inquirer's radio has device IDs and clocks of all radios in its range of coverage. After completion of the first inquiry, the inquired device changes its scan frequency and continues scanning for the next inquiry and follow-up FHS signaling.

13.4.7 Security

Bluetooth specifications provide usage protection and information confidentiality. Bluetooth has three modes of operation—nonsecure, service-level, and link-level security. Devices also can be classified into trusted and distrusted. It makes use of two secret keys (128 bits for authentication and 8 to 128 bits long for encryption), a 128-bit long random number, and the 48-bit MAC address of devices. Any pair of Bluetooth devices that wish to communicate will create a session key (called the link key) using an initialization key, the device MAC address, and a PIN number. This protocol has been shown to have several vulnerabilities [WET01] by which a malicious entity could obtain the PIN numbers and keys depending on how the session initialization of the communication protocol is performed [BRA01].

13.5 INTERFERENCE BETWEEN BLUETOOTH AND 802.11

Obviously, when two wireless network overlap in their coverage and operate at the same frequency at the same time without any access coordination, they will interfere with one another. The literature on military communication systems offers many detailed analyses of the performance of communication systems in the presence of various intentional interferers or jammers [SIM85]. These jammers are designed to disrupt the operation of a system, and they can employ relatively sophisticated techniques, such as multitone jamming and pulsed jamming. In civilian applications, the interference is neither intentional nor sophisticated. Most often, the interferer is simply another system designed to operate in a portion of or the entire band of operation of our system, and the users are generally willing to cooperate so as to minimize the mutual interference. Depending on the level of coordination of the overlapping wireless network since the early days of the IEEE 802.11 [HAY91], [WOR91], the WLAN industry has specified three levels of overlapping: interference, coexistence, and interoperation.

Multiple wireless networks are said to *interfere* with one another if colocation causes significant performance degradation of any of the devices. Multiple wireless networks are said to *coexist* if they can be colocated without significant impact on the performance of any of the devices. Coexistence provides for the ability of one system to perform a task in a shared frequency band with other systems that may or may not be using the same set of rules for operation. *Interoperability* provides for an environment for multiple overlapping wireless systems to perform a given task using a single set of rules. In an interoperable environment multiple wireless networks exchange and use the information among each other. Interoperability is an important issue for wired as well as wireless networks. Coexistence and interference are issues mainly consuming the attention of wireless network designers, and it becomes more important for the case of ad hoc networks. This terminology for unlicensed bands was first discussed in the IEEE 802.11 community [HAY91]. Later on when WINForum approached the FCC to obtain unlicensed PCS bands they came up with *etiquettes* or rules of coexistence in unlicensed PCS bands [PAH97] that were introduced in Chapter 10. More recently, the IEEE 802.15 WPAN group is engaged in interference analysis in its task group number two. They have performed introductory interference analysis between Bluetooth and IEEE 802.11 devices operating in 2.4 GHz ISM bands and at the time of this writing are working on practical coexistence and interoperability methods [IEE01, ENN98].

Bluetooth is a fast frequency hopping (1,600 hops per second at 1Mbps) wireless system operating in the 84 MHz of bandwidth that is available in the 2.4 GHz ISM bands that are also used for DSSS IEEE 802.11 (1 and 2 Mbps) and CCK IEEE 802.11b (5.5 and 11 Mbps), as well as slower FHSS (2.5 hops per second at 1 and 2Mbps) IEEE 802.11 systems. Therefore, the interaction between a Bluetooth system and a colocated 802.11 WLAN system needs an analysis of the interference between the FHSS and DSSS, as well as fast FHSS and slow FHSS systems.

13.5.1 Interference Range

The first issue in interference is the *interference range*, which is the distance between two terminals in order to interfere, in case they operate at the same frequency and at the same time. The range of interference is related to propagation characteristics of the environment, processing gain of the receivers, and the transmitted power from different devices. Figure 13.18 illustrates an interference scenario between a Bluetooth (BT-1) device and a receiving FHSS IEEE 802.11 MS colocated in an area. The IEEE 802.11 AP is usually located on the wall to provide better coverage; as a result usually they are less likely to be interfered by the BT devices. The interference takes place both when MS is receiving information from the AP, and BT-1 is transmitting information to BT-2; or when the MS is transmitting and BT-1 is receiving. For our analysis we assume that interference from the AP to the BT devices and interference of the BT-2 device to 802.11 devices are negligible. Following the same analysis for interference presented in Chapter 5, when the MS is receiving and BT-1 is transmitting the signal to interference level at the MS is given by:

$$S_r = \frac{KP_{AP}d^{-\alpha}}{KP_{BT}r^{-\alpha}} = \frac{P_{AP}}{P_{BT}}\left(\frac{r}{d}\right)^{\alpha} \tag{13.1}$$

