7 Wireless Personal Area Networks – Bluetooth, UWB and Sensor Networks

Case Study: BMW Unveils "Tomorrow's Mobile Office" and Saab Provides Bluetooth Phone in Cars

BMW, in cooperation with Intel, have unveiled a prototype BMW 7 Series, a car that also doubles as a mobile office. The main computing system in this mobile office is based on a Tablet PC fitted into the armrest on the back seat. This PC supports a Bluetooth-enabled printer and a fax machine. For wireless connectivity to the outside world, the car has an access point which connects to GPRS and 3G cellular telephone networks (called UMTS – Universal Mobile Telecommunications System). This cellular network can be used for wireless data services such as emails, web browsing, and corporate computing. The main idea is that from the back seat of your car, you can conduct business and thus have an office on the move. In addition to BMW, other auto companies such as Toyota are working on similar projects.

Saab, also a major automobile provider, has looked to make the use of mobile phones easier and safer in their 9-3 series of automobiles. Integrating a hands-free system into their 9-3 series was not purely for convenience but also in response to recent restrictions of mobile phone use in cars. By integrating the hands-free system into their cars, drivers of the 9-3 can avoid fines in many areas of the United States, as well as countries in Europe and Asia. Saab chose Bluetooth wireless to implement the integrated hands-free system due to its ease of use, industry support, and lack of wires. Because Bluetooth supports automatic detection, using Saab's integrated hands-free system is very easy. When the driver enters the car with a Bluetooth-enabled mobile phone, the car automatically detects the phone's presence. From this point, the driver tells the 9-3's speech recognition system who to call. The 9-3 then uses Bluetooth to dial the number and streams the audio conversation to and from the mobile phone and the driver. The car also has a Bluetooth Data Communication sub-system to allow the 9-3 to download a phone book from the mobile phone or a PDA via OBEX, a data transfer protocol. By downloading the phone book, the user can now use voice recognition to dial by name as well as by phone number. Also, the Bluetooth Data Communication sub-system allows PDA's, laptops, and other devices to access the Internet by interfacing with the mobile phone via dial-up mode.

In the same vein, Intel is developing wireless devices to support mobile and fixed offices. The company has developed a variety of home PCs and "entertainment PCs," which resemble DVD players and can connect wirelessly to a PC to display movies to screens around the home. Intel also has developed new chipsets that are designed to improve the playback of video and other motion graphics on home PCs.

Source:

J. Niccolai, "Intel and BMW Unveil 'Tomorrow's Mobile Office,'" March 19, 2004, http://www.computerweekly.com/Article129327.htm

"Built-in Bluetooth keeps Saab drivers' hands free," Cambridge Silicon Radio, Dec. 11, 2003 – http://www.electronicstalk.com/news/cam/cam155.html

7.1 Introduction

Wireless Personal Area Networks (WPANs) are a special class of wireless LANs that support electronic devices in close proximity to each other (around 10 meters). Also known as short-range radios, WPANs are thus targeted for smaller and simpler LANs for home networking and wireless device attachments. Although the IEEE 802.11 LANs with a distance of 100 meters and data rates from 11 to 54 Mbps are quite popular, WPANs such as Bluetooth have found many niche applications in home networking and small office settings. In addition, cordless phones and "HomeRF" devices are being used as WPANs. Recent developments such as UWB (Ultra Wideband) wireless are being included in WPANs, and special alliances are being formed to foster cooperation in specific areas. An example is the Zigbee Alliance formed to promote standards for sensors and control devices. An interesting area of development is Wireless sensor networks (WSNs), which typically consist of small, low-powered devices (sensors) for monitoring the temperature, motion, and other attributes of a physical location. WSNs are typically based on the ad hoc network model because the sensors start communicating with each other just by being in each other's vicinity.

WPANs are driven by slightly different requirements than the wireless LANs. For example, the small appliances and sensors do not necessarily need high data rate. Instead, low battery consumption may be more important. However, it is also important to address issues such as security, interoperability, reliability and management if a WPAN solution is to migrate from the small office home office (SoHo) environment to an enterprise-class organization.

This chapter gives an overview of WPAN technologies with special attention to Bluetooth. Home networking and Home RF are used for general context setting. Recent developments such as UWB and wireless sensor networks are reviewed briefly but will be discussed in a later chapter on emerging wireless networks (Chapter 10). As we will see, there are different and competing standards in WPANs that are driven by different technical and business reasons. The chapter concludes by summarizing the main tradeoffs between the key players.

Chapter Highlights

- Due to the short-range nature of WPANS, unique situations in applications, frequency allocation, location management, and multiple access techniques arise.
- Most WPANs use the ad hoc network model so that two devices start communicating as soon as they are in the range.
- The IEEE 802.15 Working Group (WG) has been formed to develop standards for WPANs. As a starting point, the group accepted significant parts of the Bluetooth specification without modification and has now initiated several subtasks concentrating on high data rate (e.g., UWB) and low data rate (e.g., wireless sensor) networks.
- Cordless phone networks and Home RF have been an active area of work but have slowed down now considerably because of the popularity of Bluetooth, Wi-Fi and other competing technologies.
- Bluetooth is a low data rate and short distance (1 Mbps over 10 meters) WLAN that was: developed for users to connect a wide range of mobile devices quickly and easily, without cables. Bluetooth:
  - Operates in a globally available unregulated band of 2.4 Ghz (ISM band in US).
  - Facilitates real-time voice and data transmissions.
  - Is designed to eliminate the need for numerous, often proprietary, cables.
  - Supports ad hoc networking; i.e., a device equipped with a Bluetooth radio establishes instant connection to another Bluetooth radio as soon as it comes in range.

  - Raises some security concerns, like other wireless networks.
- Ultra Wideband (UWB) is emerging as a new wireless personal area network technology that promises high data rates (around 50 Mbps) in very short distances (10 meters). Originally designed for military applications, UWB is a radio system that uses narrow pulses (millions of pules per second) for communication and sensing by using short-range radar.
- Wireless sensor networks (WSNs) typically consist of small, low-powered devices (sensors) that allow the physical environment to be monitored at high resolution. WSNs use the ad hoc network model and present several unique challenges due to the very limited power of the sensors.
- The ZigBee Alliance has been formed to provide a standardized set of network solutions for sensor and control systems. The main emphasis of ZigBee has been to drive the WPAN standards (in particular, the IEEE 802.15.4). In fact, the ZigBee Alliance is so influential that the devices conforming to 802.15.4 are becoming known as “ZigBees.”

The Agenda
- Principles and Home Networking
- Bluetooth and UWB
- Sensor Networks and Examples

7.2 Principles and IEE 802.15 Standards

7.2.1 Principles and Technical Foundations at a Glance

In principle, a WPAN is a small wireless local area network, thus the basic concepts and technologies discussed in the previous chapter apply. However, as compared to most other wireless networks, WPANs use an ad hoc network model in which there is no need for an access point or a base station for the mobile units to communicate with each other. In a mobile ad hoc network, also known as ***MANET (Mobile Ad hoc Network***), the network devices “discover” each other when they are in each other’s company without pre-planning. For example, Bluetooth is based on MANET and supports automatic detection. This is why the Saab’s integrated hands-free system, described in the opening case study, is very easy to use – when the driver enters the car with a Bluetooth-enabled mobile phone, the car automatically detects the phone’s presence and establishes communication with it. The main advantage of ad hoc networks is that they are self-organizing wireless networks composed of mobile stations that communicate with each other in a peer-to-peer manner without a fixed and pre-planned infrastructure with access points, etc. We introduced MANETs in the previous chapter and will take a closer look at this topic in Chapter 10. Bluetooth and WSNs are good practical examples of MANETs.

Besides the use of MANET, the technical foundations of WPANs are similar to WLANs. Thus we can easily re-use our framework of data rate and distance covered, target applications, frequency allocation, location management, and multiple access shown in Table 7-1.

7.2.1.1 Data Rates and Distance Covered

Commonly used WPANs such as Bluetooth deliver 1 Mbps over 10 meter distance. However, there are exceptions. For example, UWB delivers much higher data rates (around 54 Mbps). In addition, sensor networks have much shorter distance -- a few centimeters in case of RFID networks.

7.2.1.2 Target Applications

The applications targeted for WPANs are mostly data applications for short-range radio and home networking situations. These applications are intended for cable replacement and/or communications between appliances, sensors, controllers and other such devices over short ranges. These applications, as stated previously, use the mobile ad hoc network model – there is no need for an access point, although one can be used to connect to the Internet or corporate networks.

7.2.1.3 Frequency Allocations

WPANs mostly use unregulated bands. For example, Bluetooth uses the ISM band. The use of unregulated bands has two major implications: a) the users do not have to pay a usage fee, and b) greater interference from other devices that also use these bands is possible.

7.2.1.4 Location Management

This is not crucial because in WPANs, mobility of users (senders and receivers) is low. Due to the extremely short communication distances (10 meters) the senders and receivers do not travel far from each other (just how far do you want your keyboard from your computer screen!). Thus extensive location management is not needed. In some cases, it is altogether ignored. For example, cordless phones only work in small areas (a home, for example). Once you are outside this range, you have nothing – no roaming support, no handoffs between cells, complete silence.

7.2.1.5 Physical Communications

At the physical communication level, multiple access mechanisms is important because contention and interference from other devices can be high. One of the main reasons is that WPANs typically operate in unregulated frequency bands which are very crowded. For example, Bluetooth operates in the same band (ISM at 2.4 GHz) as the very popular Wi-Fi LANs. The techniques used are mainly based on spread spectrum (FHSS or DSSS). As discussed in Chapter 5, spread spectrum sends signals in such a fashion that only the receiver with the right code can understand it – the others receive a noise. This reduces the interference.

Of course, forward error correction (FEC) and ARQ is used for handling errors. A combination of PSK and FSK is used for modulation. Some short-range systems such as cordless phones use a multiplexing technique called Time Division Duplex (TDD) to support multiple users simultaneously. This scheme is much simpler than the FDMA-TDMA techniques used in cellular and satellite systems. We will discuss TDD later.

Table 7-1: Basic Information about WPANs

Factor	Key Points
Data Rates and Distance Covered	1 Mbps for about 10 meter distance. are most common
Target Applications	Mostly data applications for short-range radio and home networking applications
Frequency Allocations	Mostly in unregulated bands (mostly ISM)
Location Services	Extensive location management is not needed
Physical Communications, Signal Encoding, Error Correction	Mainly spread spectrum: FHSS or DSSS for multiple access. Forward error correction used in error correction. For signal encoding, a combination of PSK and .FSK are used, Some systems use called Time Division Duplex (TDD).

7.2.2 IEE 802.15 Standards for WPANs – A Quick Overview

Wireless personal area networking is an area of tremendous activity at the time of this writing. The IEEE 802.15 Working Group (WG) has been formed to develop standards for WPANs consisting of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, sensors, control devices, and consumer electronics. As a starting point, the group accepted significant parts of the Bluetooth specification without modification and enriched it with various other features and considerations. The work of 802.15 WG is currently divided into the following task groups:

- **802.15.1 (Bluetooth):** This Task Group has reviewed and provided a standard adaptation of the Bluetooth Specifications.
- **802.15.2 (Coexistence).** This Task Group is developing Recommended Practices to facilitate coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11). Because the WPANs and WLANs have to coexist in many situations, the group is specifying the mutual interferences and the coexistence mechanisms between these two technologies.
- **802.15.3 (WPAN High Rate).** This Task Group is working on a standard for high-rate (20 Mbps or greater) WPANs. This standard is also intended to provide for low-power and low-cost solutions needed in portable consumer digital imaging and multimedia applications.
- **802.15.3a (WPAN Higher Rate).** This Task Group is chartered to develop a new standard for a higher speed (110 Mbps or greater) needed by streaming video and other multimedia applications. A new physical layer (PHY) is being developed by this Task Group for such high data rates.
- **802.15.4 (WPAN Low Rate).** This Task Group is investigating a low data rate solution with multi-month to multi-year battery life and very low complexity. This standard specifies 250 Kbps in the 2.4 GHz band and 20 Kbps-40 Kbps in the 868 MHz bands. The target applications for this standard are sensors, interactive toys, smart badges, remote controls, and home automation.

Different Task Groups (TGs) have different levels of activities. For example, the 802.15.1 TG has been in hibernation for a while because the basic work is done. However, the 802.15.3a

TG is working actively on UWB (Ultra Wideband Communication). Similarly, the **ZigBee Alliance**, an alliance of sensors and control devices, is driving the IEEE 802.15.4 standard.

The best source of information about 802.15 is the official website (http://www.ieee802.org/15/), obviously! The site (www.polowireless.com) has a section on 802.15 that includes industrial developments and breaking news in this area. The book by [Gutierrez 2003] has a great deal of technical information on this topic.

POTS and PANs

In many cases, personal area networks (PANs) such as Bluetooth need to connect to POTS (plain old telephone system). For example, a Bluetooth-enabled car provides access to a regular telephone through wireless. This is an example of putting POTS and PANS together to solve real-life problems!

