Recent Developments In Wireless Network Systems

By

Mehmet Ali NUREL

A Dissertation Submitted to the
Graduate School in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

Department: Computer Engineering
Major: Computer Software

İzmir Institute of Technology
İzmir, Turkey

September, 2001

We approve the thesis of **Mehmet Ali NUREL**

Date of Signature

25.09.2001

…….. .....

Prof. Dr. Halis PÜSKÜLCÜ
Supervisor
Department of Computer Engineering

25.09.2001

…….. .....

Prof. Dr. Sıtkı AYTAÇ
Department of Computer Engineering

25.09.2001

…….. .....

Asst. Prof. Dr. Tuğkan TUĞLULAR
Department of Computer Engineering

25.09.2001

…….. .....

Prof. Dr. Sıtkı AYTAÇ
Head of Department

ACKNOWLEDGMENTS

I would like to thank to my advisor *Prof. Dr. Halis PÜSKÜLCÜ,* firstly for his advice about studying on this subject and for his enduring support and supervision that made this thesis possible.

Additionally, my deepest thanks to my colleagues for their support. I also present my special thanks to my family for their patients and love especially to my wife, *Bengü* for her great encouragement.

ABSTRACT

Recent Developments In Wireless Network Systems

by Mehmet Ali NUREL

Over last decades, a tremendous growth in wireless communication systems could be seen. This great success of wireless telephony and messaging systems, nowadays, is beginning to be applied to the world of personal and business computing systems. As a result, instead of facing with the some problems or restrictions of the wired networks, people could access and share information nearly anywhere they want on the earth.

This study is aimed to present the various aspects of wireless systems. In order to do this the history of wireless network systems is introduced, some definitions are extracted, the answers to the some basic questions on why and where wireless networks can be applied are given and the definitions of protocols that have been developed are presented. Moreover, the benefits of wireless networks, related configurations and standards, several underlying technologies, and some markets related with wireless systems are described. Comparisons between wireless and wired networks and among each other are also given.

ÖZ

Kablosuz Ağ Sistemlerindeki Son Zamanlarda Meydana Gelen Gelişmeler

Son yıllarda kablosuz iletişim sistemleri uygulamalarında ve kullanımında olağanüstü bir gelişme gözlenmektedir. Kablosuz telefon ve mesaj sistemlerinin göstermiş olduğu bu büyük başarı, kablosuz sistemlerinin kişisel ve iş bilgi sistemleri dünyasına da uygulanmaya başlanmasına neden olmuştur. Bunun sonucunda, kablolu ağların bazı problemleri ve kısıtlamaları ile karşılaşmak yerine, insanlar, dünya üzerinde bulundukları her yerden kablosuz sistemler yardımı ile istedikleri bilgilere ulaşabilmekte ve bunları paylaşabilmektedirler.

Bu çalışmada kablosuz sistemlerin çeşitli yönleriyle tanıtılması amaçlanmıştır. Bunun için, kablosuz ağ sistemlerinin tarihçesine biraz değinilmiş, bazı tanımlamalar üzerinde durulmuş, kablosuz ağlar nerede ve ne zaman uygulanabilir gibi temel soruların cevapları verilmiş, ve geliştirilen protokoller tanıtılmıştır. Bunların yanı sıra, kablosuz ağların sağladığı avantajlardan, ilgili konfigürasyonlar ve standartlardan, çeşitli teknolojiler ve kablosuz sistemlerle ilgili pazarlardan bahsedilmiştir. Kablosuz sistemlerin kendi aralarındaki ve kablolu sistemlerle olan karşılaştırılmaları, ayrıca verilmiştir.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

There has been an enormous growth on the market for wireless communications over recent years [27]. Nowadays, wireless technology reaches or is able to virtually reach to the every location on the earth. Every day hundreds of millions of people exchange information using pagers, cellular telephones, and other wireless communication products. With the great success of wireless telephony and messaging services, the wireless communication is beginning to be applied to the almost all the aspects of personal and business computing. It is very near, for the benefit of human being with the usage of wired networks, people will be able to access and share information and data on nearly anywhere on the earth where they want.

1.1 Motivation

As a result of the success of the Ethernet project at Xerox's Palo Alto Research Center in the early 1970's and other similar digital protocols, the basic technology has found the chance of growth for local area networks (LANs) in both the public and private sectors [27]. Standard LAN protocols, such as Ethernet, that operate at fairly high speeds with inexpensive connection hardware can bring digital networking to almost any computer. Today, organizations of every size access and share information over a digital network. The power and the benefits of networking and collaborative, distributed computing are beginning to be noticed. However, until recently, LANs were beginning to be limited with the physical, hard-wired infrastructure of the buildings. Even with phone dial-ups, network nodes were limited to access through wired, landline connections. Many network users, especially mobile users in business, the medical profession, factories, and universities etc. find benefit from the added capabilities of wireless LANs.

Wireless LAN technology is rapidly becoming a crucial component of computer networks, and its use is growing by leaps and bounds [12]. At the beginning wireless technology was the world of lots of proprietary implementations. But by the finalization of the IEEE 802.11 wireless LAN standard, it become an open solution for providing mobility as well as essential network services where wireline installations seemed to be impractical. Now companies and organizations are increasingly investing in wireless networks to take advantage of mobile, real-time access to information.

Today, most wireless LAN suppliers have 802.11-compliant products, allowing companies to realize wireless network applications. After the 802.11 standardization, there is a trend for lowering prices and enabling wireless LANs to operate. This is making the implementations of wireless networks more feasible than before, creating vast business opportunities for system implementation companies and consultants.

Many end-user companies and system integrators, however, have little knowledge of, and experience in, developing and implementing wireless network systems. In many cases, there is also confusion over the capability and effectiveness of the 802.11 standard. The implementation of wireless networks is much different from traditional wired networks. In contrast to Ethernet, a wireless LAN has a large number of setup parameters that affect the performance and operability of the network. An engineer designing the network and the person installing the network must understand these parameters and how they affect the network.

Wireless and mobile networks have provided the flexibility required for an increasingly mobile workforce [39]. As shown in figure 1.1(a), the worldwide number of cellular, GSM, and PCS subscribers increased from 140 million in 1996 to over 300 million in 1999 and is expected to grow to 650 million by 2001 [48]. In the U.S., capital investment increased from $6.3 billion in 1990 to $66.8 billion in 1999 and service revenues were up from $4.5 billion to $38.7 billion in 1999 [55] as shown in figure 1.1(b). During the same period, the average local monthly bill diminished from $80 to $39 as shown in figure 1.1(c), indicating the technological maturity and the tremendous competition among service providers.

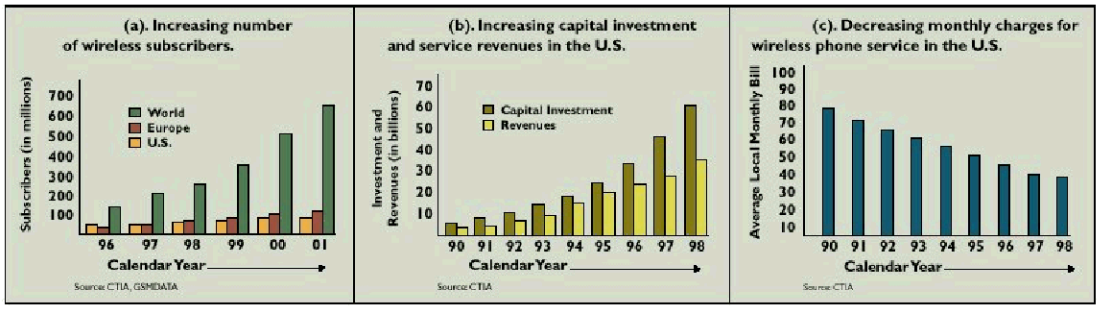

FIGURE 1.1 Recent changes in usage [55]

1.2 History of Wireless Networks

The first wireless networks were developed in the preindustrial age [43]. These systems transmitted information over line-of-sight distances using smoke signals, torch signaling, flashing mirrors, signal flares, and semaphore flags. An elaborate set of signal combinations was developed to convey complex messages with these fundamental signals. Observation stations were built on hilltops and along roads to relay these messages over large distances. These early communication networks were replaced first by the telegraph network (invented by Samuel Morse in 1838) and later by the telephone. In 1895, twenty years after the telephone was invented. Marconi demonstrated the first radio transmissions over larger distances with better quality, less power, and smaller, cheaper devices, thereby enabling public and private radio communications, television and wireless networking.

Early radio systems transmitted analog signals. Today most radio systems transmit digital signals composed of binary bits, where the bits are obtained directly from a data signal or by digitizing an analog voice or music signal. A digital radio can transmit a continuous bit stream or it can group the bits into packets. The latter type of radio is called a packet radio and is characterized by bursty transmissions the radio is idle except when it transmits a packet. The first packet radio network, Alohanet, was developed at the University of Hawaii in 1971. This network enabled computer sites at seven campuses spread out over four islands to communicate with a central computer on Oahu via radio transmission. The network architecture used a star topology with the central computer at its hub. Any two computers could establish a bi-directional communications link between them by going through the central hub.

Alohanet incorporated the first set of protocols for channel access and routing in packet radio systems, and principles underlying these protocols are still in use today. Activity in packet radio, promoted by DARPA, peaked in the mid 1980s, but the resulting networks fell far short of expectations in terms of speed and performance. Packet radio networks today are mostly used by commercial providers of wide area wireless data access. These services, first introduced in the early 1990s, enable wireless data access (including e-mail, file transfer, and web browsing) at fairly low speeds, on the order of 20 Kbps. The market for these data services has not grown significantly.

In the 1970s Ethernet technology steered companies away from radio-based networking. Ethernet's 10 Mbps data rate far exceeded anything-available using radio.

In the 1980s, amateur radio hobbyists, hams, designed and built terminal node controllers (TNCs) [59]. They aimed to interface their computers through ham radio equipment (figure 1.2), so that, they kept radio networking alive within the United States and Canada. TNCs act much like a telephone modem, converting the computer's digital signal into one that a ham radio can modulate and send over the airwaves by using a packet-switching technique. In fact, the American Radio Relay League (ARRL) and the Canadian Radio Relay League (CRRL) have been sponsoring the Computer Networking Conference since the early 1980s to provide a media for the development of wireless WANs. Thus, hams have been utilizing wireless networking for years, much earlier than the commercial market.

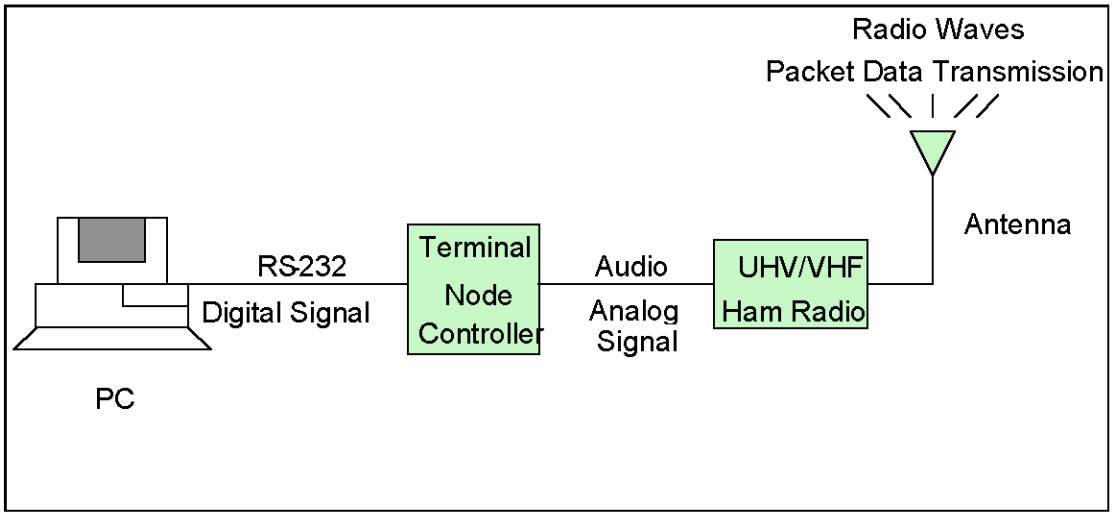

FIGURE 1.2 Terminal node controllers with a ham radio [Geiger 1999]

In 1985 the Federal Communications Commission (FCC) enabled the commercial development of wireless LANs by authorizing the public use of the Industrial, Scientific, and Medical (ISM) frequency bands for wireless LAN products. This band of frequencies resides between 902 MHz and 5.85 GHz, just above the cellular phone operating frequencies.