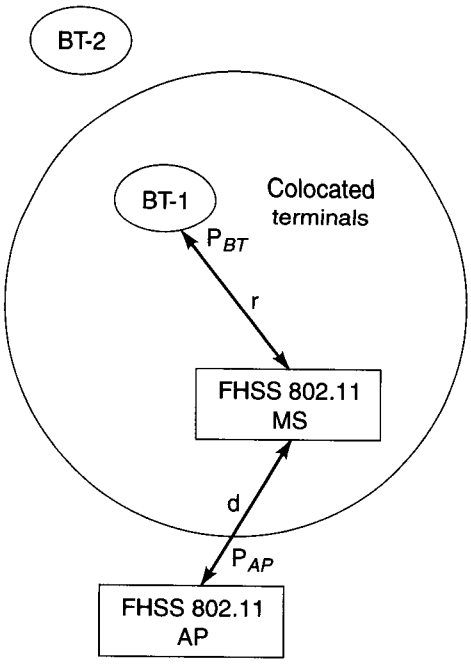


Figure 13.18 The basic interference scenario between Bluetooth and IEEE 802.11 FHSS.

where d and r are the distances between the MS and AP and Bluetooth device, respectively. Also, P_{AP} and P_{BT} represent the transmitted power by the AP and the Bluetooth device, respectively, and α is the distance power gradient of the propagation environment. Therefore the *range of interference* between the Bluetooth and the MS is given by:

$$r_{int} = d\sqrt[\alpha]{S_{min}P_{BT}/P_{AP}} \tag{13.2}$$

where r_{int} is the maximum distance at which the two terminals interfere, and S_{min} is the minimum acceptable received signal to noise ratio needed for proper operation of the MS. In other words, the range of interference of the BT-1 terminal to the MS is directly related to the distance to the AP, required signal-to-noise ratio for proper operation of the MS, and transmit power of BT-1, and it is inversely related to the transmit power of the AP. In general, as we discussed in Chapter 5, the value of α may change from less than two in hallways and open areas up to around six in building with metal partitioning. Depending on the location of the Bluetooth device, the path loss gradients may be different as well. In open areas with no walls, which include a number of scenarios involved with short-range devices, the environment is close to free space propagation and α is often close to 2 [PAH95]. Although the coverage of the 802.11 devices is estimated to be 100 meters (at 20 dBm transmit power), in practice 802.11 APs are installed every 20–40 meters allowing maximum distances of d = 10–20 meters between an AP and a MS. The low power

(0 dBm transmit power) Bluetooth devices are used for WPAN applications where, r, the distance between the devices, is only a few meters. Bluetooth also allows 20 dBm operation that can cover up to 100 m.

Example 13.12: Interference of Bluetooth with FHSS 802.11

a) Assuming an open area with $\alpha = 2$, $S_{min} = 10$ (10 dB), $P_{AP} = 100$ mW (20 dBm), $P_{BT} = 1$ mW (0 dBm), and $d = 20$ m, we have $r_{int} = 6.4$ m. That means if the frequencies of the BT-1 and MS are the same and BT-1 transmits at the same time that the MS receives, a BT-1 device that is closer than 6.4 m to the MS will interfere and destroy the received packets.

b) In a partitioned environment with $\alpha = 4$ we will have $r_{int} = 10.2$ m.

c) If the Bluetooth device is at its maximum transmit power of 100 mW (20dBm) in the same partitioned area, then $r_{int} = 17.7$ m, which is an order of magnitude larger than the value in the 0 dBm mode.

Figure 13.19 illustrates the simple scenario for the interference of FHSS 802.11 to Bluetooth terminals. In this case the MS is transmitting to the AP, and BT-1 is receiving from BT-2. If we assume that the transmitting MS terminal is at a distance r from BT-1 and the two Bluetooth devices are a distance d apart, we have:

$$r_{int} = d\sqrt[\alpha]{S_{min}P_{MT}/P_{BT}} \tag{13.3}$$

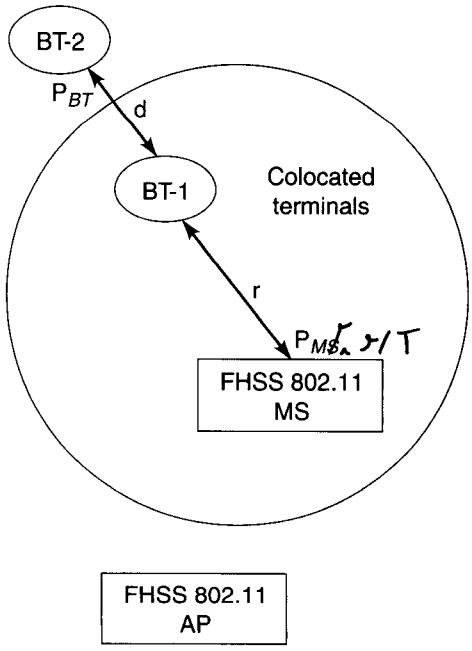


Figure 13.19 The basic interference scenario between FHSS IEEE 802.11 and Bluetooth.

Again the range of interference is directly proportional to the distance between desired terminals, the minimum acceptable signal-to-noise ratio of the receiving terminal, and the power of the interfering terminal, and inversely proportional to the power of the desired transmitter.

Example 13.13: Interference of FHSS 802.11 with Bluetooth

a) With a typical values of 2 m for the distance between the two Bluetooth devices, P_{BT} = 1mW (0 dBm), S_{min} = 10 (10 dB), and P_{MT} = 100 mW (20 dBm), we will have r_{int} = 63.2 m. This is because the 802.11 device is radiating 100 times more power.

b) If the Bluetooth device operates at 20 dBm, with the same power as the 802.11 then r_{int} = 6.32 m.

If instead of FHSS we use DSSS in the scenario of Figure 13.18, as we discussed in Chapter 4, the minimum required received signal to interference ratio at the MS is reduced by a factor equivalent to the value of the processing gain of the DSSS, N. Then, the interference range (BT-1 interfering with MS) becomes:

$$r_{int} = d\sqrt[\alpha]{S_{min}P_{BT}/P_{AP}N} \tag{13.4}$$

For the case of MS interfering with the Bluetooth device, the spectral height of the DSSS is reduced by the value of the processing gain that results in a similar effect and a range of:

$$r_{int} = d\sqrt[\alpha]{S_{min}P_{MT}/P_{BT}N} \tag{13.5}$$

Example 13.14: Interference of Bluetooth with DSSS 802.11

a) Assume an open area with α = 2, S_{min} = 10 (10 dB), P_{AP} = 100 mW (20 dBm), P_{BT} = 1 mW (0 dBm), and d = 20m. For a processing gain of N = 11, used in IEEE 802.11, the interference range will reduce to around r_{int} = 1.9 m (from 6.4 m) (BT-1 interfering with the MS).

b) For P_{BT} = 100 mW (20 dBm), we have an interference range of r_{int} = 19 m.

c) With a typical values of 2 m distance between the two Bluetooth devices, P_{BT} = 1 mW (0dBm), S_{min} = 10 (10 dB), P_{MT} = 100 mW (20 dBm), and N = 11, we will have r_{int} = 19 m (the MS interfering with BT-1).

d) If the Bluetooth device operates at 20 dBm option, then r_{int} = 1.9 m.

The conclusion from these simple examples is that considering the 10 m range of operation of a Bluetooth piconet and a 100 m range of operation of the 802.11 devices, if a Bluetooth hop coincides with frequency of a FHSS or DSSS IEEE 802.11 WLAN, the interference is serious. The DSSS reduces the interference of the narrowband systems and interference to the narrowband system by the value of its processing gain. This results in a $\sqrt[\alpha]{1/N}$ reduction in the range of interference compared with an FHSS system. However, the spectrum of DSSS is much wider and the probability of frequency coincidence of the DSSS and Bluetooth is much

higher than the probability of a hit of a FHSS system and Bluetooth. In the next section, we quantify this statement further.

13.5.2 Probability of Collision

In the last section, we showed that the range of interference of Bluetooth and IEEE 802.11 DSSS is smaller than the range of interference of Bluetooth and FHSS 802.11 systems. However, FHSS is a narrowband signal that changes its frequency of operation randomly while a DSSS is a true wideband system. A narrowband Bluetooth transmitter will interfere with the reception of a wideband DSSS signal with a greater probability than it will with the reception of a FHSS signal on a different narrowband channel. Therefore, the probability of interference between Bluetooth and 802.11 DSSS or 802.11b CCK devices is much higher than the probability of interference between a Bluetooth device and a FHSS 802.11 system.