7.3 Wireless Home Networks: Cordless Networks and HomeRF

7.3.1 Overview of Wireless Home Networking

Many people want to wander around their homes while having continual access to a home network. For example, I usually use a laptop sitting in the living room. There is a desktop computer upstairs with cable modem access – a printer is also connected to the desktop. If I want to print a file currently on my PC, then I have to copy the file to a floppy and take it upstairs to print. However, if the file is too large to fit on a floppy, then I have a major problem. I have to disconnect the printer from the desktop, connect it to my laptop and then print. Similarly, if I need Internet access, I have to go upstairs to access the Internet. A wireless home network is an interesting solution for people like me who want to roam around their homes and be connected to a network, a printer, and other such things. The following factors drive the wireless home data networking market:

- The explosive growth and usage of the Internet for delivery of information and entertainment into the home
- The widespread emergence of cheaper home PCs (less than $1000) allows middle-income households to obtain a PC if they so wish.
- Home PCs, printers and general computer peripherals can only be reached within a 3-foot diameter. This shortcoming offers a huge opportunity for wireless home networking (who wants 50 feet cables connecting their PCs and computing devices!).

Of course 802.11-based wireless LANs can be used at home, but wireless networks, cheaper and easier to install and maintain, are desirable for home markets. In particular, wireless home networking solutions should satisfy the following requirements [Dhir 2001]:

- No new wiring infrastructures should be needed.
- The solutions must also be simple to install and easy to use.
- Interoperability with other networks such as phone line-based home networks is also essential.
- Solutions need to be economical and home security cannot be compromised.
- Distances should be large enough for consumers who own large households.

Figure 7-1 shows a conceptual view of a wireless home network that connects laptops, desktops, printers, phones and other devices though a wireless network. We will revisit this view later. Wireless networks in a household have the obvious advantage of providing access from anywhere at any time. However, security is a big concern because eavesdropping on a wireless network is much easier than on a wired one.

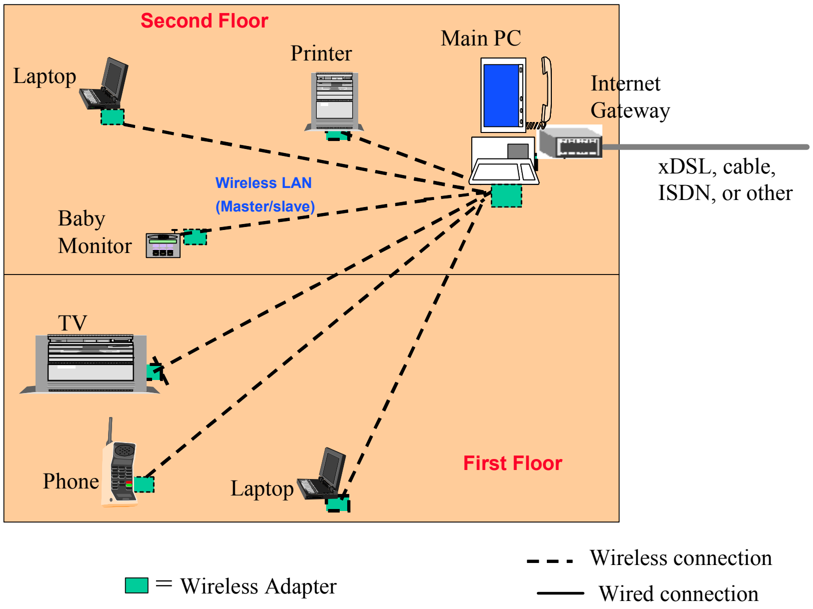


Figure 7-1: Conceptual View of a Home Network

Market research analysts are predicting steady growth in the home wireless solutions. According to Strategy Analytics, 19 percent of the households in the U.S. and 15 percent of European households are expected to have wireless home networks by the year 2005. Although the market outlook is good for wireless home networks, they present a variety of technical and deployment challenges. The main challenge is that there are many choices such as the following:

- Cordless networks
- Home RF
- Bluetooth
- Wireless Ethernet (802.11) networks

We have discussed 802.11 in a previous chapter. We will discuss the others here.

7.3.2 Cordless Networks

7.3.2.1 Overview of Cordless Networks

Cordless phones are a special class of cellular networks in which the cell sizes are very small (less than 100 meters, typically) and there is no need for location and roaming support. Each cordless telephone, for example, comes with its own base station and needs to be only compatible with that base station (see Figure 7-2). The base station unit is connected to the regular PSTN and acts as the base transceiver for the handset. However, the handset cannot wander too far off. Thus the cordless phones are typically used within a house or a small office. Because the handset cannot be more than a few feet away from the base station, cordless networks do not need location registry or roaming support. Thus the extensive location-based services discussed in Chapter 5 are not needed. In addition, since the base station and the handset are owned by the same entity, the need for standards for cordless phones has been minimal. But this is beginning to change now.

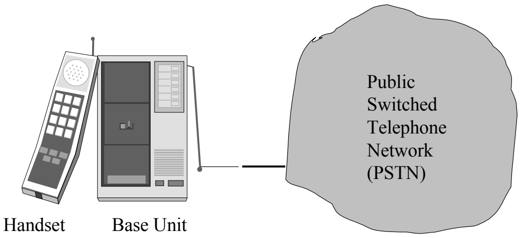


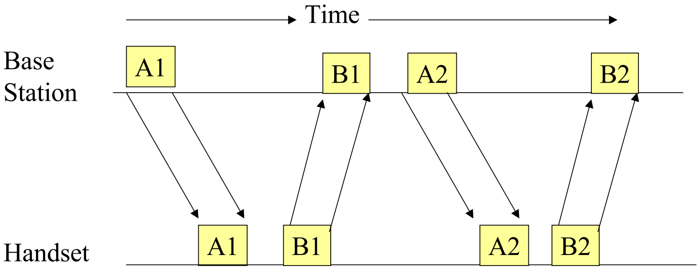
Figure 7-2: A Cordless Phone System

Cordless systems most commonly operate in residential settings, where a single base station can provide in-house voice and data support. Cordless systems can also be used in ***small office home office (SoHo)*** environments where a single base station can support a small office. However, multiple base stations in a cellular configuration can support a larger office. Another possible application of cordless systems is a telepoint where a base station is set up in a public place, such as an airport or a shopping mall.

7.3.2.2 Design Considerations for Cordless Standards

Design of a cordless network differs from a cellular network in several fundamental ways. First, the range of handset distance from base station is modest, so low-power designs are used. Second, inexpensive handset and base stations dictate simple technical approaches. Finally, the cordless system needs to be able to seek low-interference channels for its users because frequency flexibility is limited.

For these reasons, a technique called **Time Division Duplex (TDD),** also known as time-compression multiplexing, is used in cordless systems to support multiple users. This scheme is much simpler than the FDMA-TDMA techniques used in cellular and satellite systems. In TDD, data is transmitted in one direction at a time, with transmission between the two directions alternating. In a simple TDD, a bit stream is divided into equal segments and transmitted in bursts. Figure 7-3 shows how data blocks (A1, A2, B1, B2,,) are exchanged between a handset and a base station by using TDD. Because the data is transmitted in both directions simultaneously, the effective data rate is twice the data rate in one direction.



•Base station sends data blocks A1, A2
•Handset sends data blocks B1, B2

Figure 7-3: TDD (Time Division Duplex) Transmissions

Wireless TDD is typically used with TDMA, where a number of users receive forward channel signals and then transmit reverse channel signals in turn, all on the same carrier frequency. In most cordless systems, TDMA/TDD is used more often because it improves capacity allocation and also has improved ability to cope with fast fading. Fast fading, as discussed in a previous chapter, is encountered while a mobile unit travels through busy areas, causing the radio signals to scatter, diffract, and reflect from different objects surrounding the mobile. The pattern of fading changes with frequencies; thus it is possible for a mobile unit transmitting and receiving at two different frequencies to experience stronger fade in one frequency than the other. The TDD base station can use this to reduce fading – it can select the incoming antenna with the strongest signal and then use the same antenna for responding, thus eliminating or reducing the fading effect.

7.3.2.3 Cordless System Standards and Speech Processing – DECT

Development of cordless system standards has been slow because, as stated previously, the handset as well as the base station are owned by the same user. Two standards have been developed a) DECT (Digital Enhanced Cordless Telecommunications) developed in Europe and b) PWT (Personal Wireless Telecomm) developed in the US. DECT is the most commonly used standard and is briefly discussed here. DECT, as discussed later, is also used in HomeRF.

DECT architecture, shown in Figure 7-4, consists of the following layers based on the ISO-OSI model:

- The physical layer transmits data in TDMA-TDD frames over RF carriers.
- The medium access control (MAC) layer selects/establishes/releases connections on physical channels, and supports three services: broadcast, connection-oriented, and connectionless.
- The data link control layer provides for the reliable transmission of messages using traditional data link control procedures.
- Higher level services support a variety of user services such as call control (connection setup and release), connectionless-message services, connection-oriented services, mobility management (security of communications), and supplementary services (services independent of phone calls).

The main purpose of DECT is to support speech processing in cordless systems. Speech processing in cordless can take advantage of the fact that speech signals tend not to change much between two samples. Thus instead of transmitting the redundant pulse code modulation (PCM) values, you only transmit difference values between adjacent samples. This technique is used in Differential PCM (DPCM), which transmits the difference between the sample and estimated sample. At the receiver, the incoming difference value is added to the estimate of the current. This technique considerably improves the data rates without increasing bandwidth requirements.

For QoS in speech processing, subjective measures are needed because measures such as signal to noise ratio (SNR) and bit error rates do not mean much for speech. A subjective mean opinion score (MOS) is widely used to measure quality of speech. MOS uses a scale of 1 to 5 for speech impairment (1 for imperceptible to 5 for very annoying). Several groups are used for rating speech impairments. MOS is used in standards such as IEEE806.16.

Detailed discussion of DECT architecture with message formats is beyond the scope of this book (see Stallings [2002]). A great deal of information about DECT can be also found at the DECT site (www.DECTweb.com).

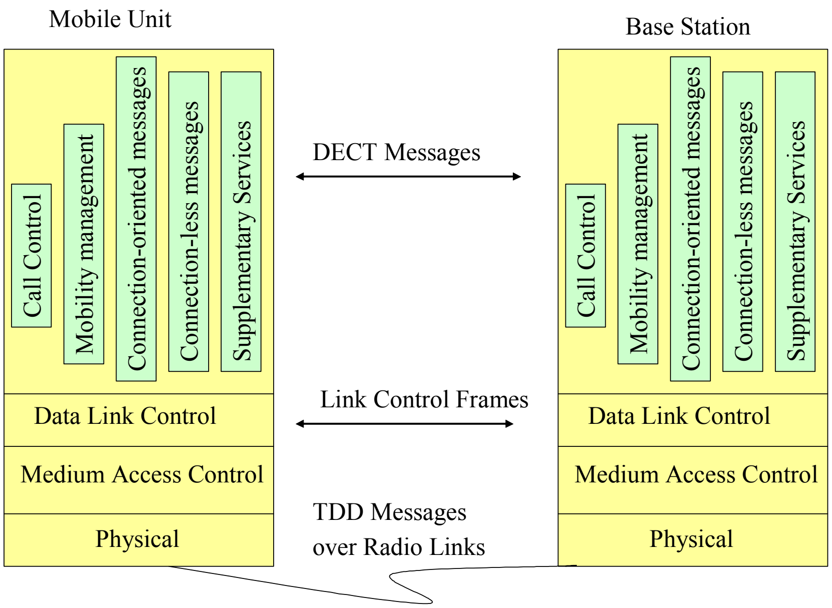


Figure 7-4: DECT Architecture

7.3.3 Home RF

7.3.3.1 Overview

The Home Radio Frequency Working Group (HomeRF WG) was formed in 1998 and developed a specification, the ***Shared Wireless Application Protocol (SWAP),*** for a broad range of home consumer devices. The HomeRF working group includes more than 100 companies from the personal computer, software and semi-conductor industries. The final development of SWAP 2.0 is designed to handle 10 Mbps Ethernet speeds to operate in the license-free 2.4 GHz radio frequency band and utilize frequency-hopping spread-spectrum radio frequency technology.

Home Radio Frequency (home RF) is designed specifically for wireless networks in homes. This is in contrast to cordless systems that were developed for telephone users and later expanded to include wireless home networking. This also differs from 802.11, which was created for use in businesses. HomeRF networks are designed to be more affordable to home users than other wireless technologies. Using radio frequency waves for the transmission of voice and data, HomeRF has a range of up to 150 feet. The foundation of HomeRF is Shared Wireless Access Protocol (SWAP). Thus HomeRF has gone through several releases based on different versions of SWAP, with improvements in data rates, security, and other features. For example, HomeRF 1.0 ran at 1.6 Mbps, but HomeRF 2.0 increases the bandwidth to 10 Mbps – the same speed as standard wired Ethernet LANs. The HomeRF 2.0 standard also includes support for security, interference dodging from other users, and quality of service.

Although the HomeRF Group disbanded in January 2003, the group produced some good technical documents, and some HomeRF products are still in the marketplace. In addition, some of the concepts developed by HomeRF are appearing in some other products. The following two-page description is included in that spirit. The reader can choose to skip this discussion “without loss of generality.”

7.3.3.2 Home RF Characteristics

Figure 7-5 shows a conceptual view of HomeRF. The system revolves around the main PC that is linked to the Internet through xDSL, cable modem, ISDN or other connections. Computing devices ("data devices") such as laptops and printers directly connect to the home PC through wireless cards that support ***SWAP (Shared Wireless Application Protocol)***. Voice devices such as cordless telephones and wireless handsets are connected to a control point that is also connected to the home PC through a local connection (USB). The control point offers some power-saving and bandwidth-management options for ultra-portable devices.