The wireless LAN vendors were very pleased with this occurrence and also were attracted by the ISM band since they did not need to obtain an FCC license to operate in this band [43]. However, the wireless LAN systems could not interfere with the primary ISM band users, which forced them to use allowed power profile and an inefficient signaling scheme. Moreover, the interference from primary users within this frequency band was quite high. As a result, these initial LAN systems had very poor performance in terms of data rates and coverage. The ISM band allocation has had a dramatic effect on the wireless industry, prompting the development of wireless LAN components [59]. Without a standard, however, vendors began developing proprietary radios and access points.

The primary wireless LAN technologies had some shortcomings as operating in the 900 MHz, having low speed (1-2Mbps), lack of standardization, high cost and concerns about security [13]. Nevertheless, the freedom and flexibility of wireless enabled these early products to find there some way into markets like retail and warehousing where mobile workers used hand-held devices for inventory management and data handling.

In 1991, Aironet started to develop the standards with other wireless companies by notifying the success of the wireless LANs acceptance in the market.

Around 1992, wireless LAN makers began developing products operating in the unlicensed 2.4 GHz frequency band. This caused the formation of two additional vertical markets. Healthcare, with a highly mobile workforce, began using portable computers to access patient information. And as computersmade products was founding the way into the classrooms more, educational institutions began installing wireless networks to avoid the high cost of wiring buildings.

In the late 1980s, the Institute of Electrical and Electronic Engineers (IEEE) 802 Working Group, responsible for the development of LAN standards, such as Ethernet and token ring, began development of standards for wireless LANs [59]. Under the chairmanship of Vic Hayes, an engineer from NCR, the IEEE 802.11

Working Group developed the Wireless LAN Medium Access Control and Physical Layer specifications.

The IEEE Standards Board approved the standard on June 26,1997, and the IEEE published the standard on November 18, 1997. IEEE 802.11 standard supports transmission in infrared light and two types of radio transmission within the unlicensed 2.4 GHz frequency band: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). The finalizing of this standard was encouraging the producers to release 802.11-compliant radio cards, access points and other products throughout 1998. Other manufacturers new to the wireless market are now sure to develop and release 802.11-compliant products based on the standard blueprint provided by the 802.11 standard.

Another widely accepted wireless network connection has been wireless WAN services, which began surfacing in the early 1990s. Companies such as ARDIS and RAM Mobile Data were first selling wireless connection equipments between portable computers, corporate networks, and the Internet. Companies then began developing and introducing Cellular Digital Packet Data (CDPD) services. These kinds of services enable users to send and receive data packets by using digital transmission services. Those developments enable people to access email and other information services from their personnel devices without using the telephone system while meeting with customers, traveling in the car, or staying in a hotel etc.

Today, by the help of adoption of the IEEE 802.11b WLAN standard, the speeds of greater than 10 Mbps Ethernet-like data transmission availability, and the existence of wireless PC Card adapters, wireless networking has come of age and become the new fact of the any kind of network systems. Now, faster, more robust products are available that offer unparalled speeds and standards-based operability.

By far, the most successful application or wireless networking has been the cellular telephone system [43]. Cellular telephones have approximately several hundreds million subscribers worldwide, and their growth continues at an exponential rate. The mixing of radio and telephony systems were in 1915, when wireless voice transmission between New York and San Francisco was first established. In 1946 public mobile telephone service was introduced in 25 cities throughout the United States. These initial systems used a central transmitter to cover an entire metropolitan area. This inefficient use of the radio spectrum coupled with

the state of radio technology at that time severely limited the system capacity. Thirty years after the introduction of mobile telephone service the New York system could only support 543 users. A solution to this capacity problem emerged during the fifties and sixties when researchers at AT&T Bell Laboratories developed the cellular concept.

Cellular systems exploit the fact that the power of a transmitted signal fails off with distance, so the same frequency channel can be allocated to users at spatially separate locations with minimal interference. A cellular system divides a geographical area into adjacent, monoverlapping "cells". Cells assigned the same channel set are spaced apart so that interference between them is small. Each cell has a centralized transmitter and receiver (called a base station) that communicate with the mobile units in that cell, both for control purposes and as a call relay. All base stations have high-bandwidth connections to a mobile telephone switching office (MTSO), which is itself connected to the public-switched telephone network (PTSN). The handoff of mobile units crossing cell boundaries is typically handled by the MTSO, although in current systems some of this functionality is handled by the base stations and/or mobile units.

The original cellular system design was finalized in the late 1960s and deployed in the early 1980s. The large and unexpected growth led to the development of digital cellular technology to increase capacity and improve performance.

The current generations of cellular systems are all in digital. In addition to voice communication, these systems provide e-mail, voice mail, and paging services. Unfortunately, the great market potential for cellular phones led to an increase in digital cellular standards. For instance, today there are three different digital cellular phone standards in the U.S. alone, and other standards in Europe and Japan, none of which are compatible. The incompatible standards make roaming throughout the U.S. using one digital cellular phone impossible. Most cellular phones today are dual-mode: they incorporate one of the digital standards along with the old analog standard that provides coverage.

Radio paging systems represent another example of a successful wireless data network. Their popularity is starting to decrease with the widespread penetration and competitive cost of cellular telephone systems. Paging systems allow coverage over

very wide areas by simultaneously broadcasting the pager message at high power from multiple base stations or satellites. Early radio paging systems were analog 1-bit messages signaling a user that someone was trying to reach him or her. These systems required callback over the regular telephone systems to obtain the phone number of the paging party.

Paging systems now allow a short digital message, including a phone number and brief text, to be sent to the pagee. In paging systems most of the complexity is built into the transmitters, so that pager receivers are small, lightweight, and have a long battery life. The network protocols are also very simple since broadcasting a message over all base stations requires no routing or handoff. The spectral inefficiency of these simultaneous broadcasts is compensated by limiting each message to be very short. Paging systems continue to evolve to expand their capabilities beyond very low-rate one-way communication. Current systems are attempting to implement two-way, "answer-back" capability. This requires a major change in pager design, since it must now transmit signals in addition to receiving them, and the transmission distances can be quite large.

Commercial satellite communication systems form another major component of the wireless communications infrastructure. They provide broadcast services over very wide areas and help fill the coverage gap between high-density user locations. Satellite mobile communication systems follow the same basic principle as cellular systems, except that the cell base stations are now satellites orbiting the earth. Satellite systems are typically characterized by the height of the satellite orbit, low-earth orbit (LEO), medium-earth orbit (MEO), or geosynchronous orbit (GEO).

The idea of using geosynchronous satellites for communications was first suggested by the science fiction writer Arthur C. Clarke in 1945. However, the first deployed satellites, the Soviet Union's Sputnik in 1957 and the NASA-Bell Laboratories Echo-1 in 1960, were not geosynchronous due to the difficulty of lifting a satellite into such a high orbit. The first GEO satellite was launched by Hughes and NASA in 1963, and from then until very recently GEOs dominated both commercial and government satellite systems. The current trend is to use lower orbits so that lightweight handheld devices can communicate with the satellite. Services provided by satellite systems include voice, paging and messaging services, all at fairly low data rates.

1.3 The Components of a Wireless Network

In general wireless networks perform the similar functions to transfer the information from source to destination with other wired network systems such as Token-ring and Ethernet. Generally speaking networks do the below tasks to manage transfers.

1. The medium provides a bit pipe (path for data to flow) for the transmission of data.
2. Medium access techniques facilitate the sharing of a common medium.
3. Synchronization and error control mechanisms ensure that each link transfers the data intact.
4. Routing mechanisms move the data from the originating source to the intended destination.
5. Connectivity software interfaces an appliance, such as pen-based computer or bar code scanner, to application software hosted on a server.

The network architecture, whether wireless or wired, which is basically composed of the protocols, major hardware, and software elements, may be considered in two parts, physically and logically.

1.3.1 Physical Architecture of a Wireless Network

The physical components of a wireless network implement the Physical, Data Link, and Network Layer functions to satisfy the functionality needed within local, metropolitan, and wide areas.

1.3.1.1 End-user Appliances

Users always needs to interface with applications and services for any given system. There is no matter the network is being wireless or wired, an end-user appliance is an interface between the user and the network. The most used devices that classified as end-user appliances can be listed as:

- Desktop workstations
- Laptop computers

- Palmtop computers
- Handheld PCs
- Pen-based computers
- Personal digital assistants (PDA)
- Handheld scanners and data collectors
- Handheld printers

It is definite that the features of physical components of a wireless network extend the capability of Ethernet and token ring.

1.3.1.2 Network Software

In the different part of it, a wireless network is consisted of some kind of software. Because the underlying nature of the system, many network operating systems (NOS's) are server oriented where the main application software and databases exist. In most cases, the appliances will interface via TCP/IP with application software or a database running on the NOS.

Client software, running on the end-user's device, directs the user's commands to the local appliance software, or steers them out through the wireless network. The wireless network software residing on the appliance is too resembles to the wired one except that it has to be optimized for working in a relatively small amount of underlying network's bandwidth.

The software performing application functions can run on a server/host, the end-user device, or a combination of both. In some cases, such as with applications running on an IBM mainframe, IBM AS/400, or UNIX-based hosts, the wireless appliances may need to run terminal emulation. By performing this function, the appliance act as a dummy terminal, just interfacing the keyboard, screen, printer, and so on, with the application running on the host. With client/server systems, the software on the appliance may perform part or all of the application's functionality and merely interface with a database located on a server, such as Microsoft NT Server.

A wireless network appears transparent to application software and operating systems on the network. As a result, applications written for a wired network can generally run without changes over a wireless network but of course not all the time.

In some cases there is a need for using a gateway running as middleware to provide an interface between the appliance and the application software running on the server. By using the gateway, the network appliances can communicate with the host/server. The gateway can be used as a proxy for the various appliances. The main advantages of using a gateway can be situated as:

- *Better RF throughput:* With the presence of a transport and application gateway, there is a chance for the appliances communicate with the gateway by using a refined protocol that is more wireless friendly, unlike TCP/IP.
- *Reliability:* Because the gateway proxies all the appliances, any outages in communication due to the appliances roaming out of range are transparent to the host/server.
- *Longer battery life:* When the appliances are idle, the network software does not have to periodically send out keep-alive packets to keep the connection to the host/server open. The gateway can manage this.

1.3.1.3 Wireless Network Interface

Computers use low direct current (DC) voltages representing data 1s and 0s to process information digitally. But these signals are intended to be optimum use for transmissions within the computer not for transporting data through wired or wireless media. A wireless network interface couples the digital signal to enable an efficient transfer of data between sender and receiver. This process includes the modulation and amplification of the digital signal to a form acceptable for propagation to the receiving location.

Modulation is the process of translating the baseband digital signal used in the device to an analog from suitable for transmission through the air. This process is very similar to the common telephone modem. The wireless modulator translates the digital signal to frequency that propagates well through the atmosphere. Of course wireless networks employ modulation by using radio waves and infrared lights.

The wireless network interface generally gets the shape of a network interface card (NIC) or an external modem that performs the modulator and communication protocols. These devices speak with user appliances by using a computer bus, such as ISA (Industry Standard Architecture) or PCMCIA (Personal Computer Memory Card Interface Architecture). Additionally some manufactures also produce wireless devices that use the RS-232 serial port to communicate.

The interface residing between the user appliance and NIC also uses a software driver to perform communication. The most common driver standards are:

• *NDIS (Network Driver Interface Specification):* Driver used with Microsoft network operating systems

• *ODI (Open Datalink Interface):* Driver used with Novell network operating systems

• *PDS (Packet Driver Specification):* A generic DOS-based driver developed by FTP Software, Inc. for use with TCP/IP-based implementations.

Former radio cards generally have two pieces to manage a link, one for transiting activity and the other for user appliance connectivity. This structure may be acceptable for big size devices such as forklift-mounted appliances but not operable for most handheld appliances. Newer ones have one piece as a PCMCIA card that inserts into the appliance with an integrated radio and transceiver assembly.

1.3.1.4 Antenna

The antenna is an instrument that radiates the modulated signal into the air providing that destination node can receive. Antennas are produced in various shapes and sizes and have some special electrical characteristics as:

• Propagation pattern

• Gain

• Transmit power

• Bandwidth

The propagation pattern defines the coverage capability of an antenna. A real omnidirectional antenna transmits its power in all directions, whereas, a directional antenna concentrates most of its power in one direction. Figure 1.3 illustrates the differences.

Gain refers to degree of amplification. A directional antenna has more gain than the omnidirectional one and also propagates the signals farther because of focusing the power in a single direction. The directivity characteristic of an antenna defines the amount of gain. Because that omnidirectional antenna does not focus in one direction to propagate it has the degree of "1" as gain. They are the most suitable type of antennas for indoor wireless networks by requiring the relatively shorter ranges and so less susceptible to outward interference.