To further analyze the interference we first pay attention to interference between Bluetooth and FHSS 802.11 devices. Both Bluetooth and FHSS 802.11 are frequency-hopping systems using the 78 carrier frequencies in the 2.4 GHz ISM bands shown in the vertical axis of Figure 13.20. Bluetooth packets are normally shorter than 802.11 packets and hop at a much slower rate of 2.5 hops per second. When a terminal is in the interference range of the other terminal and the hopping

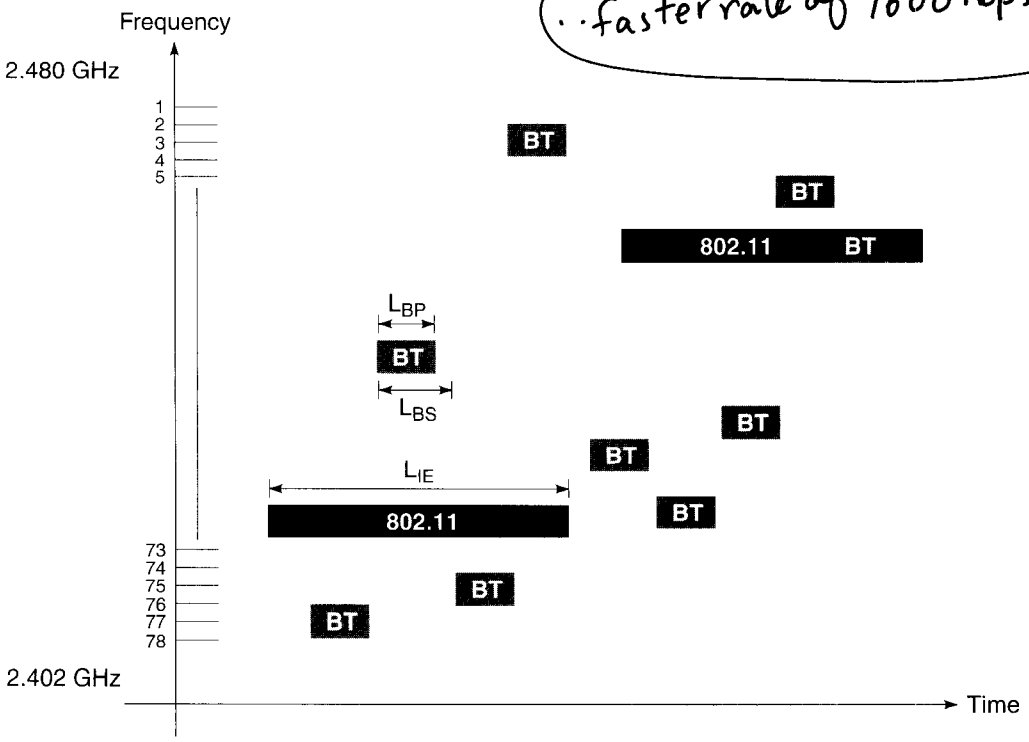


Figure 13.20 Time-frequency characteristics of the FHSS IEEE 802.11 and Bluetooth.

frequencies are the same, packets collide and get destroyed. To analyze this situation, we need to find the probability of collision in time and in frequency.

Because Bluetooth packets are shorter than 802.11 packets, during transmission of one 802.11 packet, the colocated Bluetooth device hops and sends one packet per hop several times. Assuming L_{IE} is the length of the IEEE 802.11 packet and L_{BS} the length of a Bluetooth slot, the minimum number of Bluetooth hops occurring during transmission of one 802.11 packet is $n = [\, L_{IE} / L_{BS} \,]$ where [x] represents the smallest integer greater than or equal to x. The maximum number of Bluetooth hops occurring in duration of an 802.11 packet is $[\, L_{IE} / L_{BS} \,] + 1$. It can be easily shown [ENN98] that the probability of an 802.11 packet overlap with $n = [\, L_{IE} / L_{BS} \,]$ Bluetooth dwell periods of duration L_{BS} is

$$P_n = L_{IE}/L_{BS} - [\, L_{IE}/L_{BS} \,]$$

The probability that it overlaps with $n + 1 = [\, L_{IE} / L_{BS} \,] + 1$ dwell periods is

$$P_{n+1} = 1 - L_{IE}/L_{BS} + [\, L_{IE}/L_{BS} \,]$$

Example 13.15: Overlap between Bluetooth and FHSS 802.11

If $L_{IE} / L_{BS} = 4.3$, the probability of overlap of 802.11 packet with $n = 4$ Bluetooth dwell periods is 30 percent and the probability of overlap with $n+1 = 5$ dwell periods is 70 percent.