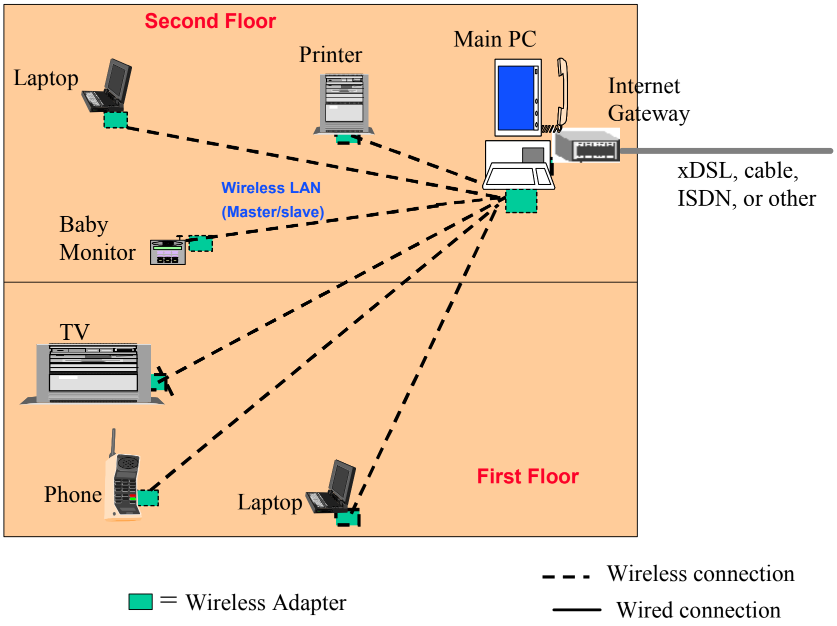


Figure 7-5: HomeRF Environment

By using a HomeRF configuration, all home devices are connected to the main PC through RF cards. This provides several options for the HomeRF users and supports new "home" applications. At present, more than 25% of US homes have 2 or more PCs (our homes are becoming computing centers – a horrible thought!). HomeRF can provide sharing of printers, Internet connections and other computer peripherals. For example, several PC users in the same household can share a printer and a common DSL line. HomeRF also enables several voice applications. For example, you can take caller ID information and send it to the home PC where it looks up the name of the caller. In addition, the cordless telephone could be used to switch on or off cooking equipment, change central heating temperatures, and initiate voice-over-IP conversations. The main characteristics of HomeRF are:

- **Voice Communications Support.** HomeRF uses DECT for voice communications. By using DECT, HomeRF supports up to 4 conversations and up to 8 phone handsets.
- **Interference Resistance.** HomeRF uses 2.4 GHz, the same frequency used by 802.11b, and is subject to interference from other 2.4 GHz devices like some cordless phones. But HomeRF tracks the particular kinds of interference in your home and works around them. It does this by identifying what "data channel" the interference is on, and then telling the frequency hopper to not use that channel. HomeRF does not interfere with Bluetooth.

- **Security.** HomeRF has several security features. First, it uses a "network password" without which the peripherals cannot communicate with your home network. HomeRF also uses frequency hopping that keeps the "data channel" shifting from one frequency to another many times a second. Frequency hopping makes it very difficult for someone to eavesdrop on your home network. Finally, the HomeRF 2.0 standard includes support for 128-bit encryption so all the data traveling across the radio waves is encrypted (HomeRF 1.0 supported 56-bit encryption).
- **QoS** (Quality of Service). QoS support in HomeRF guarantees bandwidth and prioritizes network packets. It makes sure that the important data gets across the network first when you are using your home network simultaneously for voice conversations, copying files, and Internet access. For example, you may want to give voice conversations the highest priority. QoS is part of HomeRF 2.0.
- **Low Power Requirements.** The HomeRF chipset is small and uses very little power, making it appropriate for a variety of handheld devices.

7.3.3.3 HomeRF Technologies – A Closer Look

HomeRF is based on the SWAP specification. A SWAP network consists of three types of devices: control point, voice devices, and data devices. The SWAP protocol uses a client-server model between the control point and the voice devices, but a peer-to-peer model between the control point and data devices.

Figure 7-6 shows a layered view of HomeRF and depicts how DECT and the IP stack are used to support voice as well as data applications. It can be seen that voice applications are supported through DECT and data applications are supported through the IP stack. HomeRF has modified the Physical (PHY) and Data Link (MAC) layers to make them simpler and more appropriate for home use.

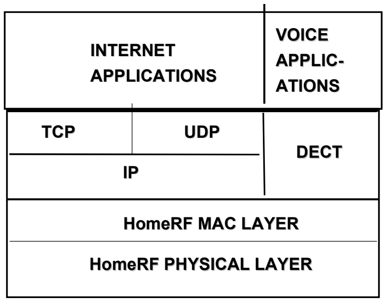


Figure 7-6: Layered View of HomeRF

The physical layer specification for SWAP was largely adopted from IEEE802.11PH. It has been modified significantly to reduce cost and to allow a single-chip implementation of the functionality needed for home usage.

The MAC layer has been optimized for the home environment and is designed to carry both voice and data traffic and to inter-operate with the PSTN using a subset of DECT. The SWAP MAC provides support for voice and data by using both TDMA (for voice) and CSMA/CA (for data) access mechanisms, data rates of 1.6 Mbps and 10 Mbps, data security, power management for voce and data devices, and 24-bit Network ID.

Figure 7-7 shows how SWAP supports both voice and data users. A TDMA service is used to support the delivery of voice and a CSMA/CA service (based on IEEE802.11) is provided to support the delivery of data. These two services are represented in a SWAP frame that is sent to various HomeRF devices.

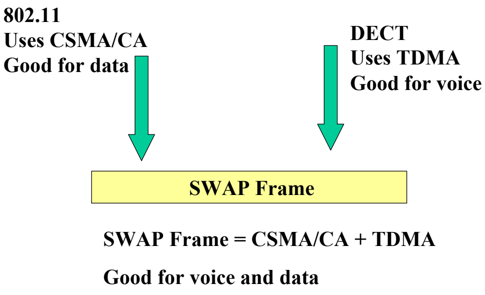


Figure 7-7: How SWAP (Shared Wireless Application Protocol) Supports Voice and Data

SWAP is designed for use mainly in Windows 2000 and XP, but can also be used in Windows 98 with some modifications. SWAP devices are supported in Microsoft Windows via the NDIS driver library. The NDIS library provides a standard interface that higher-level applications can access. The interfaces include a connectionless interface used by Ethernet and a connection-oriented interface for ATM.

7.3.3.4 HomeRF State of the Market and Summary

There were several players in the HomeRF market such as IBM, Compaq and Intel. Intel launched its Anypoint wireless home network option in 2000. This HomeRF product allows users to connect printers and laptops through HomeRF adapter cards. In addition Anypoint software needs to be installed on each PC. The product also includes a built-in firewall for security. Proxim unveiled Symphony HRF also in 2000. Symphony HRF is compatible with the HomeRF standard and connects up to 10 computers at 1.6 Mbps up to a distance of 50 meters away. Proxim has designed Symphony HRF to be interoperable with a wide range of HomeRF based products from Compaq, IBM and Intel. HomeRF Group did a good job by including DECT into SWAP specifications to support voice and data users.

The HomeRF Group was disbanded in January 2003 because it had difficulty competing with 802.11 and Bluetooth – both very strong players in the home networking market. The HomeRF Working Group website (www.homerf.org) is not operational at present. For the nostalgia buffs, the HomeRF Resource Center (http://www.palowireless.com/homerf/) provides a rich set of resources for HomeRF and wireless home networking. It points to numerous articles (overview, technical and marketing, whitepapers), market research reports, HomeRF headlines, specifications (e.g., HomeRF 2.01 Specification), and a wireless bookshop.

Time to Take a Break
✓ • Principles and Home Networking
• Bluetooth and UWB
• Sensor Networks and Examples

7.4 Bluetooth Wireless LANs

7.4.1 Overview

Bluetooth is a medium speed wireless LAN (1 Mbps, 10 meter) specification introduced by Ericsson, IBM, Intel, Nokia, and Toshiba in May 1998. Bluetooth is an always-on, short-range radio hookup that resides on a microchip and uses the 2.4 GHz ISM band to support devices in small LANs (within 10 meters or less). In reality, Bluetooth can provide up to 720 Kbps of capacity (theoretically up to 1 Mbps). Bluetooth is available globally for unlicensed users and supports an open-ended list of applications that include data, audio, graphics, video, etc.

The main idea of Bluetooth is to develop a way for users to connect a wide range of mobile devices quickly and easily, without cables. For this reason, as we will see, the Bluetooth specification includes numerous "cable replacement" specifications (e.g., the RS232 replacement specification) that allow existing devices to communicate wirelessly without any changes. To ensure that this technology is seamlessly implemented in a diverse range of devices, a special interest group was formed in May 1998 to design a royalty-free, open-specification technology, code-named "Bluetooth." The SIG has quickly gained membership from companies such as 3COM/Palm, Axis Communication, Compaq, Dell, Lucent Technologies UK Limited, Motorola, Qualcomm, Xircom, and is encouraging the involvement of all other companies. Currently, almost 2000 companies are part of the Bluetooth SIG.

Bluetooth coexists with most wireless LAN solutions. The Bluetooth specification of 1 Mbps is intended as a small form-factor (i.e., few participants), low-cost radio solution that can provide links between highly mobile devices such as mobile phones, mobile computers and other portable handheld devices. This technology, embedded in a wide range of devices to enable simple, *spontaneous* wireless connectivity, is a complement to wireless LANs which are designed to provide *continuous* connectivity via standard wired LAN features and functionality. Bluetooth provides support for the following three broad application areas:

- **Cable replacement** – Bluetooth contains several cable-replacement specifications that eliminate the need for numerous cable attachments. This allows wireless connection to existing devices such as printers and keyboards.
- **Data and voice access points**. Bluetooth supports real-time voice and data transmissions by providing wireless connections to stationary and portable devices.
- **Ad hoc networking**. A device with Bluetooth radio can automatically establish connection with another Bluetooth-enabled device when in range.

Figure 7-8 shows a simple Bluetooth configuration. Bluetooth was designed to allow low-bandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. The idea originated from connecting different devices (e.g., mouse, printer, headset, cellular phone) to a laptop in a small personal area network, called Piconet (see Figure 7-8). The Piconet could, however, be connected to a wired LAN (through an access point), or to a cellular network through a cellular phone (see Figure 7-8). A simple example of a Bluetooth application is updating your cellular phone directory as soon as soon as the cell phone is within the range (10 meters) of your desktop computer where your directory resides.

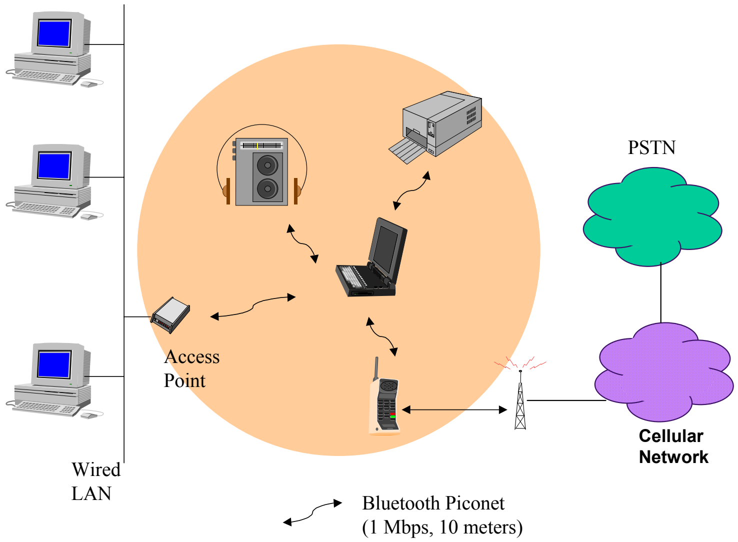


Figure 7-8: A Simple Bluetooth Configuration

Bluetooth connects and synchronizes automatically with other Bluetooth-enabled devices as they enter the room (or frequency area), including devices that are not in line-of-sight. Bluetooth technology is comprised of a specially designed microchip with a radio transceiver built into the electronic devices. The range of each radio transceiver is about 10 meters but can be extended through proper amplification and setup to over 100 meters. Bluetooth is able to send both data and voice communications through its transmissions, making voice-activated communications more of a reality for mobile users.

Due to these attractive features, we may see Bluetooth-enabled thermostats, refrigerators, coffee makers and other devices. Of course, mobile PCs can communicate wirelessly with other mobile PCs, access points, cameras, headsets, and other peripheral devices. Earlier applications of Bluetooth concentrated on cellular phone to PDA or earphone support.

Origin of the Name "Bluetooth"

Bluetooth technology was named after an ancient Viking king named Harald Blåtand ("blå" meaning "dark skinned"; "tan" meaning "great man"). He grew up in a "master-slave" society where one's status in the community dictated their trade or level of service. By 960 AD, Harald had secured rulership of all areas that make up present-day Norway and Denmark. In order to defend his land, he built impressive ringed fortresses at strategic sites on his land to protect his people and even was known to construct massive bridges, some as long as 1 kilometer, to link the land with his people.

The Bluetooth technology is not named after Harald himself but is instead based on the concept of the ringed fortresses that Harald built during his reign. These fortresses that were strategically placed throughout the land allowed his kingdom the ability to network with each other, as best they could, using the bridges built by Harald to travel from one fortress to the next with as little trouble as possible. The Bluetooth uses similar idea, i.e., it allows the devices to network with each other with ease.