In contrast to omnidirectional, directional antennas are good for satisfying the requirements of interconnecting buildings within metropolitan areas. Their characteristics of having huge ranges and minimal interference with other systems are the key points of usage within metropolitan areas.

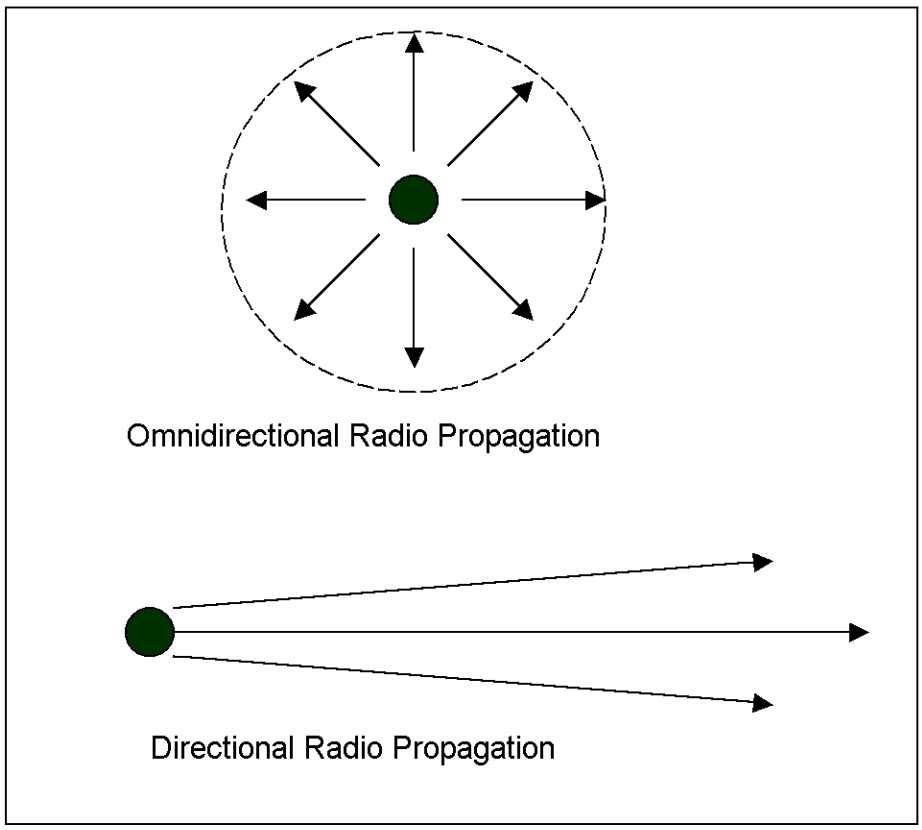

FIGURE 1.3 Omnidirectional and directional antenna propagations. [Geiger 1999]

The combinations of transmit *power* and gain of an antenna defines the distance the signal will propagate. Long-distance transmissions require higher power and

directive radiation patterns, whereas, shorter distance transmissions can get by with less power and gain. With wireless networks, the transmit power is relatively low, typically one watt or less.

In the market there are mainly three types of antennas are sold by most spread spectrum radio vendors:

• *Snap-on antenna*: Connects directly to the radio card and provides relatively low gain via an omnidirectional radio propagation pattern. This relatively small antenna is best for highly mobile applications when a larger antenna is impractical.

• *Dipole antenna*: Sits on a desk or table and connects to the radio card via a short antenna cable. This approach provides relatively low gain. This antenna is best for portable applications.

• *High gain antenna*: Attaches to a wall or antenna pole/tower and connects to the radio card or access point via a relatively long antenna cable. This approach provides relatively high gain and is best for access points and permanent stations.

The last characteristics *bandwidth* is the effective part of the frequency spectrum that the signal propagates. As an example the classical telephony system operates over a bandwidth roughly from 0 to 4 KHz. This range is enough for us to accommodate most of the frequency components within our voices. Of course radio systems have much more bandwidth amounts at much higher frequencies to satisfy the accumulation of data. Data rates and bandwidth are directly proportional: if there is a need for high data rates, there is also need for more bandwidth.

1.3.1.4.1 Sectored Antenna

These are very similar to directional antennas, and heavily used in cellular phone base stations. A set of wide-angle directional antennas is assembled on a vertical pole, each one covering one portion of the horizon (a sector, for example 3 antennas 120 degrees wide). When talking to a specific node, the base station just select the sector of the sectored antenna that cover this node, giving the benefit of directionality without sacrificing the coverage.

1.3.1.4.2 Beam Forming Antenna

This is an adaptive directional antenna, using a set of unidirectional antennas and interferometry to enhance the signal. Basically, by adding all the signal of the different antennas with specific offset (to compensate propagation delay), it is possible to aim the system towards a specific direction and have the same benefit as directional antenna. As this system is adaptive and dynamic, it could be used for Wireless LANs.

1.3.1.5 Wireless Local Bridges

Bridges are the main part of system to be a network because they supply the connections of multiple LANs at the Medium Access Control (MAC) layer to form a single logical network. The MAC layer mainly provides medium access functions and it is part of IEEE's architecture describing LANs. By combining with Logical Link Control (LLC) the functionality of the MAC layer constitute the Data Link Layer of ISO's OSI Reference Model. Bridges connects LANs together such as Ethernet to Ethernet or Ethernet to token ring and provides them to understand each other. They also provide a filtering of packets based on their MAC Layer address so that an organization can be segmented within an enterprise network.

If a networked station sends a packet to another station located on the same segment, the bridge will not forward the packet to other segments or the enterprise backbone. If the packet's destination is on a different segment, however, the bridge will allow the packet to pass through to the destination segment. Thus, bridges ensure that packets do not wander into parts of the network where they are not needed. This process, known as *segmentation,* makes better use of network bandwidth and increases overall performance.

There are mainly two types of bridges:

• *Local bridges:* These connect LANs within close proximity.

• *Remote bridges:* These connect sites that are separated by distances greater than the LAN protocols can support.

Figure 1.4 illustrates the differences between local and remote network bridges. It can be briefly stated that, local bridges connect LANs within a local area, whereas remote bridges connect LANs over a wider area.

Most companies that develop wireless LAN NICs also sell a wireless local bridge referred to as an *access point* that makes available connections to wired network-based servers and enables multiple wireless cell configurations. The filtering process of a local bridge (whether it is a wireless or wired type) is critical in maintaining a network configuration that minimizes unnecessary data traffic. The combination of wireless NICs and bridges gives network managers and engineers the ability to create a variety of network configurations. A wireless LAN can assume two main configurations: single-cell and multiple-cell.

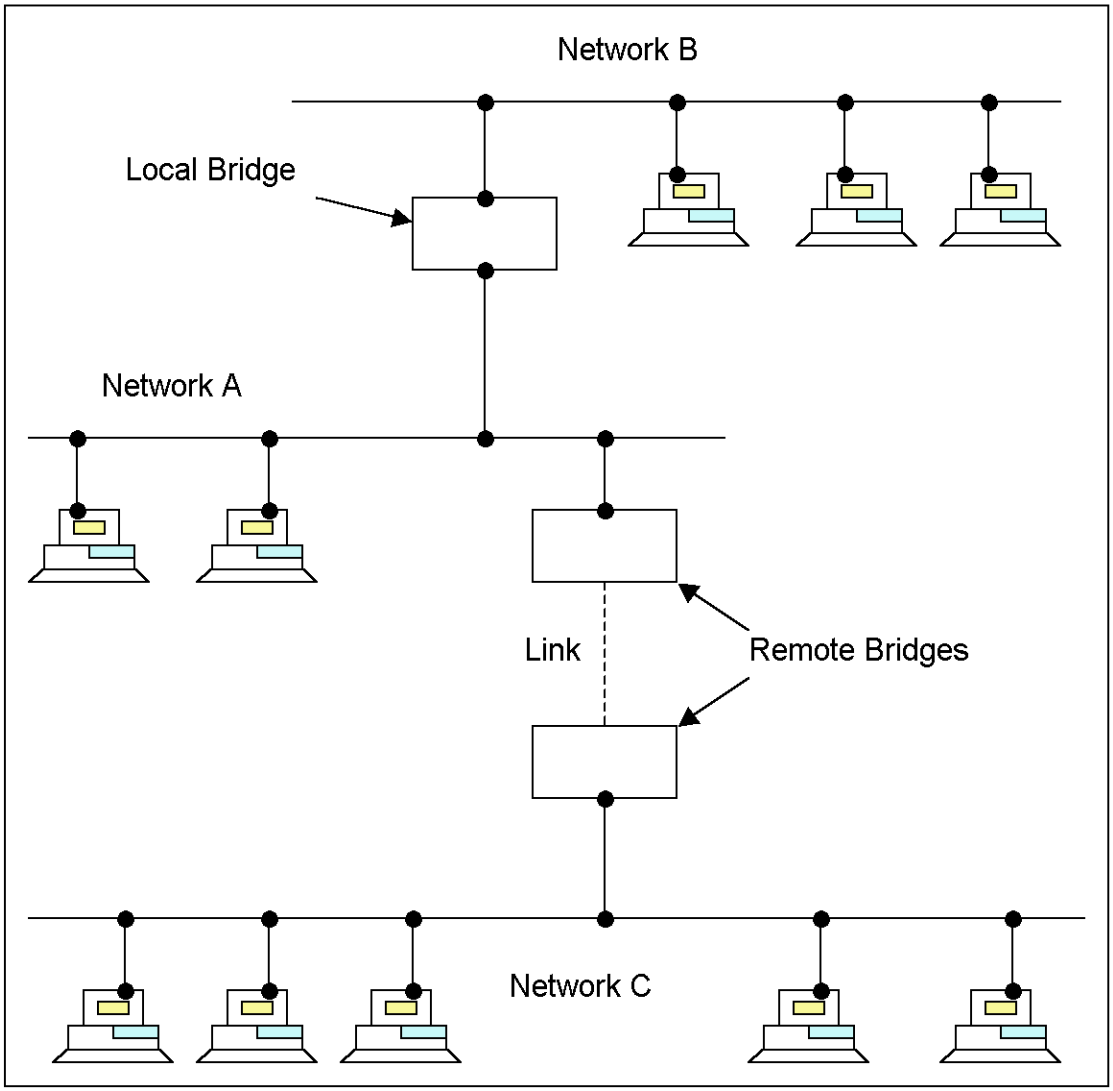

FIGURE 1.4 Local and remote bridges [Geiger 1999]

1.3.1.6 Wireless And Mobile Middleware

Middleware unites different applications, tools, networks, and technologies, giving users a common interface [40]. Mobile middleware is an enabling layer of software to connect e-commerce applications with different mobile networks and operating systems without introducing mobility awareness—the need to adjust to wide variations in bandwidth and resulting delays, and changes in user location—in the applications, as figure 1.5 shows.

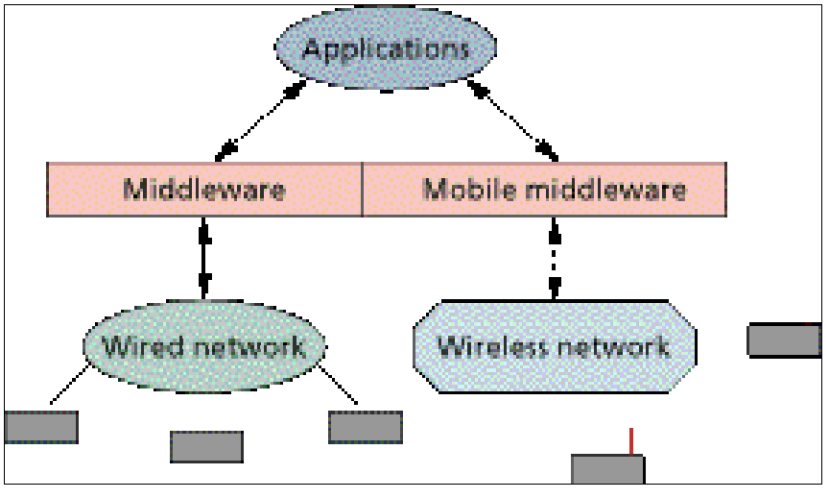

FIGURE 1.5 Mobile middleware [Varshney 2000]

Mobile middleware can hide the differences in applications from a mobile user. It can also reduce the content size and format to better adapt to the inherent characteristics of wireless networks and the limitations of mobile devices.

Middleware gives applications better response times and far better reliability. Typically, middleware uses optimization techniques, such as header compression, delayed acknowledgments, and concatenation of several smaller packets into one to reduce wireless network traffic. Some middleware supports intelligent restarts, which take the user to the break point after disconnection instead of back to the beginning. With its ability to hide the underlying network's details from applications while providing a uniform and easy-to-use interface, middleware is extremely important for developing new mobile commerce applications. Middleware, however, does introduce additional complexity and significant initial cost.