Considering these expressions, the probability of an 802.11 packet surviving BT interference, $P_{survive}$, is approximated by:

$$P_{survive} = (1 - P_{hit})^n P_n + (1 - P_{hit})^{n+1} P_{n+1}$$

where P_{hit} is the probability of having the same frequency for both 802.11 and Bluetooth. The probability of collision is given by $P_{collision} = 1 - P_{survive}$.

Example 13.16: Collision between FH-SS 802.11 and Bluetooth

The probability of a Bluetooth hop to occur at the operating frequency of the FHSS system is $P_{hit} = 1/79 = .013$. For a 1,000 byte 802.11 packet at 2 Mbps,

$$L_{IE} = \frac{1{,}000(bytes) \times 8(bits/byte)}{2(Mbits/s)} = 4ms$$

If Bluetooth is sending 1-slot packets $L_{BS} = 625$ μsec. Therefore,

$$n = \left\lceil \frac{4m \text{ sec}}{625 \text{ μsec}} \right\rceil = 6$$

and $P_n = 0.4$ that result in $P_{n+1} = 0.6$. Therefore,

$$P_{survive} = (1 - 0.013)^6 \times 0.4 + (1 - 0.013)^7 \times 0.6 = 0.92$$

and the collision probability is 0.08 or 8 percent.

Example 13.17: Collision between DSSS 802.11 and Bluetooth

Figure 13.21 shows the mechanism with which the frequency-hopping pattern of Bluetooth and the spectrum of the DSSS 802.11 or CCK 802.11b hit one another. The probability of a Bluetooth hop to occur at the operating frequency of the DSSS system is $P_{hit} = 26/78 = 0.33$. For a 1,000 byte 802.11 packet at 2 Mbps, all the other parameters remain the same as the last example, and we have:

$$P_{survive} = (1 - 0.33)^6 \times 0.4 + (1 - 0.33)^7 \times 0.6 = 0.072$$

The probability of collision is 0.928 or 92.8 percent as compared with 8 percent for the FHSS 802.11 example.

Example 13.18: Bluetooth Interference with 802.11b

The IEEE 802.11b uses the same band as 802.11 DSSS to transmit at 11 Mbps. Therefore, again we have $P_{hit} = 26/79 = 0.33$. However, for a 1,000 byte 802.11 packet at 11 Mbps, we have

$$L_{IE} = \frac{1000(bytes) \times 8(bits/byte)}{11(Mbits/s)} = 727\ \mu s$$

With Bluetooth 1-slot packets we have $n = \left\lceil \frac{727m \text{ sec}}{625\ \mu\text{sec}} \right\rceil = 1$ and $P_n = 0.16$, which results in $P_{n+1} = 0.84$. Therefore,

$$P_{survive} = (1 - 0.33)^1 \times 0.16 + (1 - 0.33)^2 \times 0.84 = 0.49$$

The collision probability is 0.51 or 51 percent which is substantially better than 802.11 DSSS and much worse than the 802.11 FHSS.

13.5.3 Empirical Results

The analysis in the last section is at the PHY layer, but a more thorough analysis including the effects of all layers should be done experimentally. A group of undergraduate students at Worcester Polytechnic Institute developed a testbed for the experimental analysis of the interference between the IEEE 802.11b and Bluetooth voice and data channels for their senior undergraduate project [CHA00b]. In this project they considered a number of scenarios and measured the overall packet

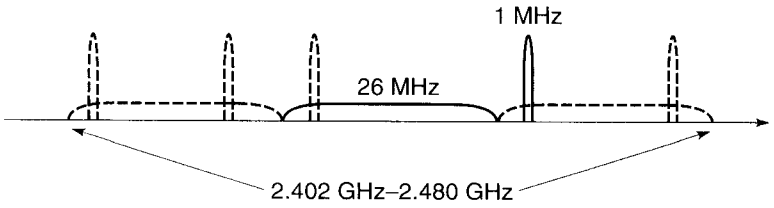


Figure 13.21 Overlapping DSSS IEEE 802.11 and FHSS Bluetooth spectrum.

loss, throughput, and delay characteristics of the interfering Bluetooth and 802.11 devices, as well as cordless telephones. In this section we provide some of their results and conclusions that are related to the scenarios described in Figures 13.18 and 13.19 which relate the performance of interfering 802.11b and BT terminals to the distance between the devices.