7.4.2 Main Features of Bluetooth

Bluetooth is a system solution, consisting of hardware, software and interoperability requirements. The Bluetooth specification describes the complete system with the following details (see Table 7-2):

- Operating frequencies. The radios operate in a globally available 2.4 GHz band and use frequency-hopping spread-spectrum techniques (able to jump over congested frequencies) to keep communication flowing even in spaces that are "noisy."
- Synchronous/asynchronous communications. Bluetooth supports both synchronous and asynchronous communications. Bluetooth's synchronous bands carry relatively high-quality voice, while the asynchronous communication supports data at slightly more than 700 Kbps.
- Data and voice access points. Bluetooth facilitates real-time voice and data transmissions. It uses short packets and FEC (forward error correction) to limit impact of interference.
- Cable replacement. Bluetooth eliminates the need for numerous, often proprietary, cable attachments for connection of practically any kind of communication device. Connections are instant and they are maintained even when the devices are not within line of sight. The range of each radio is approximately 10 meters, but can be extended to around 100 meters with an optional amplifier.
- Ad hoc networking. A device equipped with a Bluetooth radio establishes instant connection to another Bluetooth radio as soon as it comes in range. Software for service and device discovery is available. Since Bluetooth supports both point-to-point and point-to-multipoint connections, several piconets can be established and linked together ad hoc. The Bluetooth topology is best described as a multiple piconet structure.
- Power Consumption. This technology achieves its goal by embedding tiny, inexpensive, short-range transceivers into the mobile devices that are available today, either directly or through an adapter device such as a PC Card. The Bluetooth specification targets power consumption of the device from a "hold" mode, consuming 30 microamps, to the active transmitting range of 8-30 milliamps (or less than 1/10th of a watt). We will discuss different states of Bluetooth devices later.
- CPU requirements. To incorporate this technology, the device must have some sort of general-purpose CPU able to run the lightweight networking and data-link protocols that govern Bluetooth transmission.
- Security. Bluetooth, like other wireless networks, raises some security concerns. The short range of Bluetooth radio in a sense makes it somewhat safer because an intruder has to be within a few feet of the devices to break in. Some security checks, such as encryption and authorization, can be done at the application level. But since wireless technology lends itself to eavesdropping, it is crucial to understand the application-level security needs. In addition, an authentication protocol is necessary to ensure that the communicating devices are on a Bluetooth network. Spoofing and similar problems that exist on IP networks today will be much worse with Bluetooth because it does not require any physical connection to the network. Security is an important feature of Bluetooth and improvements are being made continuously.

Table 7-2: Typical Characteristics of Bluetooth

Normal Range	10 meters (0dBm)
Optional Range	100 meters (+20 dBm)
Frequency Band	2.4 Ghz
Gross Data Rate	1 Mbs

Maximum Data Transfer	721 +56 kb/3 voice channels
Power Consumption, Hold/Park	~50µA
Power Consumption, Standby	300 µA
Power Consumption, Maximum	30 µA

7.4.3 Bluetooth versus Wi-Fi

Although Bluetooth and Wi-Fi (802.11b) LANs are designed for slightly different applications, there are some overlaps and areas of commonalities. Table 7-3 compares and contrasts Bluetooth with Wi-Fi.

Data rates and range: Bluetooth operates at about 720 Kbps (1 Mbps maximum) with a maximum range of 10 meters, but Wi-Fi delivers 11 Mbps for distances up to 100 meters. Thus Bluetooth is too slow for video transfers and to connect a hard drive to your computer. In addition, Bluetooth is not suitable for covering a large room or a conference hall.

Applications: Wi-Fi LANs are designed to address bandwidth-heavy applications that require connectivity to corporate networks and the Internet while Bluetooth concentrates on cable replacement and ad hoc connectivity between peripherals. Although Bluetooth access points can bridge the wireless network to the corporate networks, they are not the best choice in most applications. Wi-Fi, on the other hand, is designed to connect an entire network of wireless devices to corporate LANs. Although Wi-Fi can be used to connect one computer directly to another, that is not its real strength. For example, there are already Wi-Fi wireless print servers from companies such as Linksys.

Ease of use: Bluetooth piconets make it easy to find and connect to the device you are looking for or to switch between devices, such as two computers. In particular, Bluetooth devices advertise their capabilities to others, and a single device can be connected to up to seven other devices at the same time in a piconet. In contrast, Wi-Fi is more complex and requires a great deal of pre-arrangement and planning that is comparable to wired networks.

Power: Bluetooth has a smaller and weaker power requirement than Wi-Fi. Thus the Bluetooth devices can be physically smaller, making it a good choice for appliances and consumer electronics devices.

Frequency band: Wi-Fi and Bluetooth share the same ISM band of frequencies and could interfere with one another. In addition, as the battery of Bluetooth is much weaker than Wi-Fi, the Wi-Fi transmitters can overwhelm the Bluetooth receivers while operating in the same geographical area.

Security: Bluetooth is somewhat more secure than Wi-Fi primarily because Bluetooth has a much shorter range than 802.11b. Thus, to break into your Bluetooth network, a hacker almost has to first break into your room. In addition, Bluetooth offers two levels of (optional) password protection. Wi-Fi suffers from the well known limitations of WEP, but several improvements of Wi-FI security are underway.

In summary, Bluetooth is well suited for connecting single devices when speed is not a major issue and is not great for connecting high-bandwidth devices such as digital video cameras, computers, and external disk drives. Wi-Fi on the other hand is the best choice for connecting computers to one another and to the Internet. If you can only choose one wireless network, then Wi-Fi is a better choice because it has more capabilities. In addition, Wi-Fi is extremely popular at present and is creating a seamless entity that people can plug into and out of with no wire, no plug, and no configuration at airports, shopping centers, apartment buildings, and other hot spots. As the Wi-Fi-based public hotspots grow, Wi-Fi users should be universally mobile. Wi-Fi popularity is also reducing the cost of Wi-Fi adapters. Bluetooth does not enjoy such a broad use, despite many developments.

Table 7-3: Bluetooth versus Wi-Fi

Factor	Wi-Fi	Bluetooth
Data Rate	11 Mbps	1 Mbps
Distance Covered (range)	100 meters	10 metters
Application focus	Connection to corporate networks	Cable replacement
Battery Power	High power	Very low power
Frequency Band	2.4 GHz	2.4 GHz
Ease of use	Complex even for 2 devices	Piconets good for small networks
Security	WEP and its improvements	Short distance, multiple levels (link level, application level)

7.4.4 Setting Up a Bluetooth Network

For each Bluetooth device, a setup procedure is needed by the manufacturer as well as the user. The procedures performed by the manufacturer of the Bluetooth-enabled device include setting a default PIN and device name, and placing the Bluetooth radio in a particular mode such as authentication. The device user customizes the PIN and device name and creates trusted groups.

Users identify their Bluetooth devices using a Bluetooth name which enables them to distinguish one Bluetooth device from another. For example, a printer will have a different name than a keyboard. The name can be any combination of characters that the device has the means to generate, although the characters must belong to a single character set among the ones that the device supports. A user will most likely need to provide a PIN for a Bluetooth device to allow it to communicate with other devices. This PIN is used to create the trusted groups. Only devices that know (or whose users know) each other's PINs can communicate with each other. A PIN entered into a Bluetooth device creates a semi-permanent stored link key that trusted devices could use to authenticate each other in the future.

Creating trusted groups requires the interaction of at least two devices. This means the user needs multiple devices or multiple friends with devices. Whenever a trusted relationship needs to be developed a user and the device must do the following:

- The devices are placed near each other
- The devices are allowed to "discover" each other. Each device will register the other device's 48-bit Bluetooth address (hardwired by the Bluetooth manufacturer). For first-time connection, the user needs to enter a common Bluetooth PIN in both devices.
- If the user of the devices desires to establish a lasting trust between the two devices, the 128-bit temporary key establishes said relationship.
- Future connections between the devices will use the semi-permanent key to authenticate each other and to encrypt information flowing between them. This trust will last until the key is removed from any one of the devices.
- Once the connection is established, the devices can "discover" each other.

Interference in Bluetooth Networks

Bluetooth devices have to tolerate interference from several devices because the unregulated ISM band (2.4 GHz) used by Bluetooth is also used by many other devices such as cellular phones and 802.11 LANs. The complicating factor is that Bluetooth has a much weaker battery than the other players in the ISM band.

In particular, cellular phones are one of the major areas of applications for Bluetooth. However, putting a cellular phone next to a Bluetooth network can cause problems because cellular phones have more powerful batteries than Bluetooth. The powerful phone transmitters can block the weak Bluetooth receivers or simply overwhelm them.

There are different ways of handling the interference. One approach is to assign unique addresses. For example, the manufacturer programs each unit with an address that falls between the range of addresses R1 it has established for its units. Similarly, an address range R2 is established for another set of devices. Thus, when a cordless phone is turned on, it transmits to all units in address range R1, while a DVD only transmits to R2. Thus, these subnets are formed between different types of devices. This address differentiation works between different network types. For example, Bluetooth networks assign different addresses than 802.11. In addition, different types of devices within each technology segment have different address ranges. Thus, your Bluetooth-enabled keyboard should not inadvertently connect to your baby cradle monitor.

Another approach is the use of spread-spectrum technology. Different spread-spectrum (SS) schemes assure that only the devices programmed for certain SS patterns can communicate with each other. For all others, the communications appear as background noise. Bluetooth, 802.11, and cellular devices use different SS schemes to avoid interference with each other.

Yet another approach is to carefully measure and control the level of noise generated by different devices. The basis for this approach is that all devices generate some noise that can interfere and block the other devices. The specific techniques include building a variety of filters to eliminate noise. For additional information on these techniques, see the paper by S. Brown, and M. Lame, "Integrating Bluetooth in the GSM Cell Phone Infrastructure" (Sept. 2001), available from www.rfdesign.com.

7.4.5 How Does Bluetooth Work – Piconets and Scatternets

Piconets. The basic unit of Bluetooth networking is a Piconet consisting of a master and between one and seven slave devices The Bluetooth technology supports both point-to-point (e.g., between two masters) and point-to-multipoint (e.g., between a master and its multiple slaves) communications (see Figure 7-9). For example, each room in an office can be a piconet, or each cubicle can be a piconet. ePiconets are essentially networks within a network. The channel (and bandwidth) within a piconet is shared among all devices in the piconet and the master determines channel and phase within a piconet. Each piconet spans about 10 meters and is set up to connect and communicate automatically with any Bluetooth device once it enters within the range of the piconet. In reality, there can be up to seven *active* slaves in a piconet and up to 256 inactive ("parked") slaves. Slaves change status between active and parked on an as-needed basis.

Multiple piconets can be set up in a particular office to allow users the mobility to move throughout an office or building while still maintaining a wireless connection to either their network or their devices. For example, a piconet can be set up in each office cubicle as shown in Figure 7-9. Because the piconets are so close, they have overlapping coverage areas. Thus PCs in two of the piconets can exchange email. As a matter of fact, a master from one piconet can communicate with a slave of another piconet. Thus a device in one piconet may also exist as part of another piconet and may function as either a master or slave in each piconet (see Figure 7-9). This scenario is called a ***scatternet*** in Bluetooth. A scatternet allows many devices to share the same area and makes efficient use of the bandwidth. By using scatternets, a PC from cubicle1 can print on the printer of cubicle2 or cubicle3 without any additional setup.

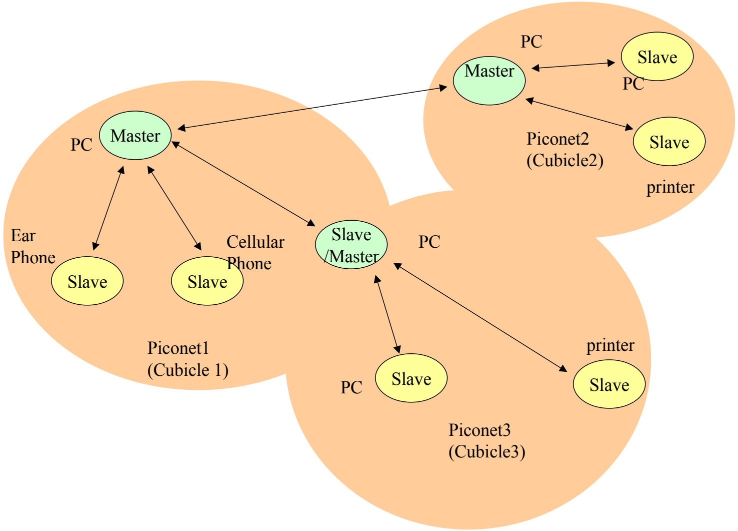


Figure 7-9: Bluetooth Piconets

Bluetooth Hardware. Bluetooth hardware consists of a Radio Module and a Link Module. The Radio Module is responsible for implementing the Bluetooth frequency hopping. As stated previously, Bluetooth uses RF channels from 2402 to 2480 MHz with a channel spacing of 1 Mhz. To support frequency hopping, the Radio Module hops to the next channel within the 2402-to-2480 MHz band after every 625 microseconds. Each piconet has its own frequency-hopping sequence. The Link Module, and the closely associated Link Software, is responsible for authentication, setting up connections, sending/receiving data, and error detection/correction. Some companies are working on single-chip solutions that implement the Radio as well as Link Module.

Power Consumption. The Bluetooth devices that are communicating with each other only use the level of power needed to establish that connection. In other words, if two devices are only a few feet apart from one another, the device will only use enough power to reach that device as compared to devices that might be across the room. In general, a Bluetooth device consumes only 3% of the power used by a traditional mobile phone.