1.3.1.7 The Communication Cannel

All information systems need a medium to satisfy the accumulation of data from one point to other. For instance, Ethernet networks may drive twisted-pair or coaxial cable. By its nature, wireless networks use air as the medium. At the earth's surface, where most wireless networks operate, pure air contains various kinds of gases, such as nitrogen and oxygen. That provides an effective medium for the propagation of radio waves and infrared light.

However, air also has some factors such as water molecules that can cause significant *attenuation* to the propagation of modulated wireless signals. Additionally rain, snow and fog can raise the amount of water molecules by providing the more attenuation. Smog also clutters the air, adding attenuation to the communications channel as well. Attenuation can be defined as the decrease in the amplitude of the signal, and so it limits the operating range of the system. There are of course some ways to overcome the attenuation such as increase the transmit power of the wireless devices (but this solution is generally is limited by the FCC for most cases), or incorporate special amplifiers called *repeaters* that receive attenuated signals, revamp them, and transmit downline to the end station or next repeater.

1.3.2 Logical Architecture of a Wireless Network

The term 'logical architecture' means the network's protocols, which guarantees a well-managed and efficient communication between nodes. All the devices that constitute a network must obey the strict rules to perform proper and faultless coordination and transfer of information.

The most popular logical architecture standard is the seven-layer Open System Interconnection (OSI) Reference Model, which is developed by the International Standards Organization (ISO). OSI defines a complete set of network functions by specifying a layered system. Figure 1.6 illustrates the OSI Reference Model.

These layers have functions as:

• Layer 7—*Application Layer:* Establishes communications with other users and provides such services as file transfer and email to the end users of the network.

• Layer 6—*Presentation Layer:* Negotiates data transfer syntax for the Application Layer and performs translations between different data types, if necessary.

• Layer 5—*Session Layer:* Establishes, manages, and terminates sessions between applications.

• Layer 4—*Transport Layer:* Provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, while shielding the higher layers from the network implementation details. Such protocols as TCP operate at this layer.

• Layer 3—*Network Layer:* Provides the routing of packets though routers from source to destination. Such protocols as IP operate at this layer.

• Layer 2—*Data Link Layer:* Ensures synchronization and error control between two entities.

• Layer 1—*Physical Layer:* Provides the transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications.

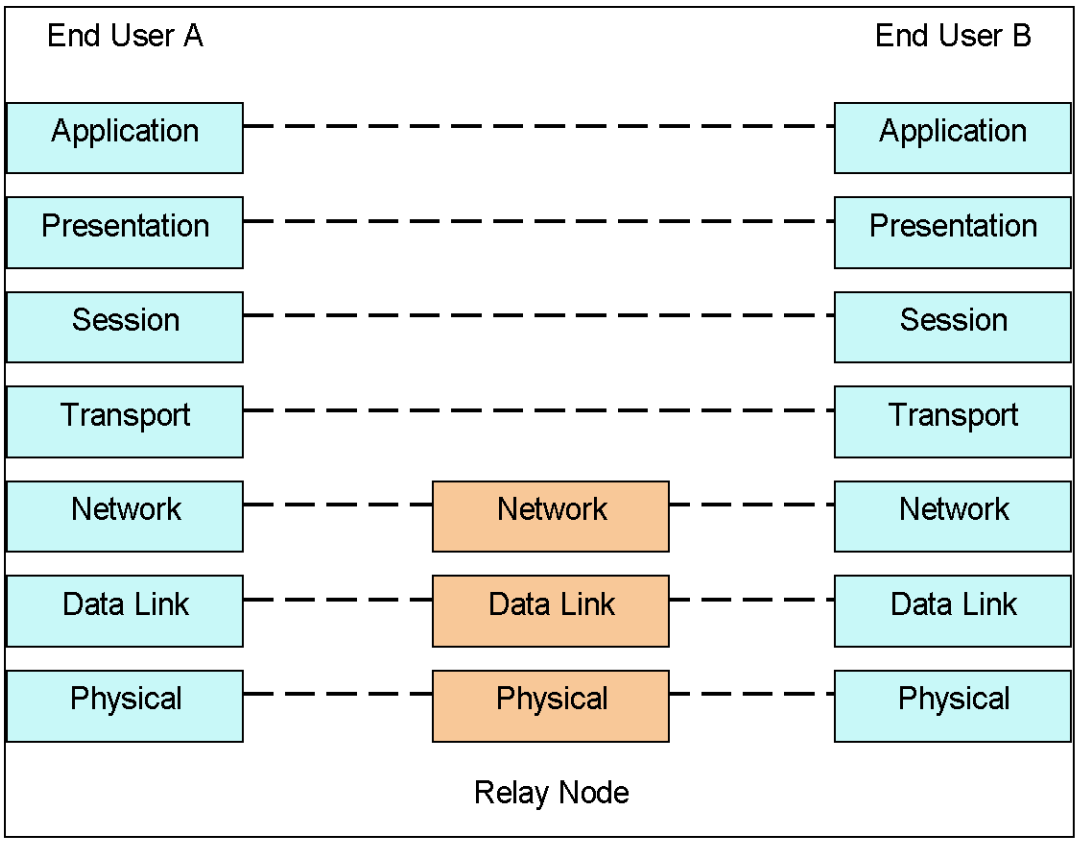

FIGURE 1.6 OSI Reference Model levels [Geiger 1999]

Wireless networks do not exactly functions these layers; except from wireless WANs they operate only within the bottom two layers. Wireless wide area networks also perform Network Layer functions as shown in figure 1.7. In addition to these wireless network properties, complete network architecture needs to include such functions as end-to-end connection establishment and application services to make it useful.

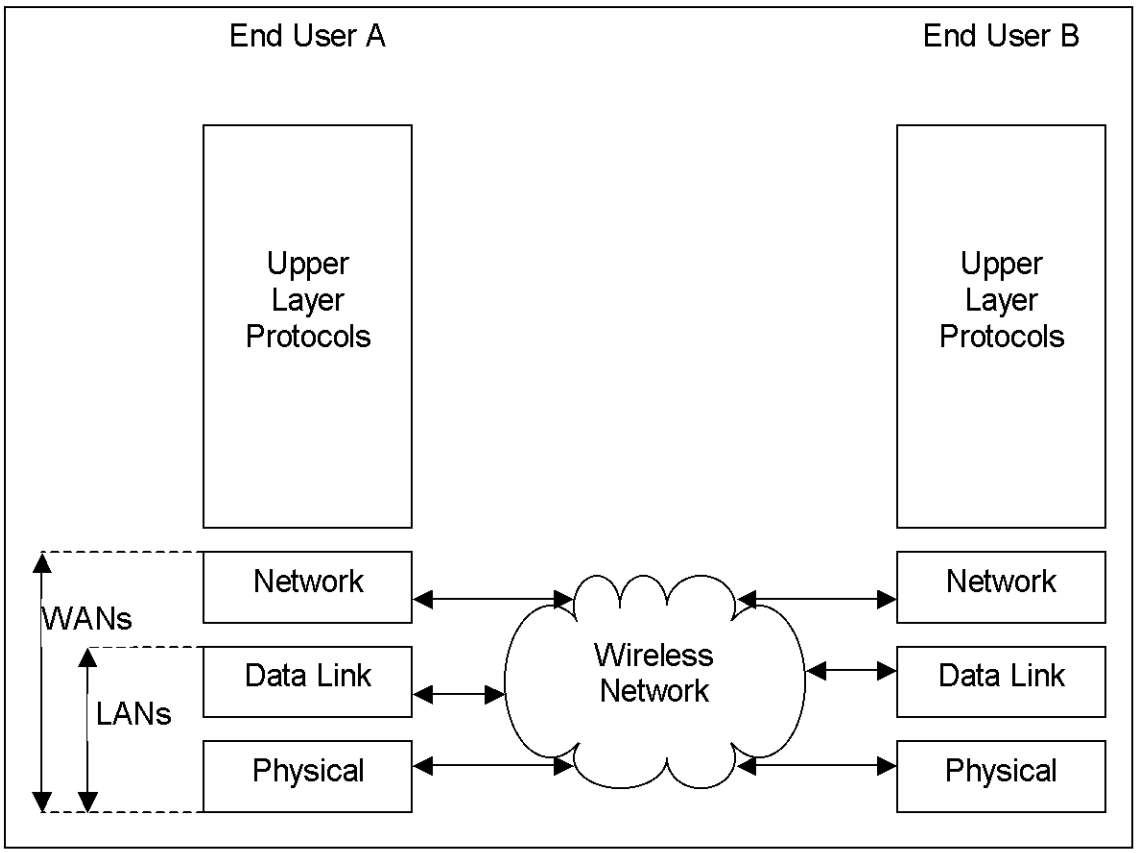

FIGURE 1.7 Wireless LANs, MANs and WANs network layers [Geiger 1999]

1.4 Wireless Network Concerns

The benefits of wireless networks are really accepted by the companies and organizations [12]. However, authorized network people such as engineers and managers should consider the basic concerns of the wireless networking while doing implementations

1.4.1 Multipath Propagation

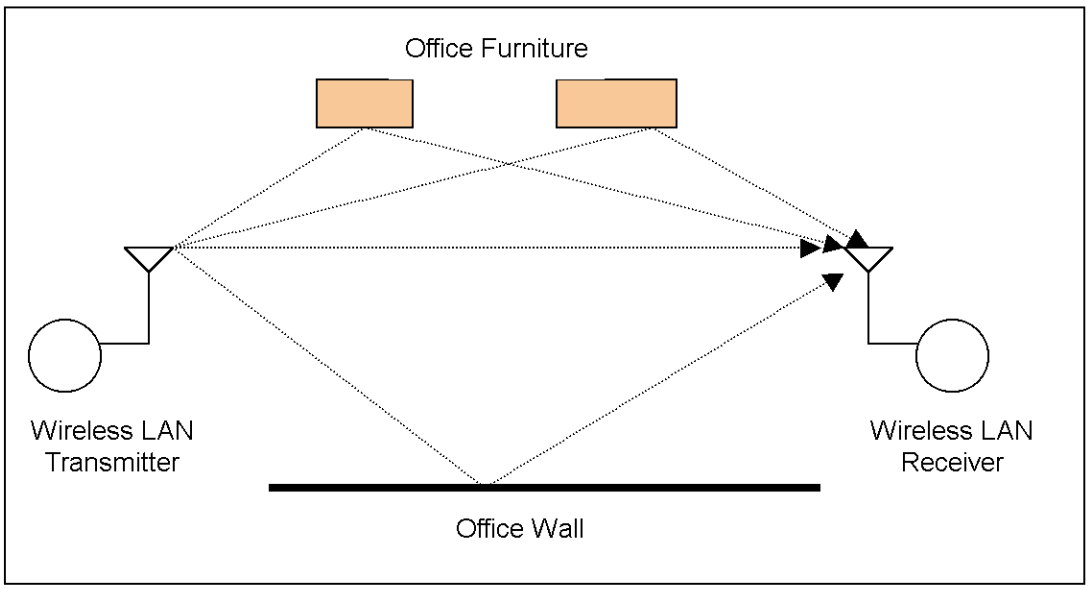

FIGURE 1.8 Multipath Propagation [Geiger 2001]

As it can be seen from figure 1.8 that, transmitted signals can mix up with reflected ones so as to corrupt the signal detected by the receiver. This is known as *multipath propagation*. *Delay spread* is the amount delay experienced by the reflected signals compared to the primary signal. As delay spread increases, the signal at the receiver becomes more distorted and possibly undetectable even when the transmitter and receiver are within close range.

Especially with indoor applications, multipath propagation can be a significant problem. Office furniture, walls, and machinery are the elements that can cause redirected parts of transmitted signal. Wireless LAN manufacturers use some special processing techniques to overcome the effects of multipath propagation. For instance, equalization and antenna diversity are methods for reducing the number of problems arising from multipath propagation.