Example 13.19: Packet Loss Rate (PLR) in Bluetooth with Interfering 802.11b

Figure 13.22 shows the floor plan and one of the measurement scenarios in which two 20 dBm Bluetooth equipped laptops (triangles) are separated by 10 meters and an 802.11b laptop (circle) is moved from a distance of 1 to 10 meter from the Bluetooth laptop. The 802.11b station is communicating with another laptop that is far away and does not interfere significantly with the Bluetooth device. Figure 13.23 shows the PLR of the Bluetooth device. As the distance of the interfering 802.11 device increases the packet loss reduces. When the Bluetooth and 802.11b interferers are next to one another, the PLR is 70 percent, as the distance increases to five meters, there is no interference effect. The lengths of the 802.11 packets are approximately 1,000 bytes and Bluetooth data packets are 366 bits long. Figure 13.24 shows the delay characteristics evaluated using ping messages that measure the round trip delay [CHA00].

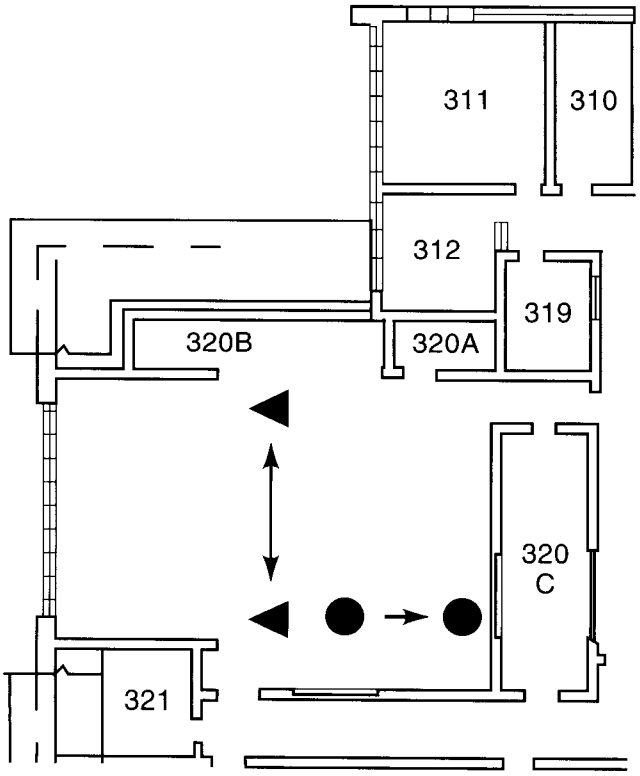


Figure 13.22 Bluetooth interfering scenario for the experiemental interference analysis.

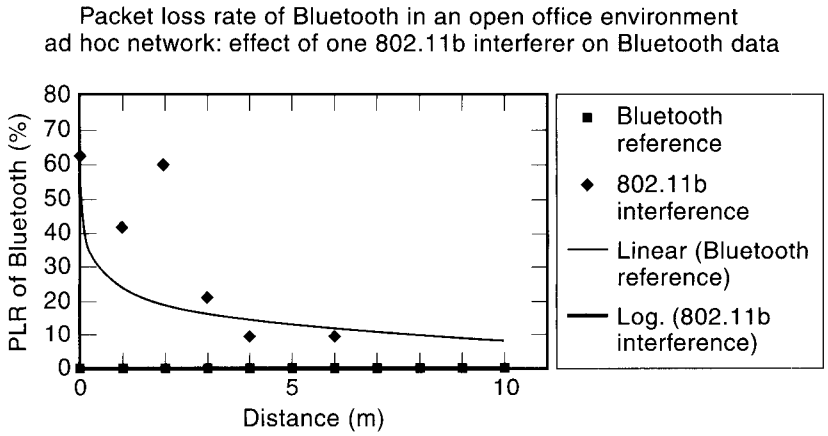


Figure 13.23 Packet loss rate (PLR) of Bluetooth with and without 802.11b interfering terminal.

Example 13.20: PLR in 802.11b with Interfering Bluetooth

Figure 13.25 shows the PLR of 802.11b in a scenario that is the opposite of the last example shown in Figure 13.21. In this example two 802.11b devices are located at a distance of 10 m, and an interfering Bluetooth terminal is moved from one to 10 meters from them. At close distances, the PLR is close to 45 percent, and as the distance of the interfering Bluetooth device increases beyond 3 m, the effects of interference are negligible.