How are the Bluetooth Networks Formed? The Bluetooth-enabled devices, known as ***Bluetooth radios***, can become masters or slaves in a piconet. The piconet configuration is determined at the time of network formation. Typically, the connecting device becomes a master, however, a "master/slave" swap function allows the roles to be reversed (recall that a device can be master in only one piconet).

To support many radios, the ISM frequency band is divided into 79 channels, each at 1 MHz. The radios hop around these channels by using frequency-hopping spread spectrum (FHSS). Each piconet uses the same hopping sequence, shifted by a phase. To form a piconet, the Bluetooth radio needs to understand two parameters: the frequency-hopping (FH) pattern and the phase shift within that pattern. The master sends the new radio its ID, its FH pattern and its phase to form a piconet. Figure 7-10 shows the states and state transitions in Bluetooth in forming a network. A typical scenario consists of the following:

1. All radios initially exist in "standby" mode. In this mode, the radios are not connected to any piconet.

2.The standby radio issues an "inquire" command to indicate, "I am available, does someone need me?" The inquire request is issued to a particular frequency range – an inquiry list is created as a result.

3.Other radios scan the inquire list periodically (every 1.25 seconds) to discover the radios they want to talk to. If there is a match, the radios issue a "page" command to the ones they want to invite. A standby radio can also issue a page to a specific radio.

4.The paged radios, if there is an agreement, typically become the slaves to the pager and join its piconet. The master sends its FH sequence, ID, and phase to the slave. At this stage, the slave radios go into an "active" state and are in transfer mode within the piconet. In the active state, useful work is done (after all, this is the main idea!). In this state, each active radio is assigned a 3-bit Active Member Address (AMA). The master is assigned an AMA of 0 – it uses the slave AMAs to send information to them.

5.If another radio wants to join a piconet, and too many radios are in the piconet (8 active radios), then the master puts one of the slaves into a "park" state. In a park state, the radio does not lose its status in the piconet (it keeps its FH sequence) but is assigned a PMA (parked member address). While only 8 radios can be active in a piconet, 256 can be in the parked state. In addition to parked states, the radios can be also put in "sniff" or "hold" states – i.e., told to go away for a while. In the hold state, no data is transferred, while in the sniff mode, some data could be transferred now and then (for example, a keyboard could be placed in sniff mode). In the parked/sniff/hold states, the radios do not lose their status in the piconet (they still have the same FH sequence) and can go to active status quickly.

6.Once a radio is done with a piconet, it goes into standby mode, from where it can join another piconet.

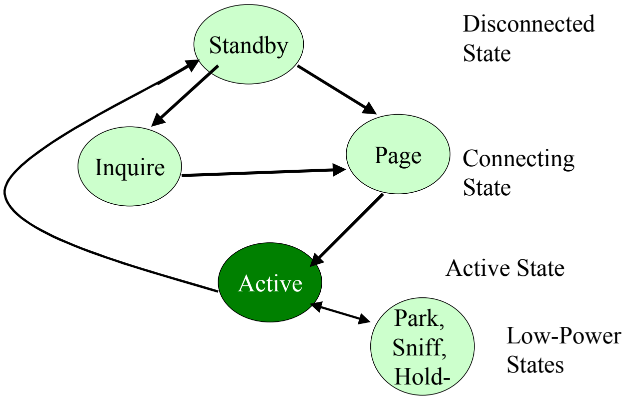


Figure 7-10: States in Bluetooth – A Simplified View

Relationship Between States and Battery Consumption

Battery consumption is an important issue in designing wireless systems. For example, in wireless sensor networks (ZigBees), it is extremely important to conserve batteries. Systems that support many states during operation consume more battery power because the battery has to support all states. This is the main reason why wireless sensor networks support only two major states: active (transmit/receive) or sleep – the battery is only used when the system is active. In contrast, the many states of Bluetooth (active, parked, inquire, standby, poll, etc.) shown in Figure 7-10, have to be supported and consume more battery power.

7.4.6 Sample Applications of Bluetooth

Bluetooth technology enables short-range wireless connections between desktop and notebook computers, personal digital assistants, mobile phones, camera phones, printers, digital cameras, headsets, keyboards, a computer mouse, and many other devices. Under the general slogan of "unplug and communicate," Bluetooth has been used widely to replace the cables of digital peripherals with wireless communications. Bluetooth-enabled products are being used in several wireless personal area networks to synchronize, connect, share and listen to a wide range of mobile devices. Devices such as PDAs, pulse oximeters, gaming devices and barcode scanners have been Bluetooth-enabled by companies such as Nokia, Lexus, Toshiba, Apple, BMW, Toyota, and Logitech. Here are some examples of Bluetooth-enabled commercial products (see the Bluetooth site (www.bluetooth.com) for additional examples):

- **The Apple PowerBook**. This computer uses Bluetooth technology extensively. In general, Apple has embraced Bluetooth technology and Bluetooth is integrated across the board on Apple computers. It is built, for example, into all Apple PowerBook G4 computers as a standard feature and can be integrated into iBook, iMac and Power Mac computers as an option. Bluetooth-enabled Macs can perform file transfers, synchronize data and improve security by assuring that only trusted devices talk to your Mac, and by using 128-bit over-the-air encryption.
- **Bluetooth-enabled mobile phones with GPRS.** These phones allow synchronization with Address Book, support exchange/display of SMS messages with Macs, and enable the cellular phones to act as a modem for wireless Internet access. You can also use a camera phone such as the Nokia 6600 to take pictures, download them to your Mac over a Bluetooth connection, create an iCard, and then send it using your phone's GPRS connection.
- **Gaming, Mobile Phone N-Gage.** The N-Gage game deck is built for active and hardcore gamers. It provides mobile and connected game decks with 3D support over Bluetooth and GPRS.
- **Automotive 2004 Toyota Prius**. Several (up to four) cellular phones with built-in Bluetooth can be registered in a Toyota car for hands-free calling. The touch-screen panel and/or steering wheel controls can be used to make and receive calls. Visit toyota.com/prius for details.
- **Toshiba Fully Automatic Electric Washer-Dryer.** This washer-dryer can download the washer/dryer software for new clothes from the home terminal before the wash cycles. In addition, an error code is transmitted to the home terminal if this washer-dryer breaks down.

- **Medical Avant™ 4000 Digital Pulse Oximetry System.** Pulse oximetry system which allows pulse rate data to be transmitted from a wrist-worn sensor to a monitor.

In addition to the aforementioned commercial products, consider the following Bluetooth applications.

Automatic backup synchronization. Consider an example of a trade show. A user with a qualified Bluetooth device such as a PDA (acting as a client) would simply walk by a schedule-of-events kiosk incorporating Bluetooth wireless technology (the server). When the user's device notices that the kiosk is in range, it automatically starts the synchronization process to get the updated schedule. How does the synchronization work? The PDA first establishes a Bluetooth connection to the server (allowing for any authentication if needed) and then gets the device information object from the server. This object tells the PDA which object formats are supported by the server, and can be used to tell if the server is known to the client (the client has synched before) or if it is a brand new server which has not synched with this client before. The number in this change counter object is incremented each time there is a change to the events database. If the last synchronization was performed at 10, but now it is 14 (2 PM), the device can tell what changes need to be made. The PDA begins to download the two changes that were made to the schedule.

Bluetooth Home Networking Scenarios. Some pervasive computing applications of Bluetooth in the home include the following:

- The Three-in-One Phone: A Bluetooth-capable mobile phone could be used as a standard cellular phone, using a wireless service provider as a carrier; it could also be used like a cordless phone through a Bluetooth voice access point in the home, using the home's normal wired telephone system. The phone could also be used as an intercom with direct point-to-point voice communications within the home, without involving any carrier (this case especially would be most useful with a power-amplified 100-meter range Bluetooth radio). Benefits include "one telephone, one number" regardless of location, and reduced airtime charges for the phone user.
- The Untethered Computer: A Bluetooth-capable notebook computer could be connected to a network such as the Internet via a Bluetooth modem access point in the home. The modem access point provides connectivity to the network in the normal fashion, such as over telephone lines, cable or ISDN, but the computer need not be cable-connected to the modem. Thus the user would be free to cordlessly move about the area while maintaining a connection to the network. Multiple access points within the home could provide additional untethered computer work areas and in the future might enable roaming throughout the home.
- The Universal Remote: As Bluetooth becomes prevalent on more devices found in the home, any personal Bluetooth device such as a PDA or smartphone could be used to query and control the other devices. Thus, when consumer electronics, home security systems and "smart goods" include Bluetooth interfaces (and companies from these industries have signed on as Bluetooth adopters), one could receive an alert from the dryer that the clothes are dry, start the dishwasher, arm the security system, change channels on the television, and route the television's audio to the stereo system, all from one personal device. Even in the absence of direct Bluetooth links on all of these devices, this could still be accomplished via a Bluetooth-capable home gateway that uses other physical interfaces to communicate with the home devices.

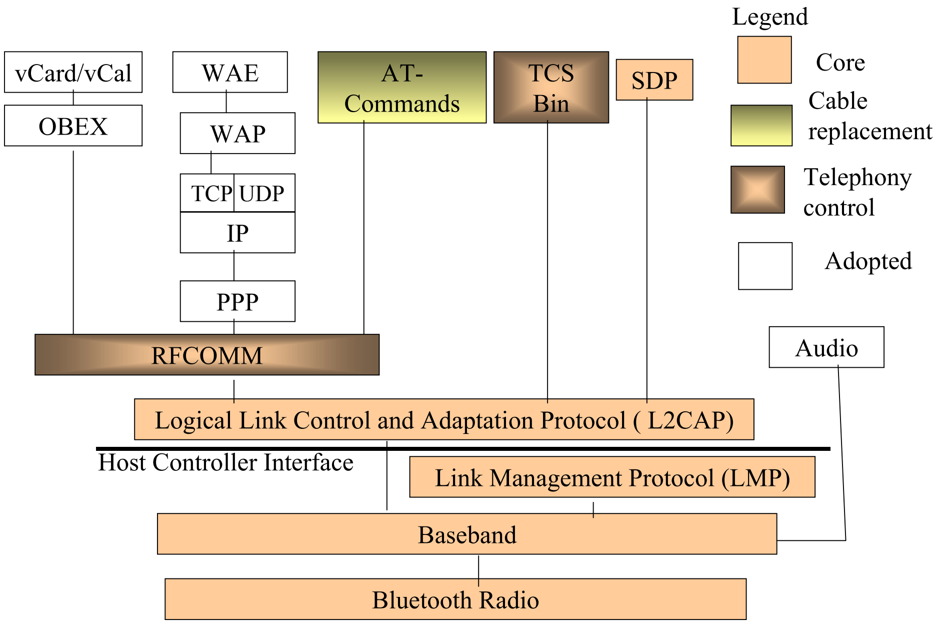
Bluetooth Office Scenarios. A company could allow all of the devices in its office to "discover" each other. Office workers can have access to the LAN all the time through multiple devices (Bluetooth LAN access points) in multiple office locations. Bluetooth access points can become a familiar sight around the office. During meetings, an employee can pull down reference documents and presentations from file servers or the web and can backup her meeting notes by accessing her project notes via the Bluetooth technology. At the end of meeting, she could print her notes from the PDA and command the coffee machine to prepare a hot cup of coffee as she walks down the hall to her desk.[1]

7.4.7 Bluetooth Stack and Bluetooth Protocols – An Overview

Looking at stacks can be boring. The Bluetooth stack is no exception. Bluetooth documentation is extensive (over 1500 pages). The documentation is subdivided into a) Core specifications that give details of various layers of Bluetooth protocol architecture and b) Profile specifications that show use of Bluetooth technology to support various applications. Figure 7-11 shows an overview of the stack. The layers are described briefly (more details can be found at the Bluetooth SIG website).

7.4.7.1 Bluetooth Specification

Bluetooth uses a layered protocol architecture (no surprise!) shown in Figure 7-11. These protocols are subdivided into core protocols, cable replacement and telephony control protocols, and adopted protocols. In addition, a set of usage profiles are defined. A brief overview follows.



Shaded areas (see legend) represent different families of Bluetooth Protocols

Figure 7-11: Bluetooth Protocols

Core Protocols: The core protocols consist of five layers (from bottom to top):

- **Radio layer** specifies the requirements for a Bluetooth transceiver operating at 2.4 GHz.
- **Baseband layer** specifies the Bluetooth Link Controller (LC) which carries out the baseband protocols and other low-level link routines.
- **Link Manager Protocol (LMP)** is used by the Link Managers (on both sides) for linking.

[1] This is laziness unlimited, but …..

- **Host Controller Interface (HCI)** provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.
- **Logical Link Control and Adaptation Protocol (L2CAP)** supports higher-level protocol multiplexing, packet segmentation and reassembly. It also conveys quality-of-service information.
- **Service Discovery Protocol (SDP)** provides a means for applications to discover which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services.

These protocols must be supported by all Bluetooth-compliant LANs. A closer look at the core protocols can be found in Section 7.4.8.

Cable replacement protocol: The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol, based on the ETSI standard TS 07.10, presents a virtual serial port that makes replacement of cables as transparent as possible. For example, RFCOMM emulates EIA RS232 communications over the Bluetooth baseband layer.

Telephony control protocols: Telephony control specification – binary (TCS BIN) defines the signalling and control sequences needed for telephone conversations over Bluetooth.