In a multipath environment the received signal consists of the line of sight (LOS) component together with a number of other components which are going through at least one order of reflection or diffraction, before arriving at the receiver. The reason why multipath makes wireless communication hard is because it is related with the following phenomena:

1.4.1.1 Fading

Fading occurs in a multipath environment when the received signals cancel each other out [26]. Rapid fluctuations caused by local multipath are known as fast fading or Rayleigh fading, whereas long-term variations are known as slow-fading. Short-term and long-term power variations are shown in figure 1.9:

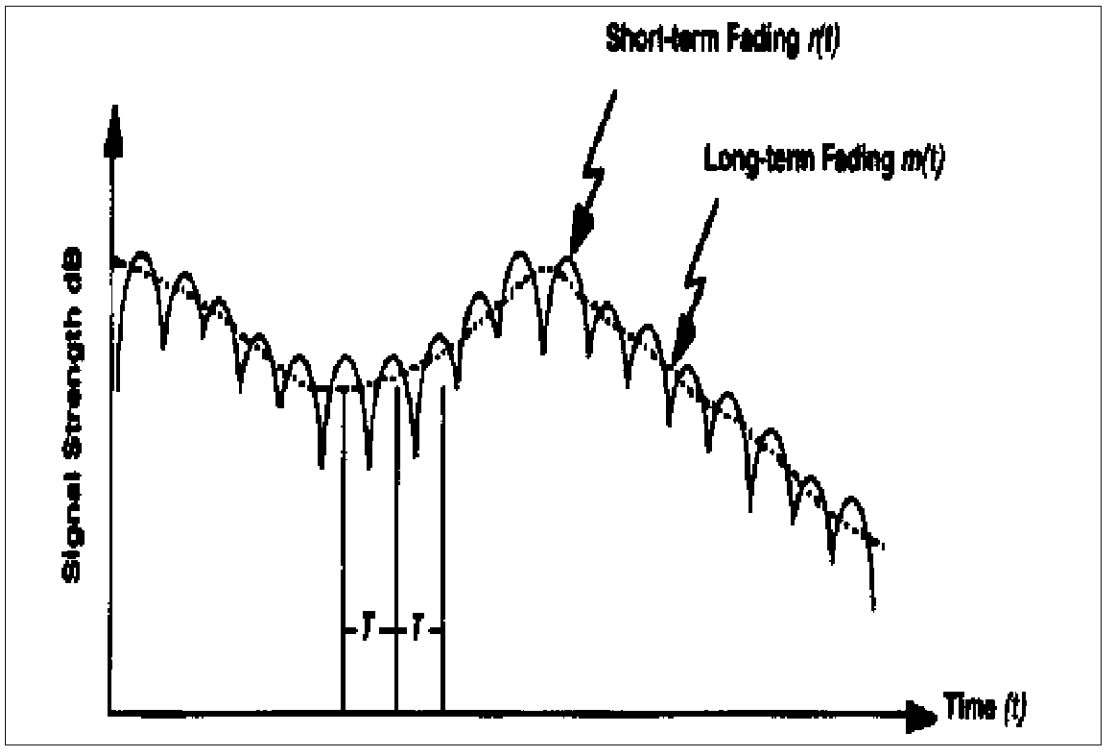

FIGURE 1.9 Short and Long-term power variations [Kounavis]

The mobile radio signal consists of a short-term fast fading signal superimposed on a local mean value, which remains constant over a small area but varies slowly as the receiver moves. Error loss, in digital data transmission, is related to the rate of level crossings and the depth and duration of fades.

1.4.1.2 Delay spread

This phenomenon, which is also called time dispersion, occurs when signals along different paths arrive at different times. Depending on the number of reflections and the propagation speed in different signals, all these signals don't

arrive exactly at the same time at the receiver [36]. It's like the "echo" that may heard in the mountains, the signal going directly will be faster than one reflecting twice on the walls.

As radio propagates at the speed of light, those differences are very small (below the microsecond). But, when the bitrate of the system increases, those time differences becomes significant with regards to the symbol time, to the point of creating destructive interferences (the current symbol will be corrupted by the echo of the previous symbols).

Bit rate lower than 1 Mb/s are relatively immune to delay spread problems (the symbol time is 1 μs and higher), but as the bit rate increase above 1 Mb/s the effect of delay spread increases. It is considered that systems faster than 5 M/s should have some technique to overcome delay spread.

The best measure of delay spread is the root mean square (rms) delay spread, which is the second central moment of the channel impulse response.

1.4.1.3 Doppler shift

Doppler shift is caused by the relative motion of the transmitter, receiver, or any object that reflects/refracts signal [26]. Relative movement causes shift in the carrier transmit frequency, so that random frequency modulation is introduced at the receiver. For example, a person walking at 3 miles per hour causes a maximum doppler shift of +/- 4 Hz for a carier frequency of 910 MHz. Doppler frequency shift is either positive or negative depending on whether the transmitter is moving towards or away from the receiver.

In a multipath environment the velocity of movement in each arriving path is different from that of another path. So, each single transmitted frequency is being received as a spectrum, which is referred to as Doppler Spectrum. Doppler spread in the frequency domain is closely related to the rate of fluctuations in the observed signal.

1.4.2 Path Loss

Another key feature when designing a wireless medium is path loss between the transmitter and receiver. Expected levels of path loss give some meaningful information to determine the necessary requirements for transmit power levels, receiver sensitivity, and signal-to-noise ratio (SNR). Actual path loss depends on the transmit frequency, and it grows exponentially as the distance increases between the transmitter and receiver. With typical indoor applications, the path loss increases approximately 20 dB every 100 feet.

1.4.3 OFDM

Orthogonal Frequency Division Multiplex (OFDM) is a new technique to combat delay spread in high-speed systems.

Using equalisation is a post-processing technique, which tries to overcome delay spread by brute force [36]. OFDM is a pre-processing technique, where the signal transmitted on the band is prepared in such a way that the impact of delay spread is reduced.

Delay spread is damaging because the symbol time is very short, so OFDM will only use large symbol time. However, by increasing the symbol time the bit-rate reduces. To overcome this constraint, OFDM transmit the symbols no longer serially but in parallel. This way, very high bit rate with large symbol time is handled.

OFDM use a set of subcarrier frequencies, the frequencies being orthogonal. Each subcarrier is modulated individually, the bit rate and signal strength of each subcarrier can be adapted to get maximum performance of the system. Then, the system splits the bits to transmit between the subcarriers, each subcarrier is modulated and then combined to produce the transmitted signal (using a Fast Fourrier Transform).

The main drawback of OFDM is that it requires greater frequency accuracy. As the OFDM signal contains many subcarrier very close to each other in frequency, the system must be very accurate to match all of them.

1.4.4 Radio Signal Interference

As the radio and laser signals travel in the air to establish the communication of the systems, they are open to get damage by atmospheric noise and the transmissions from other foreign systems. Moreover, wireless networks can interfere with other nearby wireless networks and radio wave equipment. As it can be seen from figure 1.10, interference can be on an inward or an outward direction.

1.4.4.1 Inward Interference

The harmonics of transmitting systems or some other devices that operating at the same frequency values of LANs can cause an inward interference on the wireless network. For example, microwave ovens operate in the S band (2.4 GHz) that lot of wireless LANs use to transmit and receive. That signals may cause some delays for users while they are working or may damage the bit sequences of data at the transmission. So that the wireless network coverage area may be limited by these types of interference.

Products using the public radio frequencies integrate spread spectrum modulation that limits the amount of harm an interfering signal causes. Narrowband interference with signal-to-interference ratios of less than 10 dB does not usually affect a spread spectrum transmission. Wideband interference, however, can have damaging effects on any type of radio transmission. The primary source of wideband interference is domestic microwave ovens that transmit at 2450 MHz, possibly corrupting the wireless data signal if within 50 feet of the interfering source. Other interference may result from elevator motors, duplicating machines, that protection equipment, and cordless phones.

1.4.4.2 Outward Interference

This type of interference is the other face of the interference problem and happens when a wireless network's signal disturbs other systems, such as adjacent wireless LANs and navigation devices on aircraft. This disruption results in the loss of some or all of the system's functionality. Because of operating on little power

(such as less than 1 watt) wireless LAN products operating in the public spread spectrum interfere rarely. The transmitting components must be very close and operating in the same band with each other to cause inward or outward interference.

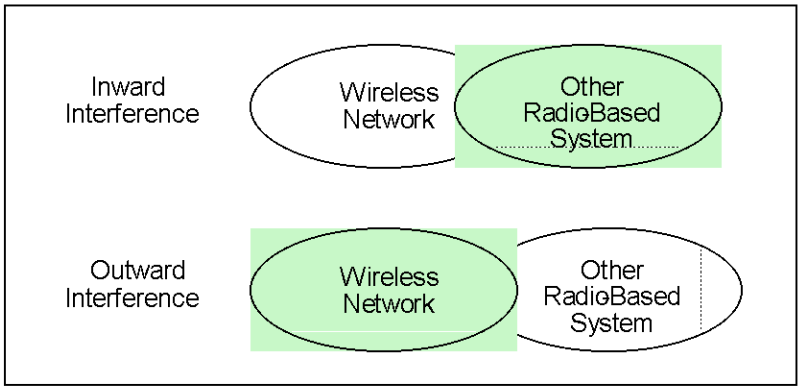

FIGURE 1.10 Wireless networks inward and outward interference [Geiger 1999]

1.4.4.3 Techniques for Reducing Interference

If one exists, the company's frequency-management organization should coordinate the operation of radio-based wireless network products to avoid interference. Government organizations and most hospitals generally have people who manage the use of transmitting devices. This coordination will prevent potential interference problems.

In fact, the coordination with frequency-management officials is a mandatory requirement before operating radio-based wireless devices.

1.4.5 Power Management

It is the natural characteristics of the wireless devices that there is always a dependency on the batteries to operate. It is obvious that plugging the computer into an electrical outlet is very hard or even impossible while using it in a car, performing an inventory in a warehouse, or caring for patients in a hospital. In addition, there are some factors that decrease the battery life before recharging such as usage of network interface cards. The manufacturers implement power management techniques in their products to overcome this problem. Without power management radio-based

wireless devices always keep working to transmit data even if there is not any action about transmission.

Proxim's wireless LAN products, for example, incorporate two modes to help conserve power: the Doze mode and the Sleep mode. The Doze mode keeps the radio off most of the time and wakes it up periodically to determine whether any messages wait in a special mailbox. This mode alone utilizes approximately 50 percent less battery power. The Sleep mode causes the radio to remain in a transmit-only standby mode. In other words, the radio wakes up and sends information if necessary, but is not capable of receiving any information.

1.4.6 System Interoperability

The network managers and engineers use very kind of devices from different manufacturers. These products must speak with each exactly the same language not to cause any problem. So that stability of network system can be kept. At the early stage of the wireless products compatibility was a real problem due to lack of standardization. However, the recently approved 802.11 standard now is solving that problem. As a result, the uniformity among the manufacturers and so the products enable to select the lowest cost that meets the requirements of wireless structure.

1.4.7 Network Security

Network security means the protection of information and resources from loss, corruption, and improper use. Being a secure media for wireless networks is a common and very important question among businesses considering the implementation of a wireless system.

A wireless network provides a bit pipe, consisting of a medium, synchronization, and error control that supports the flow of data bits from one point to another. The functionality of wireless network corresponds to the lowest levels of the network architecture and does not include other functions, such as end-to-end connection establishment or logon services that higher layers satisfy. Therefore, the only security issues relevant to wireless networks include those dealing with these lower architectural layers, such as data encryption.

1.4.7.1 Security Threats

The main security aspect of wireless networks is that they may propagate data over the network boundaries that out of control. Especially radio waves easily go through the walls of organizations buildings and then they may be kept by someone who has the same wireless network interface card (NIC). These propagating data may involve organizations private information. If the intruder also has the access codes of the network system by somehow he/she may deceive the network security personnel without being noticed.

Another problem with the security of the wireless network is the potential electronic sabotage. Someone maliciously blocks the data transmission of the network and makes the network unavailable to users. This may be done by using the carrier sense protocol properties of transmitting medium. In this protocol, if one station is transmitting, all others must wait to share the medium as common use. The intruder can easily stop the network traffic by using a wireless product of the same manufacture and setting up a station to continually resend packets. These transmissions block all stations in that area from transmitting, so as making the network inoperable. In such cases, the company stands to incur a loss.

1.4.7.2 Security Safeguards

Wireless network device manufacturers solve most security problems by restricting access to the data. Those products require establishing a network access code and setting that code within each workstation throughout the network. A wireless station cannot process the data if its access code is not set to that of network. It becomes much more difficult for someone to receive and process the data by keeping the code secret.

Some vendors also offer encryption as another solution. One option is the Data Encryption Standard (DES) as defined by the U.S. Department of Commerce. The other implements a proprietary method called Advanced Encryption Scheme (AES).

As shown in figure 1.11, the DES and AES algorithms both use a 16-hexadecimal digit key for encryption process. The key is loaded into the security chip when the adapter is configured at the installation. When a message is received

or sent, the security chip uses the key to encrypt or decrypt the message. Only those workstations in the network with the same security chip and key will be able to understand the messages. Other users of wireless LAN who do not have the key will be unable to decrypt any messages. Both DES and AES perform the encryption in one continuous stream of bits that pass through the system's modulator without affecting performance.