The general conclusion of these studies is that the interference between FHSS 802.11 and BT devices is negligible, however, DSSS 802.11 devices will

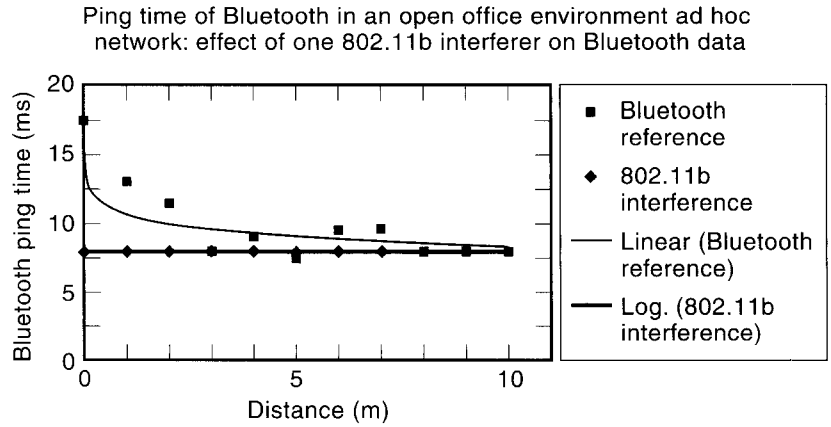


Figure 13.24 Bluetooth delay characteristics with and without 802.11b interference.

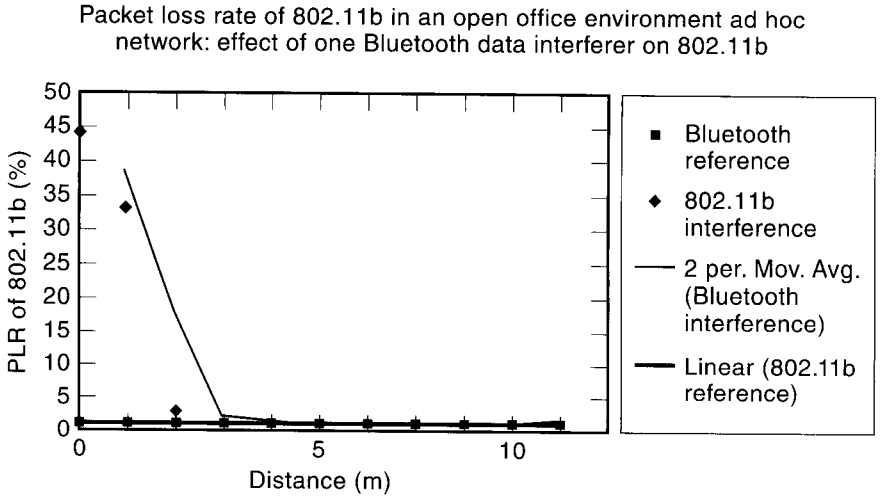


Figure 13.25 802.11b PLR with and without interfering Bluetooth device.

interfere significantly with the BT devices. The IEEE 802.15 is currently working on this issue to find remedies for the coexistence of these systems [IEE00].

QUESTIONS

13.1 What is IEEE 802.15 and what is its relation to the Bluetooth and HomeRF?

13.2 What are the differences between IEEE 802.15 device specification and the device specification of the IEEE 802.11 devices?

13.3 Divide home networking applications discussed in Figure 10.15 into those which can and those which cannot be supported by IEEE 802.15 HomeRF technology.

13.4 Name the four states that a Bluetooth terminal can take and explain the difference among these states.

13.5 Name the three classes of applications that are considered for Bluetooth technology and identify those which can also be 802.11 and HIPERLAN WLAN technologies.

13.6 What are the similarities and differences between the FHSS used in the IEEE 802.11 and Bluetooth in terms of data rate, modulation technique, available frequencies for hopping, speed of the hop, and the number and pattern of the hops?

13.7 What are the differences between ad hoc solutions offered by 802.11 and 802.15?

13.8 What is the difference between the MAC protocol of the Bluetooth and the IEEE 802.11?

13.9 What are the two standard MAC protocols that are combined in the HomeRF SWAP protocol?

13.10 Which IEEE 802.11 standards interfere with Bluetooth and which of these standards has more serious interference condition with it?

13.11 How many different voice services does Bluetooth support and how they are differentiated from one another?

13.12 How many different symmetric and asymmetric data services does Bluetooth support?

13.13 What is the maximum supported asymmetric packet data rate by Bluetooth? How many slots per hop does it use? What is its associated data rate in the reverse channel?