Adopted protocols: Bluetooth has adopted the following standards to minimize what new standards need to be by developed by Bluetooth:

- **PPP:** The point-to-point protocol is widely used to transport IP packets over point-to-point links such as dial-up lines.
- **TCP/UDP/IP**. These are the foundation protocols for the Internet.
- **OBEX:** The object-exchange protocol developed for the exchange of objects. OBEX is similar to HTTP but facilitates exchange of objects instead of documents. Examples of the objects specified are vCard and vCalendar for business cards and personal calendar entries.
- **WAE/WAP**: The Wireless Application Protocol and Wireless Application environment are included in Bluetooth.

7.4.7.2 Profiles and Usage Models

A usage model is a set of protocols that are used to implement a Bluetooth-based application. Usage models essentially represent profiles of protocols that are needed to support specific applications. Examples of the usage models are (see Figure 7-12):

- **File transfer**: This model is used to transfer files over Bluetooth. The protocols used can be SDP or OBEX.
- **Dial-up networking (Internet bridge)**: This model is used to wirelessly connect a PC with a cordless modem or a cellular phone This model uses PPP and AT protocols.
- **LAN access**: This model is used to connect a piconet device to access a LAN. The model uses SDP and PPP-IP protocols.
- **Synchronization:** This model is used to synchronize device-to-device PIM (personal information management) information such as calendars and phone books. The model uses OBEX and IrMC (infrared mobile communications) protocols – IrMC is built for synchronizing PIM information. .
- **Three-in-one phone**: Telephone headsets and handsets can be used in this model as audio input and output devices. This model uses Audio, SDP, and AT commands (not shown in the figure).

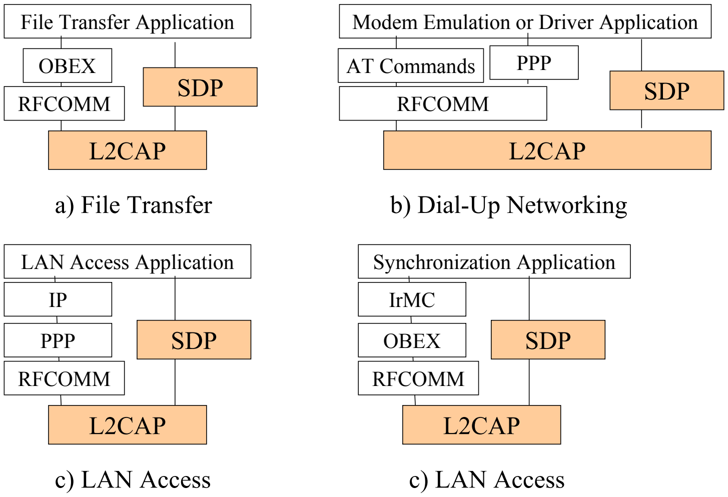


Figure 7-12: Sample Bluetooth Usage Models

7.4.8 Closer Look at Bluetooth Core Protocols

Bluetooth core protocols include five layers of protocols. We look at these protocols very briefly. Additional information can be found in the Bluetooth documents.

7.4.8.1 Radio Specification

The Radio Specification of Bluetooth is a short document that only specifies radio channels and power transmissions Bluetooth makes use of in the 2.4 GHZ ISM band that can support around 80 physical channels with 1 MHz bandwidth each. In addition, Bluetooth supports different classes of transmitters:

- Class 1: These transmitters are the most powerful. They output 100 mW for maximum range and provide greatest distance.
- Class 2: These transmitters output up to 2.4 mW and provide mid-range distance.
- Class 3: These transmitters produce nominal output at 1 mW and are intended for really short distances.

By using different classes of batteries, the distance covered by Bluetooth can be adjusted from less than 10 meters to almost 100 meters.

7.4.8.2 Baseband Specification

The Bluetooth baseband specification is quite complex. The key elements of this specification include frequency hopping, physical links, packet field formats, error correction, logical channels, Bluetooth audio, and Bluetooth Security.

Frequency Hopping in Bluetooth. The total Bluetooth bandwidth, as stated previously, is divided into 79 1-MHz physical channels, starting from 2.402 GHz and going up to 2.480 GHz. This ISM band is also compatible with other unregulated frequencies in Europe and Japan – thus Bluetooth devices manufactured in other countries can work in the US and vice versa. FH (Frequency Hopping) occurs by jumping from one channel to another in pseudorandom sequence, and the same hopping sequence is shared with all devices in one piconet. In other words, the Bluetooth radios hop around these 79 channels by using Frequency Hopping Spread Spectrum (FHSS) so that each piconet uses the same hopping sequence (but the frequency is shifted by a phase within each piconet). The frequencies hop around at 1600 hops per second.

Physical Links between Master and Slave. Two types of links can be established between masters and slaves.

- **Synchronous connection-oriented (SCO).** Bluetooth allocates fixed bandwidth between point-to-point connection of master and slave. A master maintains links using reserved slots – it can support three simultaneous links. Most SCOs are used for voice communications.
- **Asynchronous connectionless (ACL).** Point-to-multipoint link between a master and all slaves in a piconet is also supported. Only a single ACL link can exist in a piconet because only one master exists per piconet.

Bluetooth Packet Fields. The Bluetooth frame consists of a transmit packet followed by a receive packet. Each packet can consist of multiple slots (1, 3, or 5) of 625 microseconds each. Each single-slot frame hops 1600 times per second. Multi-slot frames allow higher data rates because they eliminate the turnaround time between packets and reduce the header overhead. For example, a single-slot frame can support 172 Kbps while 5-slot frames can yield 721 Kbps. The Bluetooth packets, single- or multiple-slot, consist of three fields:

- Header – used to identify packet type and carry protocol control information.
- Payload – contains user voice or data and payload header, if present. The payload may be single- or multiple-slot.
- Access code – used for timing synchronization, offset compensation, paging, and inquiry.

Error Correction Schemes: Bluetooth uses different types of error-correction codes that include forward error correction and ARQ (automatic repeat request). ARQ includes error detection (destination detects errors, discards packets), positive acknowledgment (destination acknowledges that the data was received OK), retransmission after timeout (source retransmits if packet is unacknowledged), and negative acknowledgment and retransmission (destination returns negative acknowledgement for packets with errors, and source retransmits).

Logical Channels and Channel Control: Bluetooth defines five types of channels for different types of payload such as Link Control (LC), Link Manager (LM), User Asynchronous (UA), User Isochronous (UI), and User Synchronous (US). Sophisticated protocols for Channel Control are specified to include states of operation of a piconet during link establishment and maintenance. Examples of major states are Standby (default state) and Connection (device connected). Interim substates include Page Scan (device is listening for a page), Master Response (master receives a page response from slave), and Slave Response (slave responds to a page from master). We have discussed the various states previously when we explained how the Bluetooth networks are formed (Section 7.4.5).

Bluetooth Audio. Buetooth gives a choice of two voice-encoding schemes: pulse code modulation (PCM) or continuously variable slope delta (CVSD) modulation. We have discussed PCM previously (Chapter 5). CVSD is a special case of delta modulation (DM), also discussed previously. As compared to the fixed staircase function of DM, the CVSD staircase varies according to the changes in the waveform to minimize errors. The link manager negotiates and selects the most appropriate scheme for applications.

Bluetooth Link Security. Baseband specification defines security for links between Bluetooth devices. The security includes authentication (verify claimed identity), encryption (privacy) and key management and usage. The security algorithm makes use of four parameters: unit address, secret authentication key, secret privacy key, and random number.

7.4.8.3 Link Manager Specification

The link management protocol (LMP) manages the radio links between Bluetooth masters and slaves. The LMP protocol mainly specifies exchange of LMP PDUs (packet data units) between Bluetooth entities. The procedures defined for LMP are grouped into more than 20 functional areas, each of which involves exchange of one or more messages. An LMP PDU is specified for each message type. The following is a partial list of the functional areas with PDUs supported by the LMP for each functional area:

- General response – accepted and not-accepted PDUs.
- Security service – authentication, encryption, change link key, and change current link key PDUs.
- Time/synchronization for various clocks in the piconet – clock offset request, slot offset information, timing accuracy information request PDUs.
- Station capability for various Bluetooth devices – LMP version and supported features PDUs.
- Mode control for managing various states – switch master/slave role, detach, sniff mode, park mode, power control, and quality-of-service PDUs.

7.4.9 Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP, similar in scope to the IEEE 802 LLC, provides a link-layer protocol between entities with a number of services. In a manner similar to LLC, it relies on the lower layers for flow and error control. It makes use of ACLs (asynchronous connectionless links) and does not support SCO (Synchronous Connection Oriented) links. L2CAP provides three alternative services to upper-layer protocols:

- Connectionless service supports connectionless service for Bluetooth devices. Each channel is unidirectional and is used from master to multiple slaves.
- Connection-oriented service supports connection-oriented service for Bluetooth devices. Each channel is bidirectional. A QoS flow specification is assigned in each direction.
- Signaling provides for exchange of signaling messages between L2CAP entities.

A variety of L2CAP packet formats are defined in the Bluetooth specification. Discussion of these packet formats is beyond the scope of this book.

7.4.10 Concluding Comments on Bluetooth

Bluetooth is a WPAN standard, which through its small size, considerable functionality and flexibility and very low cost, is finding its way into many modern devices, offering control and information easily and simply. The new generation of cellular telephony systems, while offering national coverage and mobility could not provide a cost-effective interconnection of so many devices, but coupled with Bluetooth, localized groups of equipment can be interconnected wherever they are and wherever they are going. Bluetooth could thus extend the reach and scope of cellular systems well beyond today's horizons.

For more infformatiopn, visit www.bluetooth.com (the Bluetooth website), http://www.palowireless.com/bluetooth/, and http:\\Bluetooth.ericsson.se.

7.5 Ultra Wideband (UWB) – A Quick Overview

Besides Bluetooth, Ultra Wideband (UWB) is emerging as a new wireless personal area network technology. UWB is in fact an old technology that was originally developed in the 1960s for the military. After being classified for many years, the FCC approved the commercial implementation of UWB in February 2002, within limits. UWB provides high data rates (around 50 Mbps) in very short distances (10 meters). Simply stated, UWB is a radio system that uses narrow pulses (millions of pules per second) for communication and sensing by using short-range radar. UWB radio sends data in millions of pulses across a wide frequency band and is legal in the US as long as it uses less power than normal radio frequency leakage.

Although UWB faces stiff competition from existing WPAN technologies, it has an established and proven track record in military applications. In addition, UWB has several attractive characteristics such as very low power consumption, very high throughput, and ability to operate without the requirement of spectrum licensing. The main strength of UWB is that it is highly secure because it is virtually impossible to intercept and interpret millions of pulses per second. The high data rate and increased security of UWB provide a number of niche opportunities for operators and vendors. You can think of UWB as a 50-times-faster Bluetooth and a more secure 802.11g (recall that 802.11g runs at around 50 Mbps also). For example, operators like Verizon could sell UWB alongside Wi-Fi to organizations that demand military-grade security. In home/RF applications, UWB could be used for wireless HDTV because HDTV requires much higher data rate than can be offered by Bluetooth.

The standards effort for UWB is being spearheaded by the IEEE 802.15.3a (WPAN Higher Rate) Task Group. But the progress is slow (see the sidebar, "UWB Progressing Through Standards – Slowly But Surely"). We will take a closer look at UWB in Chapter 10.

UWB Progressing Through Standards – Slowly But Surely

UWB's progress through the IEEE standards has been slow. In the meantime, UWB is having problems finding a wider market. The chip-makers are still in the experimental stages mainly because there is no standard. The popular MBOA (Multiband OFDM) Alliance, proposed by Intel and others to promote UWB, is repeatedly blocked at the IEEE standards body by a smaller group backed by Motorola. Motorola has managed to slow down the IEEE standards process.

Different proposals have been floating around to move the process forward. One approach proposed by PulseLink, a company specializing in UWB, is based on a low-speed communications link for the devices to make initial contact and negotiate/agree upon any higher-speed UWB standard for later communication. Attempts have been made to present this proposal to the ITU directly and bypass IEEE altogether.

Source: "Ultra-wideband fights for greater acceptance," Computerweekly.com, April 13, 2004.

Time to Take a Break

✓ • Principles and Home Networking

✓ • Bluetooth and UWB

• Sensor Networks and Examples

7.6 Wireless Sensor Networks and ZigBees – An Overview

7.6.1 What are Wireless Sensor Networks?

Wireless sensor networks (WSNs) typically consist of small, low-powered devices (sensors) that allow the physical environment to be monitored at high resolution. Sensors can be developed to measure temperature, humidity, motion, color changes in a painting, or any other measurable thing. Although most WSNs consist of very small processors communicating over slow wireless networks, WSNs may consist of devices with a wide range of computation, communication, and sensing capabilities. The devices range from relatively powerful systems with PC-class processors to tiny low-power nodes consisting of simple embedded microcontrollers. The WSNs may also use high-bandwidth wireless interfaces (e.g. IEEE 802.11) or, most commonly, low-bandwidth radios operating in the 433 or 916 MHz ISM bands.

What are the best wireless technologies for WSN? The usual suspects are standards like Bluetooth, Wi-Fi, and even cellular. But these provide mid-to-high data rates for voice, PC LANs, and video. Sensors and controls do not need high bandwidth, instead they need low latency and very low energy consumption for long battery lives. The core challenge facing WSNs is managing the tradeoff between local computation and communication. WSNs are typically battery-powered and therefore have a fixed energy budget. In addition, the energy cost to transmit even small amounts of data greatly dominates that of computation. The sensors commonly expend significant CPU cycles to perform local compression, filtering, and aggregation of data in order to save communication overhead.