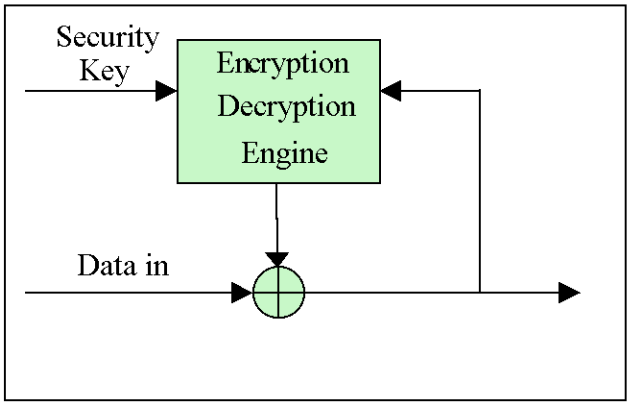

FIGURE 1.11 A data encryption process [Geiger 1999]

The Department of Commerce limits export of DES devices outside the United States. The purpose of the AES is to provide an alternative for DES to those users needing a secure air interface, but who are not allowed to use DES due to export limitations. AES implements an algorithm that has been approved for export.

1.4.8 Connection Problems

There may occur problems while using traditional wired-based protocols with wireless networks such as maintaining connections between the user's devices and the applications working on a server. TCP/IP, for example, is susceptible losing connections over wireless networks, especially when the user's device is operating in an area with marginal wireless network coverage although it provides very reliable connections over wired networks, such as Ethernet and token ring.

The mobile nature of wireless networks can offer addressing problems, additionally. Most networks need an IP address loaded in the user's appliance to be within a specific address range to maintain proper connections with applications.

When a user roams with a wireless appliance from one IP subnet to another, the appliance and the application may lose the capability to connect with each other.

1.4.9 Installation Issues

Generally, planning and installing the cabling issues of wired networks are mostly straightforward jobs. The survey of the site for deciding the cabling paths may be done easily. After the design is complete, installers can run the cables, and the cable plant will most likely support the transmission of data as planned.

A radio-based wireless LAN installation is not as predictable. Is is difficult to design the wireless system by just inspecting the facility. Prediction the way in which the contour of the building will affect the propagation of radio waves is difficult. Omnidirectional antennas propagate radio waves in all directions if there is no barrier or problem on the way of the waves. Walls, ceilings, and other obstacles attenuate the signals more in one direction than the other, and even cause some waves to change their paths of transmission. The simple example as the opening of a bathroom door can change the propagation pattern. These events cause the actual radiation pattern to distort, something like a stretched appearance, as shown in figure 1.12.

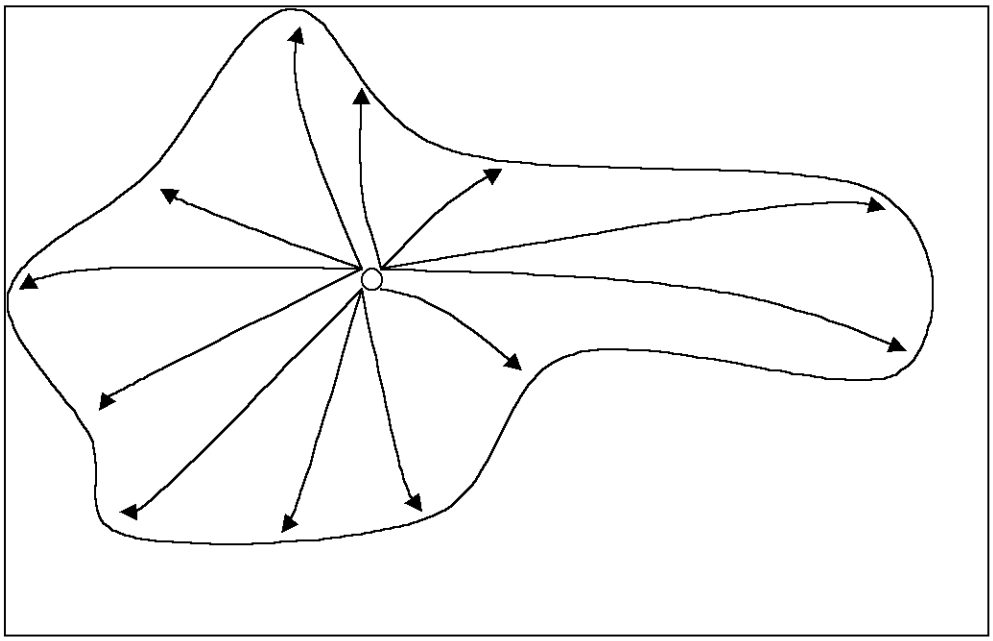

FIGURE 1.12 Unpredictable an irregular radiation pattern of an omnidirectional antenna [Geiger 1999]

There are also some difficulties for planning wireless MANs. Even though, there is a clear line-of-sight path between two buildings separated by 1,500 feet, there might be other radio transmitting devices that clutters the path.

To avoid installation problems, an organization should perform propagation tests to assess the coverage of the network. Not performing the tests may leave some of the users outside of the propagation area of wireless servers and access points. Propagation tests give the information necessary to plan wired connections between access points, allowing coverage over applicable areas.

1.4.10 Health Risks

Another common concern with wireless networks is whether they carry any form of health risk. So far, there has been no conclusive answer. Radio-based networks, however, appear to be as just safe as or safer than cellular phones. There is little or no risk in using cellular phones, which operate in frequency bands immediately below wireless networks. Wireless network components should be even safer than cellular phones because they operate at lower power levels, typically between 50 and 100 milliwatts, compared to the 600 milliwatts to 3 watt range of cellular phones. In addition, wireless network components usually transmit for shorter periods of time.

Laser-based products, found in both wireless LANs and MANs, offer very little or no health risks. In the United States, the Center for Devices and Radiological Health (CDRH), a department of the U.S. Food and Drug Administration, evaluates and certifies laser products for public use. The CDRH categorizes lasers into four classes, depending upon the amount of harm they can cause to human.

Supermarket scanners and most diffused infrared wireless LANs satisfy Class I requirements, where there is no hazard under any circumstances. Class IV specifies devices, such laser-scalpels, which can cause serious danger if the operator handles them improperly. Most long-range, laser-based wireless networks are rated as Class III devices, whereby someone could damage his eyes if looking directly at the laser beam. Therefore, care should be taken when orienting lasers between buildings.

1.5 The Benefits Of Wireless Networking

Some basic factors, such as the need to lower the costs associated with network infrastructure and to support mobile networking applications that offer gains in process efficiency, accuracy, and lower business costs are mainly the driving forces of the emergence and continual growth of wireless networks [12].

1.5.1 Mobility

Mobility makes users free to physically move while using a device, such as a handheld PC or data collector. Many workers, such as inventory clerks, healthcare workers, police officers, and emergency-care specialists, need to be mobile while they are on work. Of course, wireline networks require a physical connection between the user's workstation and the network's resources, which makes access to these resources impossible while moving inside the building or elsewhere.

Mobile applications requiring wireless networking include those that depend on real-time access to data- usually stored in centralized databases (figure 1.13). If the application requires mobile users to be immediately aware of changes made to data, or if information put into the system must immediately be available to others, there is a definite need for wireless networking. For accurate and efficient price markdowns, for example, many retail stores use wireless networks to interconnect handheld bar code scanners and printers to databases having current price information. This enables the printing of correct price on the items, making both the customer and the business owner more satisfied.

Naturally there is no need to use wireless networking for all mobile applications. Sometimes the business case doesn't support the need for mobile real-time access to information. If the application's data can be stored on the user's device, and changes to the data are not significant, the additional cost of wireless network hardware may not provide enough benefits to justify the additional expense.

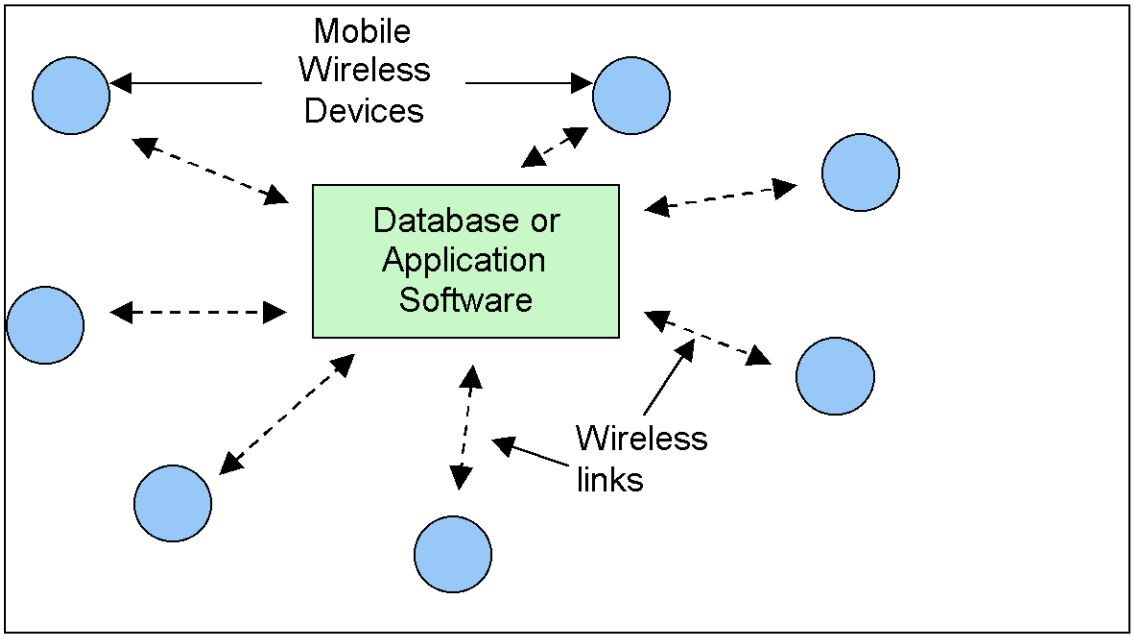

FIGURE 1.13 Support of wireless network to access real-time data [Geiger 1999]

1.5.2 Cost Savings

Because of the lack of a physical connection between the users device and a server, wireless networks offer benefits that reduce networking costs. In the next sections the cost issue is also explained by various aspects.

1.5.3 Installation In Difficult-To-Wire Areas

There may be such places that, there is a great difficulty for installing wired networks and so the application of wireless networks makes certain cost savings. If rivers, freeways or other obstacles separate buildings that must be connected, a wireless solution may be more economical than installing physical cable or leasing communication circuits, such as T1 service or 56 Kbps lines. Some organizations spend thousands or even millions of dollars to install physical links among their nearby facilities.

The deployment of wireless networking in these situations costs thousands of dollars, but will result in a definite cost savings in the long term.

The asbestos found in older facilities is another problem that many organizations come across. The breathing of asbestos particles is extremely hazardous to health; a great care must be taken when installing network cabling within such kind of areas. Although by taking the necessary precautions, the cable installations in these places can be prohibitive because of unwanted results.

In some cases, it might be impossible to install cabling, due to strict rules. Some municipalities, for example, may have restrictions for permanently modifying older facilities because of their historical values. This could limit the drilling of holes in walls during the installation of network cabling and outlets. Right-of-way restrictions within cities and countries may also prevent the digging of holes in the ground to lay optical fiber for the connection of network sites. In both situations a wireless network might be the only solution.

1.5.4 Increased Reliability

Cable faults are one of the natural problems of wired networks that cause the system to be down. As a matter fact, cable faults are said to be the primary cause of system downtime. Those faults can be occurred from eroding moisture metallic conductors by water intrusions during storms and spillage or leakage of liquids by accidentally. With wired networks, users carelessness may break their network connector when trying to disconnect their PCs from the network to move them to different locations. Badly prepared cable connections can cause signal reflections that result in unexplainable errors. Moreover, the accidental cuttings of cables can bring a network down immediately. Wires and connectors can easily break through misuse and even normal use. These problems also mix with the user' ability to utilize network resources, causing another difficulties for network managers. An advantage of wireless networking, results from the use of less cable. This makes considerable decrease in the downtime problems of the network and as a result of the cost savings associated with replacing cables.

1.5.5 Reduced Installation Time

The installation of cabling is an activity that usually causes loosing of time. For instance, to construct a LAN system, installers must pull twisted-pair wires above the ceiling and drop cables through walls to network outlets that they must fasten to the wall. These tasks can take days or weeks, depending on the size of the installation. The installation of optical fiber between buildings within same geographical area consists of digging trenches to lay the fiber or pulling the fiber through an existing channel. Weeks or possibly months might be needed to get necessary approvals and dig through ground and asphalt.