13.14 Compare the header and access code of the Bluetooth with the PLCP header of the FHSS IEEE 802.11.

13.15 What is the maximum data rate of an overlay Bluetooth network? How does it compare with the maximum data rate of the overlay FHSS IEEE 802.11?

13.16 What are the differences between the implementation of paging and inquiry algorithms in Bluetooth?

13.17 Using Figures 13.23 and 13.25 to explain the nature of interference between Bluetooth and IEEE 802.11b.

PROBLEMS

13.1 Give the complete stack protocol for the implementation of an email application over Bluetooth.

13.2 Considering that the encoded voice in Bluetooth is at 64 Kbps in each direction:

- **a.** Use packet format for the HV1 channels to show that these packets are sent every six slots.
- **b.** Use packet format for the HV2 channels to find how often these packets are sent.
- **c.** Repeat (b) for HV3 packets.

13.3 **a.** What is the hopping rate of Bluetooth and how many bits are transmitted in each one slot packet transmission?

- **b.** If each frame of the HV3 voice packets in Bluetooth carries 80 bits of the samples speech, what is the efficiency of the packet transmission (ratio of the overhead to overall packet length)?
- **c.** Determine how often HV3 packets have to be sent to support 64 kbps in each direction.
- **d.** The DH5 packets carry 2,712 bits per each five-slot packet. Determine its effective data rate in each direction.

13.4 Repeat Examples 13.7 and 13.8 for all other data rates supported by Bluetooth shown in Table 13.1.

13.5 Consider the Bluetooth and FHSS IEEE 802.11 interference scenario of Figure 13.18:

- **a.** Assuming that the acceptable error rate for the MT is 10^{-5}, determine the S_{min} that supports this error rate (use the FSK formulas in Chapter 3 for approximate calculation of S_{min}).
- **b.** Using S_{min} of (a) and Eq. (13.2), calculate r_{in} for d = 10 m, α = 2, P_{BT} = 20 dBm and P_{AP} = 20 dBm.
- **c.** Produce a computer plot to illustrate the relation between r_{in} and acceptable error rates between 10^{-2} and 10^{-7}(in logarithmic form). Using the computer plot, discuss the impact of error rate requirement on the range of interference between Bluetooth and FHSS IEEE 802.11. Assume the rest of parameters are the same as (b).
- **d.** Produce a computer plot to illustrate the relation between r_{in} and distance-power gradient of the medium for values of α between 1.5 and 6. Using the computer plot, discuss the impact of medium on the range of interference between Bluetooth and FHSS IEEE 802.11. Assume the rest of parameters are the same as (b).

e. Repeat (c) and (d) for P_{BT} = 10 dBm. Compare the results with associated results in the previous parts and discuss the effects of power level in the interference.

13.6 Consider the FHSS IEEE 802.11 and Bluetooth interference scenario of Figure 13.19.

a. Assuming that the acceptable error rate for the Bluetooth is 10^{-5}, determine the S_{min} that supports this error rate. Use equations in Table 3A.1 for calculation of S_{min}.

b. Using S_{min} of (a) and Eq. (13.3), calculate r_{in} for d = 10m, α = 2, P_{BT} = 0 dBm and P_{AP} = 20 dBm.

c. Produce a computer plot to illustrate the relation between r_{in} and acceptable error rates between 10^{-2} and 10^{-7}(in logarithmic form). Using the computer plot discuss the impact of error rate requirement on the range of interference between FHSS IEEE 802.11 and Bluetooth. Assume the rest of parameters are the same as (b).

d. Produce a computer plot to illustrate the relation between r_{in} and distance-power gradient of the medium for values of α between 1.5 and 6. Using the computer plot discuss the impact of medium on the range of interference between FHSS IEEE 802.11 and Bluetooth. Assume the rest of parameters are the same as (b).

13.7 Repeat Problem 13.5 if the FHSS IEEE 802.11 device is replaced by a DSSS IEEE 802.11 device.

13.8 An FHSS IEEE 802.11 and a Bluetooth device are operating in close vicinity to each other. Generate a computer plot illustrating the probability of collision of their packets versus the size of the FHSS packet. Using the results of computer plots, explain the impact of packet length on the probability of collision between FHSS IEEE 802.11 and Bluetooth. Note that the maximum length of the 802.11 packets is specified by the standard.

13.9 Repeat Problem 13.7 for interference analysis between the DSSS IEEE 802.11 and Bluetooth.

13.10 Repeat Problem 13.9 for interference analysis between the CCK IEEE 802.11b and Bluetooth.

13.8