A brief overview of WSNs is given in this chapter to highlight the main issues. A more detailed treatment can be found in Chapter 10.

7.6.2 ZigBees

Over the years, many proprietary wireless systems have been developed for WSNs because no suitable standards existed. These proprietary solutions created significant interoperability problems with each other and with newer technologies. The ZigBee Alliance has been formed to provide a standardized set of network solutions for sensor and control systems. The main emphasis of ZigBee has been to drive the WPAN standards (in particular, the IEEE 802.15.4). In fact, the ZigBee Alliance is so influential that the devices conforming to 802.15.4 are becoming known as "ZigBees." The 802.15.4 standard for ZigBees specifies the following main features:

- The physical layer uses direct-sequence spread spectrum to allow the circuitry to be very simple and inexpensive.
- The media access control (MAC) layer supports only two major states: active (transmit/receive) or sleep, to conserve on battery and save processing overhead. This is much better than the many states of Bluetooth (active, parked, inquire, standby, poll, etc.) as shown in Figure 7-10.
- The network layer has been designed to allow the network to grow without requiring high power transmitters.

Due to these and many other simplifications, the Zigbee devices provide a low-cost and low-battery solution for WSNs. Additional details about Zigbee and 802.15.4 can be found from the ZigBee Alliance (www.zigbee.org) and IEEE 802.15 (http://www.ieee802.org/15/) websites.

7.6.3 Components of a Sensor (Mote)

As mentioned previously, sensors can be developed to detect almost anything that can be measured. A sensor node *participating* in a sensor network, usually called a ***mote***, typically consists of 3 components; the sensor interface which actually measures the physical attributes such as temperature, the radio interface which communicates with other motes, and the CPU which performs computations and transfers information between the two components (Figure 7-13). Typical commercially available sensor nodes (motes) from companies such as Intel include a 32-bit CPU with a Bluetooth radio interface for network communications. The radio-interface is the most sensitive and power consuming component of a mote because it has to establish communications, detect and correct errors, and send/receive information over the network. The energy consumption of the radio interface influences many WSN design decisions because an attempt is always made to minimize the total energy spent by the network. Thus improvements in wireless network technology and efficient routing protocols greatly impact the sensor nodes.

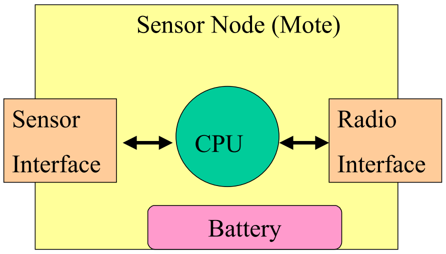


Figure 7-13: Anatomy of a Sensor Node (Mote)

7.6.4 WSN Applications and Platforms

The scope of WSN applications is only limited by the imagination of the designers. WSNs can be used to measure temperature, humidity, and the speed with which cars cross certain intersections in a city. Many WSNs have been used in military applications to detect troop and vehicle movement on the battlefield. See, for example, the case study, “Wireless Sensor Networks as a Replacement for Land Mines” (in Section 7.7.2), showing how WSNs can serve as a replacement for land mines that are disastrous to the inhabitants years after the conflict is over. Another application is structural, which involves implanting seismic sensing nodes on buildings or bridges and detecting the slightest vibration or seismic activity, or how a building or bridge reacts to earthquakes. See Section 7.7.4 for additional examples.

WSN applications need specialized platforms that include the middleware services, local services, and network transport services. The main purpose of platforms for sensor networks is to support the development and execution of sensor-based applications. As discussed in Chapter 4 (in the examples and case studies section), research in WSN middleware and platforms is continuing at present at different universities such as Berkeley, Cornell, and Rutgers. The prevalent thinking favors a hierarchy of services that range from low level sensors to higher level data aggregators, and data storage and analysis capabilities (see Figure 7-14). This approach, presented by [Hill 2004] provides a general framework for developing WSN platforms.

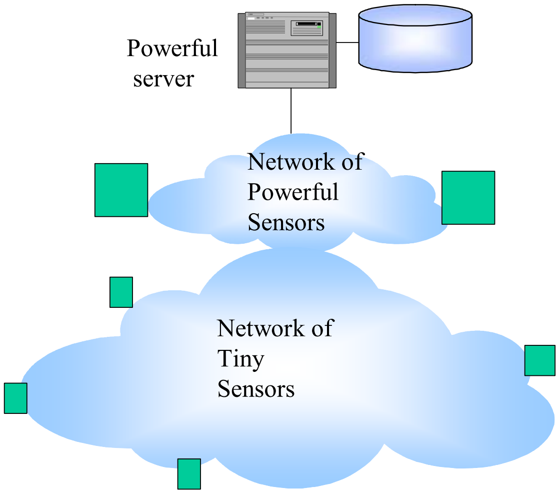


Figure 7-14: Hierarchy of WSN Platform Services

7.6.5 Wireless Sensor Network Design at a Glance

WSNs typically consist of thousands of sensor motes interacting with each other in an ad hoc manner. If a node, for instance captures some information, it will transfer this information to a chosen neighboring node until it gets to a node that is in the range of an access point (node E in Figure 7-15). The access point can then transfer this information to other interested parties through a corporate LAN, the public Internet or any other network. This shuffling of messages does not have to involve and *should not* involve all nodes on the network, as shown in the diagram. This approach of involving only a few nodes in routing conserves energy of the individual motes (one of the major design considerations). In addition, transferring information to the access point can use shortest-distance algorithms and shortest node-to-node distances to further conserve the energy of the communication system.

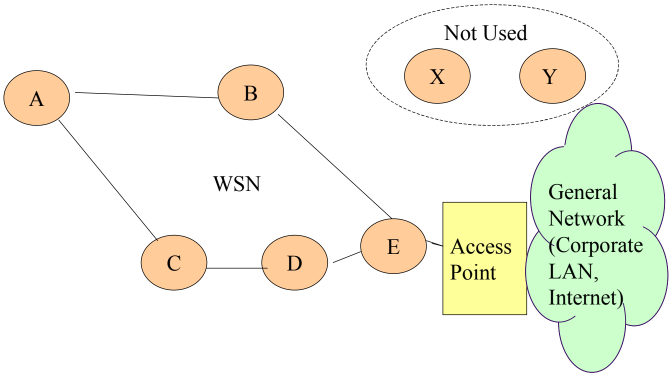


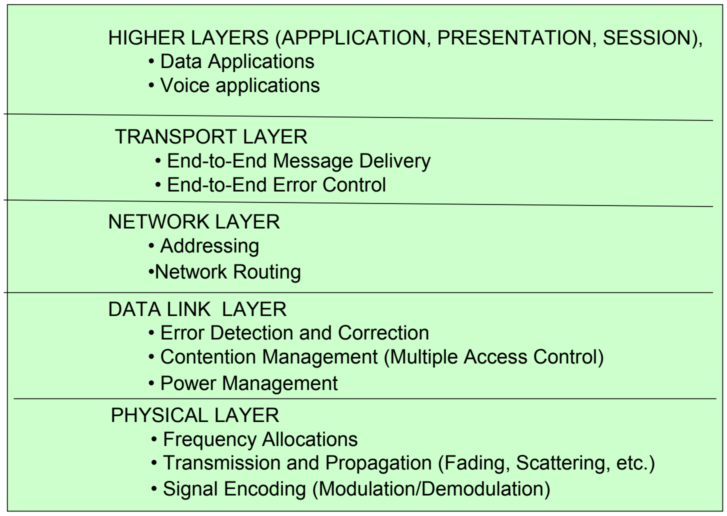
Figure 7-15: A Sample Wireless Sensor Network

Sensor networks may comprise a large collection of primitive sensor devices interspersed with a smaller collection of more capable nodes, all interconnected by some form of wireless communications. Complicated by node mobility and operation in harsh environments with extremely limited power, such devices benefit directly from the ability to offload their end-to-end communications to more capable custodians and thus extend their operational lifetime by minimizing their participation in the network. The MANET (Mobile Ad hoc Network) model, introduced in a previous chapter, is a natural for WSNs because sensors tend to speak to each other directly without an access point. It should be noted, however, that although *most* WSNs use the MANET model, it is not necessary. A WSN may use a master/slave model where a few sensors in a room may directly communicate with an access point instead of each other.

The typical features of a WSN are:

- It has a very large number of nodes, often in the order of thousands.
- The nodes are of low cost and size, are prone to failures, and possess a limited amount of energy that must be conserved. In many applications, this battery is impossible to replace or recharge.
- Communications are triggered by events and sometime by queries. Once initiated, the information flow is asymmetric, going from the observers or sensor nodes to a “command” node that may have more capabilities.
- There is more use of broadcast communications instead of point-to-point. Sensors tend to broadcast information so that any of the recipients can take the information forward.
- Nodes do not have a global ID such as an IP address. Thus IP routing does not apply. Specialized routing algorithms are chosen and implemented in WSNs.
- The security, on both the physical and communication level, is more limited than with conventional wireless networks.
- Nodes are subject to failures due to depleted batteries, captures, or environmental influences.
- There is a high degree of dynamics in WSNs such as frequent network topology changes and network partitions (i.e., the network is subdivided so that the subdivisions do not communicate with each other).
- WSNs are heterogeneous, consisting of different types of sensor devices that are interconnected to more powerful back-end systems
- WSN nodes have to operate unattended since it is impossible to service a large number of nodes that may reside in remote and hard to access locations.

These specialized features impose requirements that drive the design and development of WSNs. These design decisions have to be made at almost every layer of the protocol stack (from physical layer to application layer). Figure 7-16 shows the typical network protocol stack and displays the major decisions that need to be made at each layer. At the physical layer, limited capabilities of sensor nodes do not allow sophisticated modulation and error-correction schemes. At the data link layer, power management plays a critical role. For example, power management may require turning off the power after the device sends a message. This influences the way contention between devices is managed. At the network layer, routing protocols have to consider thousands of weak nodes that really do not want to be bothered unless really necessary. Thus special scheduling and prioritizing schemes are needed. At the transport layer, traditional TCP does not work because reliability concerns are not serious, due to many alternate sensor nodes that are sending the same information. Once again, transport protocols need to consider energy constraints and transmission times. Finally, many considerations have to be made at the application layer. The main consideration is that since sensors cannot store large programs, simple applications have to be used. Specialized protocols such as SMP (Sensor Management Protocol) are needed at the application layer.



HIGHER LAYERS (APPPLICATION, PRESENTATION, SESSION),
- Data Applications
- Voice applications

TRANSPORT LAYER
- End-to-End Message Delivery
- End-to-End Error Control

NETWORK LAYER
- Addressing
- Network Routing

DATA LINK LAYER
- Error Detection and Correction
- Contention Management (Multiple Access Control)
- Power Management

PHYSICAL LAYER
- Frequency Allocations
- Transmission and Propagation (Fading, Scattering, etc.)
- Signal Encoding (Modulation/Demodulation)

Figure 7-16: WSN Protocol Stack

In addition to the typical protocol stack issues, unique data management issues also arise in WSNs. Since sensors gather large amounts of data, managing the data in computationally weak sensors is a challenge. Some types of distributed data management schemes are needed. Security management is also an issue because sensors may collect highly sensitive information. In addition, WSNs use broadcasts over wireless networks – a dangerous combination that distresses security experts. Add to this the limited capabilities of nodes to handle sophisticated encryption and digital certificates, and you have a nightmare. Some solutions such as SNEP (Sensor Network Encryption Protocol) are being developed. Yet another issue is location management because approaches based on GPS simply do not work in WSNs.

A great deal of work, with many interesting and innovative approaches, is underway at present in this growing area. See Chapter 10 for a closer look at the various issues and the possible approaches.

7.7 Short Case Studies and Examples

7.7.1 UPS Adopts Bluetooth and GPS-enabled Scanners[2]

UPS delivers a worldwide service of transporting packages and has developed a system that allows UPS customers to track packages any where in the world. To be able to keep track of all the packages, UPS must scan each package at each major point on transit. The scanning is an essential part of the overall process, but it is time-consuming since every one of the millions of packages have to be scanned at numerous sites. UPS has developed a device called DIAD (delivery information access device) which can be used by the company's delivery workers to record signatures and delivery times when they drop off packages.

The current DIAD system requires that every loader has a hand scanner connected through a wire with a terminal on his belt that connects through a cellular network to the main server. The main server computes all the scans made by the loader. This process is inefficient. First, it requires the loader to have a device connected to his/her belt during the loading/unloading process. The battery of the unit also does not last very long, so during the 5-hour shifts, the loader must go change the battery. In addition, the current system is not commercially sold, so is expensive to repair and replace.

UPS has introduced a new DIAD system that uses Bluetooth (802.15) and WiFi (802.11). The loader has a wireless scanner that uses Bluetooth to connect to the DIAD terminal. This terminal connects to the main office server through a wireless LAN using Wi-Fi technology. Since both technologies use the 2.4 GHz frequency band, UPS uses time-division multiplexing so both technologies can coexist at the same time. Security is another concern in this new system, so the data was encrypted. The new system resolves many of the issues of the current system. Obviously, it is easier for the loader to have a wireless system instead of the cable connection of the current system. Also the life of the battery on the Bluetooth scanner is over 6 hours – this lets the loader work the whole 5-hour shift without having to recharge or change batteries. This has resulted in an increase in productivity.