The decision of using wireless networks greatly reduces the time needed for cable installation, making the network available for use much sooner. Therefore, many organizations or countries that not having a network infrastructure have decided to use wireless networking as a method of providing connectivity among computers without the expense and time associated with installing physical media.

1.5.6 Long-Term Cost Savings

Sometimes companies decide to reorganize. This results with the movement of people, new floor plans, office partitions, and other necessary replacements. These changes generally require recabling the network, and in some cases, the recabling costs of organizational changes are substantial, especially with large structured networks. A reorganization rate of 15 percent each year can result in yearly reconfiguration expenses as high as $250,000 for networks that have 6,000 interconnected devices [12]. The advantage of wireless networking is again based on the having less amount of cables. The network connection can be moved by just relocating the employee's computer or other device.

Chapter 2

WIRELESS NETWORK CONFIGURATIONS

2.1 Wireless LANs

The majority of the wireless LANs operate over the unlicensed frequencies at almost Ethernet speeds (as 10 Mbps) using carrier sense protocols to share a radio wave or infrared light medium. Most of these devices have the ability of transmitting information up to 1,000 feet between computers within an open environment [13]. Additionally, these devices also perform their functions over Simple Network Management Protocol (SNMP) to achieve network management issues with SNMP-based platforms and applications. The wireless LAN mainly consists of two components to interface with a wired network. A wireless NIC interfaces the end-user appliance with the wireless network, and a wireless local bridge, which is often named as *access point*, interfaces the wireless network with a wired network. Most wireless NICs interface appliances to the wireless network by implementing a carrier sense access protocol and modulating the data signal with a spreading sequence.

Figure 2.1 illustrates the concept of wireless local area network interfacing with a wired network.

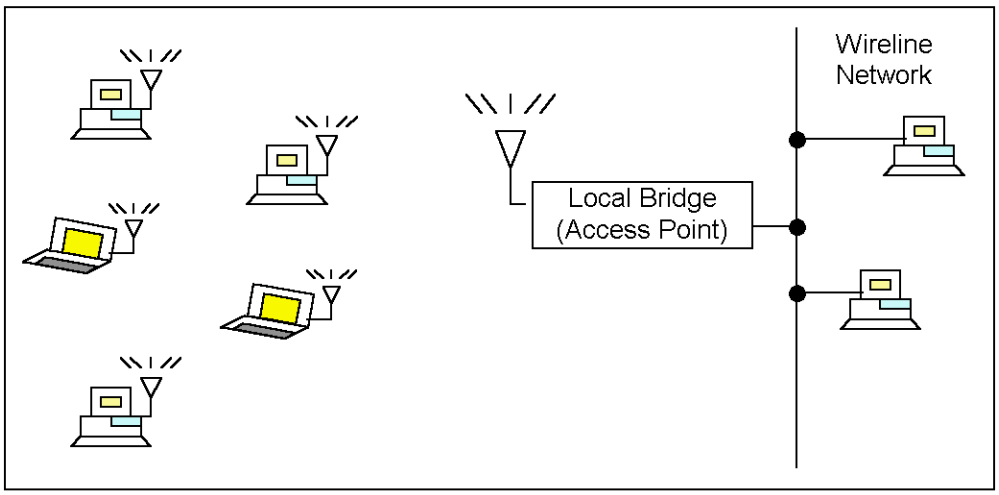

FIGURE 2.1 A wireless local area network with a wired one [Geiger 1999]

Wireless networks perform functions similar to their wired Ethernet and token-ring counterparts. In general, networks perform the following functions to enable the transfer of information from source to destination.

1. The medium provides a bit pipe (a path for data to flow) for the transmission of data.

2. Medium access techniques facilitate the sharing of a common medium

3. Synchronization and error control mechanisms ensure that each link transfers the data intact.

4. Routing mechanisms move the data from the originating source to the intended destination.

5. Connectivity software interfaces an appliance, such as a pen-based computer or barcode scanner, to application software hosted on a server.

Figure 2.2 illustrates the logical architecture of a wireless LAN. A wireless local area network provides functions to the Medium Access Control (MAC) and Physical layers of a network's architecture.

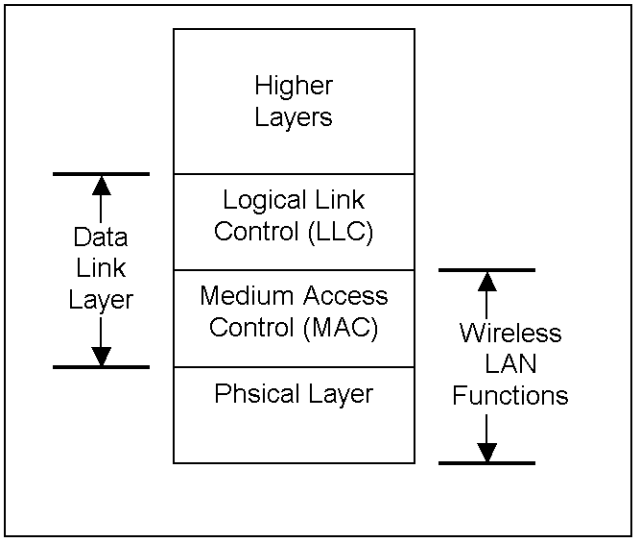

FIGURE 2.2 Logical architecture of a wireless LAN [Geiger 2001]

There are mainly three approaches to wireless networking within a local environment:

- Radio waves
- Infrared light
- Carrier currents

2.1.1 Radio-Based Wireless LANs

A variety of wireless LAN products sold at the market use radio waves to perform data transfer. The main advantage of radio waves with respect to the others is that they can provide interconnections between users without line of sight and propagate through walls and other obstructions with fairly little attenuation, depending on the type of wall construction. Although several walls might separate the user from the server or wireless bridge, users may still have the connections to the network. This gives the users true mobility. With radio-LAN products, a user with a portable computer can move freely through the facility while accessing data from a server or running an application.

A disadvantage of using radio waves is that an organization must survey the facility to determine the other electromagnetic propagation before installing a radio-based LAN. For example, medical equipment and industrial components may utilize the same radio frequencies as wireless LANs, which could cause possible interference. Because of its nature, radio waves can easily pass through the facility borders that result with undesired security problems. Unauthorized people of outside may retrieve the important and secure data of the organization. To overcome this issue, generally, manufacturers scramble the data so that the stolen information is not meaningful to intruder.

2.1.1.1 Medium Access Control

Medium access control, which is a Data Link Layer function in a radio-based wireless LAN, enables multiple appliances to share a common transmission medium over a carrier sense protocol similar to Ethernet. This protocol satisfies the needs of a group of wireless computers with sharing the same frequency and space.

Because of using same space to communicate, each element of a network mustn't send data over the medium while other one sending some data so as to avoid collisions and losing of information.

This simple protocol guarantees that only one node sending at a time, offering a shared use of the communications medium. Wireless systems operate in a similar fashion, except the communications are by way of radio signals. Figure 2.3 illustrates

the generic carrier sense protocol, commonly known as *Carrier Sense Multiple Access with Collection Detection* (CSMA/CD).

Wireless networks handle error control by having each station check incoming data for altered bits. If the destination station does not detect errors, it sends an acknowledgment back to the source station. If the station detects errors, the data link protocol ensures that the source station resends the packet.

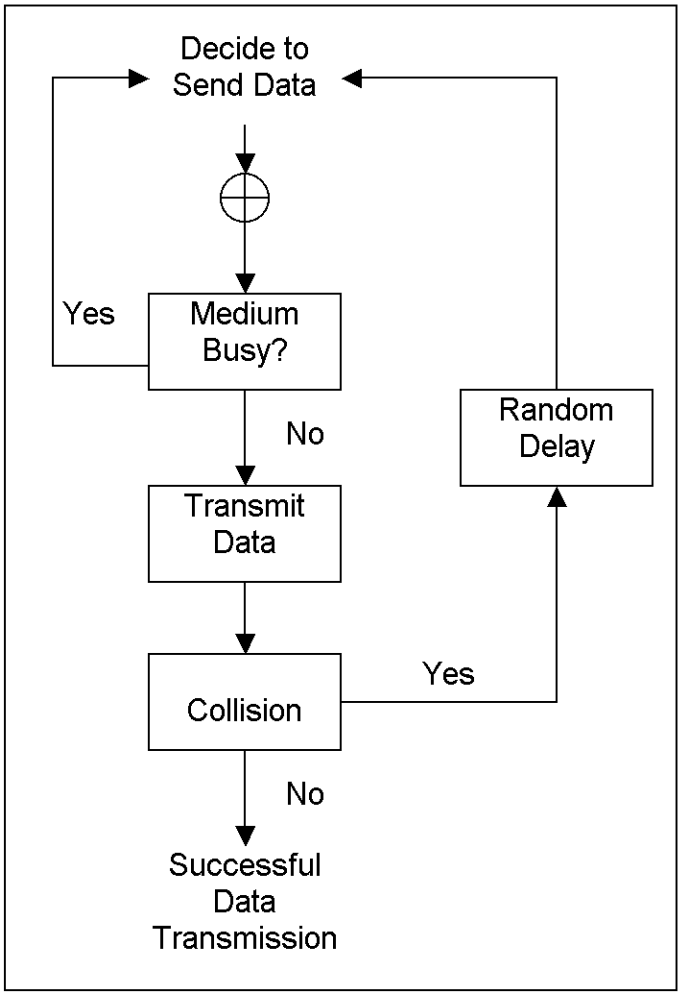

FIGURE 2.3 The operation of carrier sense protocol [Geiger 1999]

2.1.1.2 Spread Spectrum Modulation

As a job of physical layer, modulation prepares the digital signal within the NIC for transmission over the airwaves. *Spread spectrum* "spreads" a signal's power over a wider band of frequencies (indicated on figure 2.4), sacrificing bandwidth to

gain signal-to-noise performance (referred to as *process gain).* This situation makes a phenomenon with conservation of frequency bandwidth but results with less damage of signal from electrical noise than conventional radio modulation techniques. Other transmission and electrical noise, typically narrow in bandwidth, will only interfere with a small portion of the spread spectrum signal, resulting in much less interference and fewer errors when the receiver demodulates the signal.

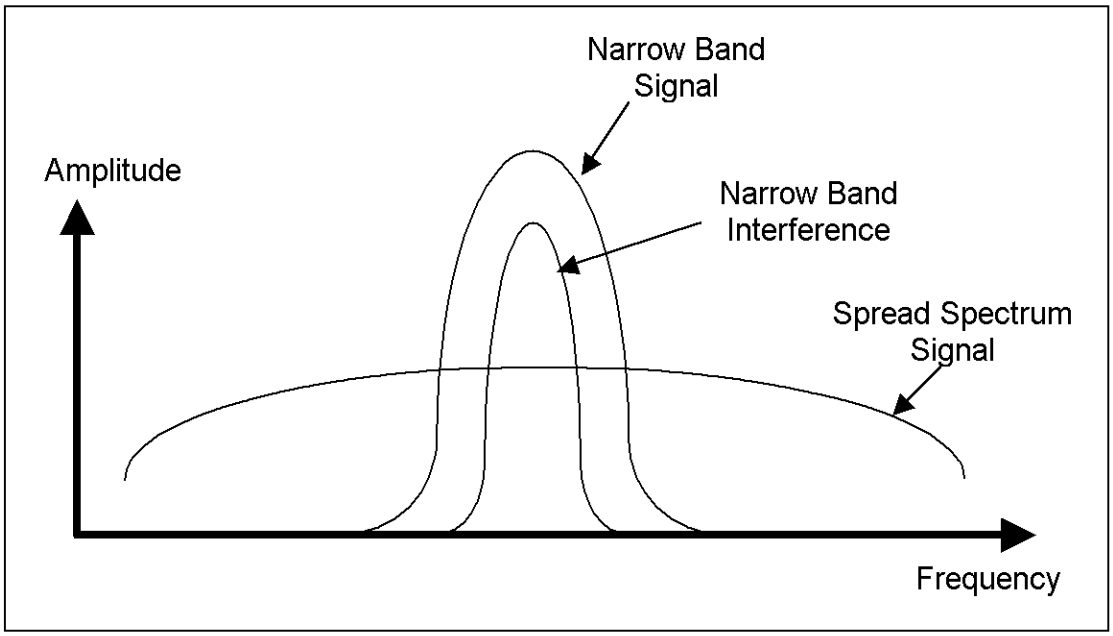

FIGURE 2.4 Interference comparisons of spread spectrum and narrow band signals [Geiger 1999]

Spread spectrum modulators use one of two methods to spread the signal over a wider area: frequency hopping or direct sequence.