UPS is also working on the next generation of its DIAD system. In addition to Bluetooth, it also supports GPS and can be supplied with a GPRS or 3G cellular network. GPS will increase the accuracy of pick-up locations, but UPS is not convinced about the real value of 3G cellular technology.

Sources

- D. Thomas, "UPS mail system packs in GPS and Bluetooth," May 4, 2004, http://www.computerweekly.com/Article130270.htm
- http://www.findarticles.com/cf_dls/m0MLY/3_3/99129893/p1/article.jhtml
- http://www.ups.com

7.7.2 Wireless Sensor Networks as a Replacement for Land Mines

Land mines have been used for years to prevent enemy truck or troop movement through remote areas. Soldiers traditionally lace the area with thousands of anti-truck or anti-personnel mines. Once the area has been mined, anyone moving through the area – friend or foe – is blown up. In addition to not being able to distinguish between friends or foes, the land mines

[2] Suggested by Felipe Hangen

present a long-range danger because, once installed, they cannot be disabled. Thus long after the conflict is over the mines are still active and deadly – killing or maiming people who happen to pass by. According to a UNICEF report, over the last 30 years, land mines have killed or maimed more than 1 million people – many of whom are children. Princess Diana of the UK, for example, campaigned aggressively against land mines before her own death.

MANETs offer a viable alternative to the land mines. To detect hostile movement in a remote area, an airplane scatters thousands of motes in that area, each one equipped with a magnetometer, a vibration sensor and a GPS receiver. The battery-operated motes are dropped at a density of one every 100 feet (30 meters) so that they can form a MANET. Each mote wakes up, senses its position and then sends out a radio signal to find its neighbors.

All of the motes in the area create a giant MANET that can collect important data. Data funnels through the network and arrives at a collection node, which has a powerful radio able to transmit a signal many miles to a control center. When an enemy truck drives through the area, the motes that detect it transmit their location and their sensor readings. Neighboring motes pick up the transmissions and forward them to their neighbors and so on, until the signals arrive at the control center and are transmitted to the commander. The commander can now display the data on a screen and see, in real time, the path that the truck is following through the field of motes. Then a remotely-piloted vehicle can fly over the truck, make sure it belongs to the enemy and drop a bomb to destroy it, if needed. This is naturally much more effective than using land mines. The main advantage is that after the conflict is over, the motes are tiny, completely harmless sensors that sit around collecting useless data that does not go anywhere. In addition, since the batteries of motes would last a year or two, they simply go silent after a while, presenting no physical threat to civilians nearby.

Source: Eva Kwan, Eric Shroup, Jim Polenski, “Mobile Ad Hoc Networks,” University of Pennsylvania Project Report.

7.7.3 Automobile Network Solutions with Bluetooth

Bluetooth SIG, with participation from IBM, has developed a Bluetooth Automotive Profile that describes how Bluetooth could be used in automobile network solutions. Scenarios illustrating how Bluetooth could be used in networked vehicles include:

- **The Car Office**: An in-vehicle Bluetooth network combined with personal Bluetooth devices brought into the car could enable access to personal and corporate data from the car. Using a mobile phone as the wide area network connection, the user could connect to the Internet or corporate intranet to retrieve information such as email. With voice recognition and synthesis technology in the automobile network, the phone audio could be routed through the vehicle’s audio system and the email or other data could be read to the user audibly. The user could then use voice commands to respond to email or make a voice call.
- **The Car Docking Station**: When a Bluetooth car is parked in the garage at home, it could connect to the home network using Bluetooth. Once bridged to the home network, information could be exchanged between the home and the automobile. This might include the car telling the home network of its current diagnostic and maintenance data (perhaps so that a message is delivered to the home information center reminding the owner that the car needs maintenance); or the car downloading new entertainment features (music, movies) from the home network, based upon user preferences and configuration. For commercial vehicles, the current day’s vehicle usage and tracking information could be uploaded and the next day’s schedule and route maps could be downloaded from the office network when the vehicle returns to the office at the end of

the day. Additional "virtual docking" scenarios could be accomplished anywhere a car might park. At the mall or parking garage, a "car finder" service could be deployed so that the owner could locate his or her car when leaving; at a gas station or store, the owner could be notified of special offers or discounts available at that time.

- **The Highway Helper**: This is a collection of applications that could leverage a Bluetooth in-vehicle network along with wide area network connectivity, such as via a mobile phone. One application is that of providing a user interface for the car's control and monitoring systems. In this scenario, when the car's sensors detect a problem, the user could be notified using the Bluetooth in-vehicle network; in addition, depending upon the nature of the problem, an email service reminder might be sent, the nearest service center could be located and notified, or a call for roadside help could be initiated. A second application is for vehicle navigation. In this scenario, current car location information (perhaps through a Global Positioning System or cellular triangulation) could be combined with map information to suggest driving routes and directions or locate the nearest restaurant or parking garage. Combined with an off-vehicle network connection, the user could even place a food order with the restaurant or make a reservation at the parking garage.

7.7.4 Examples of Mobile Sensor Networks

In many WSN applications, a mobile ad hoc network of intelligent sensors (MANIS) is formed between sensing devices. In a MANIS, traditional sensor nodes are replaced with MANIS nodes which communicate with a monitor/control system (MCS). The MANIS nodes use ASIC (application specific integrated chip) technology to minimize size and power consumption. A Wireless IEEE 1451 Standard has been proposed for Smart Sensor Networks. This standard includes:

- MANIS nodes. These network nodes run sensor/actuator applications and provide point-to-point connectivity with MCS and selectable connectivity to peer nodes.
- MCS. These network nodes run data-access algorithms or control applications and provide gateways to the corporate intranets or the public Internet.

The MANET algorithms are fault-tolerant and can work around failing or missing sensors/actuators. An MSC could discover the collection of sensors/actuators for which it is responsible and then form a communications web that carries sensor/actuator data back to the corporate intranets or the public Internet. There are several examples of using a MANIS:

- Supply Chain Monitoring: Motes could be installed on packages as they move through a supply chain to detect the movement of the product and report to an MCS. In addition, any damage done to the product while in the supply chain could be noted before the item is shipped to the customer.
- Meter Reader: Motes in an apartment complex could monitor the water and power meters and could form an ad hoc network amongst themselves since they may be within 100 meters of each other. An MCS could be part of this network with a network connection or a cell-phone link that sends all the data collected to a back-end system. This could eliminate the need for monthly meter readings.
- Smart Building Management: Motes could be attached to all electrical wires in an office building to detect power consumption in each area. An MCS could collect and present the information to a remote control center that could detect high power consumption in some areas and take corrective action, if needed.
- Traffic Monitoring: Motes placed every 100 meters on a highway and equipped with sensors to detect traffic flow could help police recognize where an accident has stopped traffic.

7.7.5 Bank Tests Bluetooth-based Biometric ID System

The Bank of America has started testing a Bluetooth-based, biometric customer identification system that uses the Bluetooth wireless technology to transmit and release account information to a bank teller. The Touch ID device allows customers to use their fingerprints to authorize financial transactions by transmitting identification to a teller. Customers using Touch ID place a fingertip against a reader at the teller window. A fingerprint sensor in the Touch ID device compares the electronic fingerprint with a fingerprint impression given by the customer when he enrolled in the pilot program. Once a match occurs, the Touch ID device transmits account information stored in the device to the teller, authorizing a transaction. This can be used instead of the driver license or other identification systems. Bank of America claims that the Touch ID system raises the identification security level to a new high and secures banking transactions. It also protects the privacy and legitimacy of the banking customers. All information transmitted by the Touch ID system is encrypted for security.

Source: B. Brewin, "Bank tests Bluetooth-based biometric ID system," Computerweekly.com, May 12, 2004.

7.8 Analysis of WPAN Technologies and Conclusions

The principal WPAN technology at present is Bluetooth. However, IEEE 802.11 LANs are also quite popular in the WPAN space. New entrants such as UWB and wireless sensor networks (WSNs) are also playing a significant role in WPANs. The following table captures the main properties of the key players.

Table 7-4: Players in the Wireless Personal Area Networks

Factor	Bluetooth	Wi-Fi	UWB	WSN
Data Rate	1 Mbps	11 Mbps	50 Mbps	< 1 Mbps
Distance Covered (range)	10 meters	100 metters	10 Meters	10-30 meters between motes
Application focus	Cable replacement	Connection to corporate networks	Military applications so far, home entertainment in future	Numerous military and civilian applications
Frequency Band	2.4 GHz	2.4 GHz	3.1 – 10.6 GHz	Unregulated
Ease of use	Piconets very easy to use for small networks	Complex even for 2 devices	Complex and intricate	Easy to use, once installed
Security	Multiple levels (link level, application level)	WEP and its improvements	Very high security	Many security exposures

Bluetooth is intended for short distance and relatively slow (10 meters, 1 Mbps) users. As discussed previously, Bluetooth technology is designed for wireless communications between personal electronic devices in close proximity to each other. The Bluetooth technology is based on a short-range radio link built into small application-specific integrated circuits (ASICs). It can support both stationary and mobile communications and uses frequency hopping, with 1,600 hops per second as opposed to 50 hops per second in HomeRF. Bluetooth supports data transmissions between devices of up to 721 Kbps and offers up to three voice channels. Bluetooth, like Wi-Fi, operates in the 2.4 GHz band. Bluetooth technology enables a user to replace cables between devices such as printers, fax machines, desktop computers and peripherals, and a host of other digital devices. Furthermore, Bluetooth technology can provide a connection between the ad hoc network and existing data networks. Bluetooth technology is popular because of its simplicity and its support from large companies. And Bluetooth members are encouraging vendors to incorporate the technology into their products by waiving intellectual property royalty fees.

IEEE 802.11 LANs are based on the wireless Ethernet specification. The most popular at present, 802.11b (also known as Wi-Fi), was originally designed to enable high-performance radio to support roaming in large offices or business campus environments. Although 802.11b supports voice-over-Internet protocol, it uses a distributed-contention-based algorithm which induces latency in voice transmissions. Initially, 802.11b did not completely support telephone functionality – features like caller ID, for example, were not available. But many 802.11-based telephone networks are appearing in the marketplace – see, for example, the system from Vocerra (www.vocerra.com).

UWB is a new player that provides highly secure and fast wireless communications over short distances. Although most UWB applications have been in the military area, UWB is finding niche applications such as highly secure WPANs and wireless HDTV.

Wireless sensor networks, though operating in the short-range radio area, have several unique features that do not directly match the other players in the WPAN market.

Moving forward, two possible scenarios exist. It is possible that several wireless technologies will survive the test of time and will find segments of long-range users. For example, HomeRF did not survive, dispute a great deal of initial fanfare. Bluetooth seems to be well entrenched for replacement of cabled computer attachments, and Wi-Fi is simply becoming a wireless network of choice for many home and office situations. The success of Bluetooth and Wi-Fi creates many interoperability problems and is creating a market for black boxes that translate between standards. There is a possible scenario that one technology will overtake all others. The strongest contender is the 802.11 family, especially the 802.11g networks, with 54 Mbps data rates that can handle HDTV and many other applications. It can compete with Bluetooth as well as UWB. Only time will tell.

7.9 Review Questions and Exercises

1) Expand Table 7-1 to include two more factors.

2) Draw a diagram to show which subtasks of the IEEE 802.15 are addressing what aspects of WPAN.

3) Why is it important to examine cordless systems? Compare and contrast cordless networks with cellular networks.

4) What are the distinguishing features of HomeRF to remember it by?

5) What are the main features of Bluetooth? Compare and contrast Bluetooth with 802.11b.

6) Scan the literature to identify some applications of Bluetooth applications.

7) Create a table that describes the various Bluetooth protocols (one row per protocol). For each protocol, give a one-line description, and indicate if it is required or adopted, as well as the layer at which it operates.

8) What is UWB and what are its main features? Which technologies does UWB compete against and why?

9) What are wireless sensor networks and what are their major applications?

10) What is the main criterion in designing WSNs and how does it impact various design choices?

7.10 References

Aiello, R., et al. "Understanding UWB – Principles and Implications for Low-Power Communications – A Tutorial." Available at: http://www.discretetime.com/papers/03157r0P802-15_WG-Understanding_UWB_For_Low-Power_Communications-A_Tutorial.pdf

Blankenhorn, D. "Ultra Wideband." *Mobile Radio Technology*. 1 January 2003. Available at http://iwce-mrt.com/ar/radio_ultra_wideband/

Briere, D. *Wireless Home Networking for Dummies*. For Dummies, 2003

Geier, Jim. *Wireless LANs*. 2nd ed. SAMS, 2002.

Gutierrez, J., et al. *IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks*. IEEE, 2003.

Hill, J., et al, "The Platforms Enabling Wireless Sensor Networks", CACM, June 2004, pp. 39-46.

Prasad, R. and Munoz, L. *WLANs and WPANs towards 4G Wireless*. Artech, 2003.

Sikora, A. *Wireless Personal and Local Area Networks.* Wiley, 2003.

Stallings, W. *Wireless Communications and Networks*. Prentice Hall, 2002.

Main Websites and Useful Web Links

- IEEE 802.15 official website (http://www.ieee802.org/15/) for WPANs
- A very good site for extensive tutorials on different aspects of wireless (www.palowireless.com)
- The Bluetooth website (www.bluetooth.com)
- The Ericsson Bluetooth site (http:\\Bluetooth.ericsson.se)
- DECT website (www.dectweb.com)
- Wireless LAN Association website (www.wlana.org)
- 802.11 resources (www.palowireless.com/80211)
- General wireless information (www.wireless.ittoolbox.com)