2.1.1.2.1 Frequency Hopping Spread Spectrum

Frequency hopping works very much like its name implies. It takes the data signal and modulates it with a carrier signal that jumps from frequency to frequency as a function of time over a wide band of frequencies as indicated as figure 2.5. A frequency hopping radio, for example, will hop the carrier frequency over the 2.4 GHz frequency band between 2.4 GHz and 2.483 GHz.

The frequency hopping technique reduces interference because an interfering signal from a narrowband system will affect the spread spectrum signal only if both are transmitting at the same frequency at the same time Therefore, the aggregate interference will be very low, resulting in little or no bit errors.

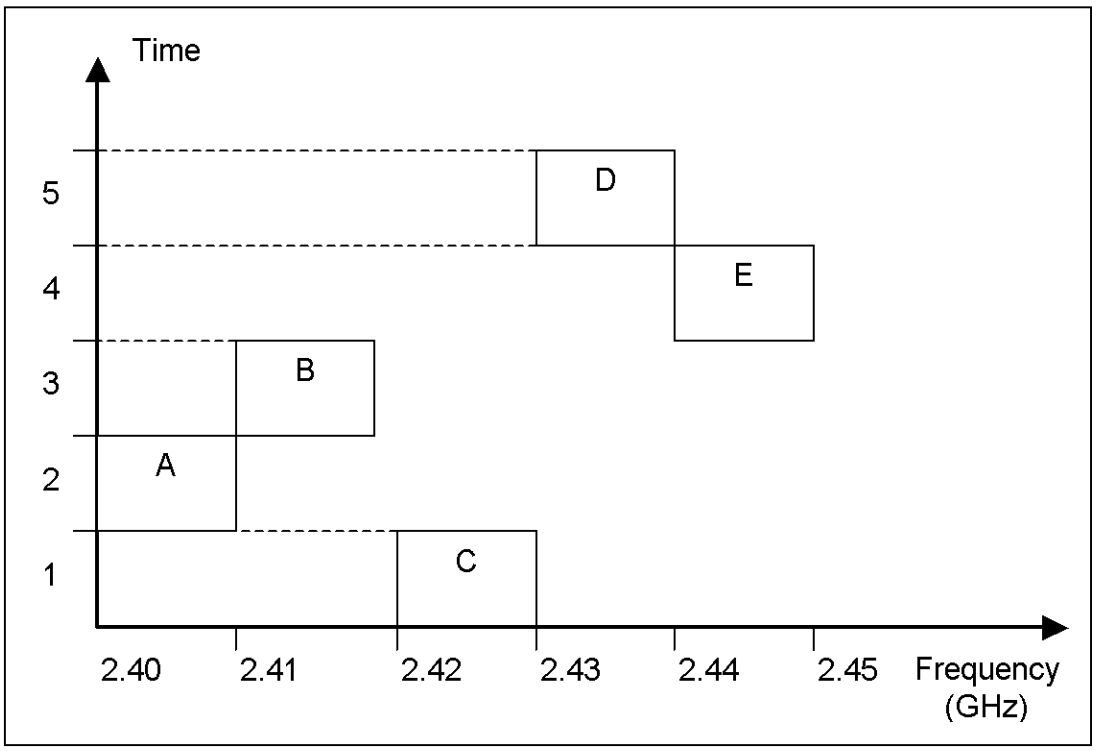

FIGURE 2.5 Frequency hopping mechanism [Geiger 1999]

2.1.1.2.2 Direct Sequence Spread Spectrum

Direct sequence spread spectrum combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a *chipping code* (also known as *processing gain). A* high processing gain increases the signal's resistance to interference. The minimum linear processing gain that the FCC allows is 10, and most commercial products operate under 20. The IEEE 802.11 Working Group has set its minimum processing gain requirements at 11. In comparison to frequency hopping, direct sequence can achieve much higher than 2 Mbps data rates. Figure 2.6 shows an example of the operation of direct sequence spread spectrum.

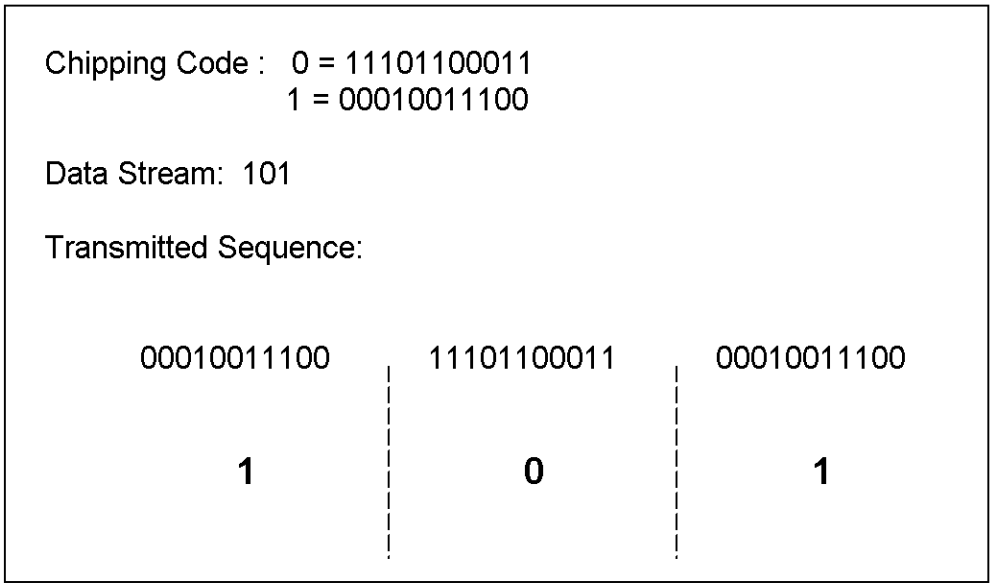

FIGURE 2.6 Specific direct sequence bits example [Geiger 1999]

2.1.1.2.3 ISM Frequency Bands

In 1985, as an attempt to stimulate the production and use of wireless network products, the FCC modified Part 15 of the radio spectrum regulation, which governs unlicensed devices. The modification authorized wireless network products to operate in the *Industrial, Scientific, and Medical (ISM) bands*. The ISM frequency bands offer greater bandwidth at higher frequencies as shown in figure 2.7.

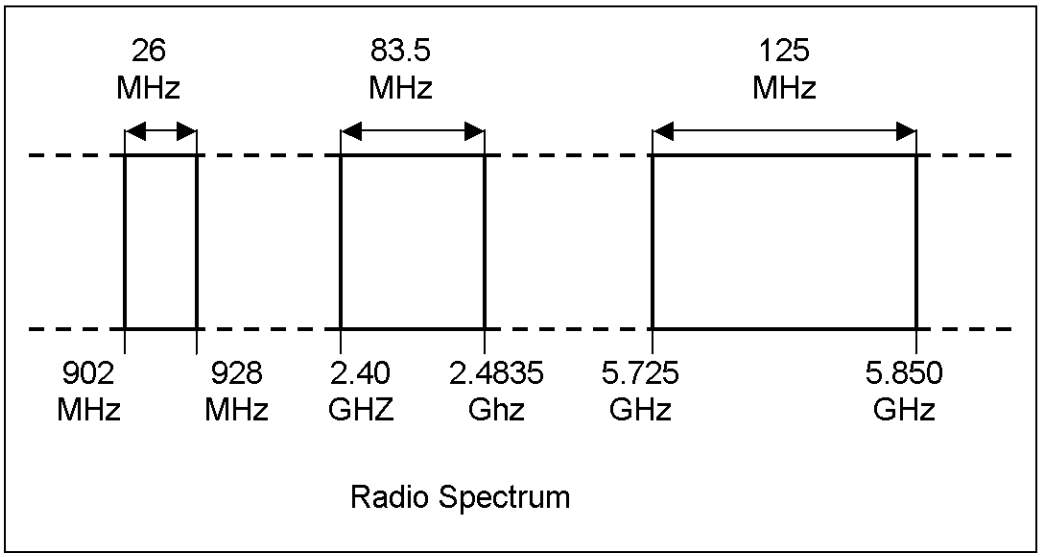

FIGURE 2.7 The ISM frequencies [Geiger 1999]

Table 2.1 depicts the tradeoffs between 902 MHz and 2.4 GHz operating frequencies, indicating that 2.4 GHz is the better choice of operating frequency for wireless LANs.

TABLE 2.1 Tradeoffs between 902 MHz and 2.4 GHz frequencies [Geiger 1999]

902 MHz	**2.4 GHz**
Lower cost	Higher cost
Longer range	Shorter range
Limited bandwidth	Wider bandwidth
Not compliant with the 802.11 standard	Compliant with the 802.11 standard
Available mostly in North America	Available worldwide
Comprises most of the currently installed base in North America	Comprises most new installations within North America and abroad

2.1.1.3 Narrowband Modulation

Basic daily use radio systems, such as television and AM/FM radio, perform narrowband modulation where the system supplies all its transmit power within a close range of frequencies, making efficient use of the radio spectrum in terms of frequency space.

Without performing any kind of control, this modulation technique will cause a great deal of interference because the noise source coming from other systems using the same transmit frequency will corrupt most of the signal. Not to face with such interference, the FCC generally forces users of narrowband systems to obtain FCC licenses to maintain the utilizations. Narrowband products, then, can have a strong advantage because there is a real satisfaction of operating without interference. If interference does occur, the FCC will generally resolve the matter. This makes narrowband modulation good for longer links traversing cities where significant interference may result.

2.1.1.4 Single-Cell (Peer-to-Peer) Wireless LANs

Peer-to-peer wireless LANs only needs wireless NICs in the appliances to form a wireless network as shown in figure 2.8. For example, any time two or more PCMCIA adapters are found within acceptable range of each other, a peer-to-peer network may easily be established. This enables an organization to form an *ad hoc* network for temporary use. Access points are not necessary unless users will need connections to wired network-based resources. For small single-floor offices or stores, a peer-to-peer wireless LAN might enough to provide the communications of devices.

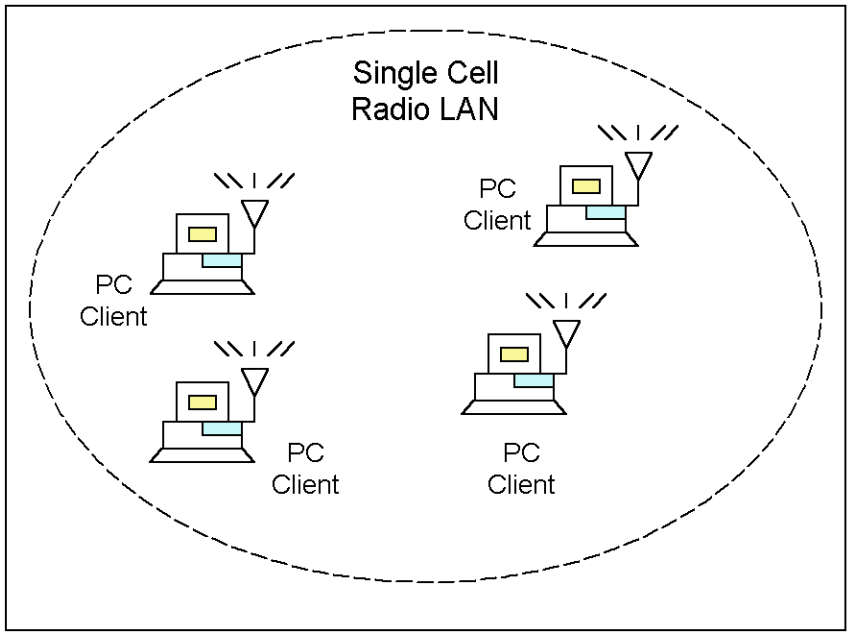

FIGURE 2.8 A single-cell wireless LAN [Geiger 1999]

2.1.1.5 Multiple-Cell Wireless LANs

If there is a need for greater range than the boundaries of a single-cell system, there can be a set of cell systems that uses access points and a wired network backbone to form a multiple-cell configuration as shown in figure 2.9. That kind of system can be established multiple-floor buildings, warehouses, and hospitals etc. In this type of LAN, a handheld PC or data collector with a wireless NIC can stroll in

the facility within the coverage area while keeping a live connection to the underlying network.

Multiple-cell wireless LANs can be configured to satisfy different connectivity requirements. By referring figure 2.9, cells A, B, and C can be adjusted identical, so that all authorized users in the facility have continuous connections. If there are several departments that perform special tasks and so there is a need for security considerations, one cell configuration may be differentiated from others to maintain secrecy. If cell A devices have diverse setup parameters, cell B and C appliances and users cannot reach the necessary information of A and vice versa.

The ideal LAN configuration system is entirely depends on the user requirements and geography. Nevertheless, bridges may be necessary to support user access to resources located on the wired infrastructure.

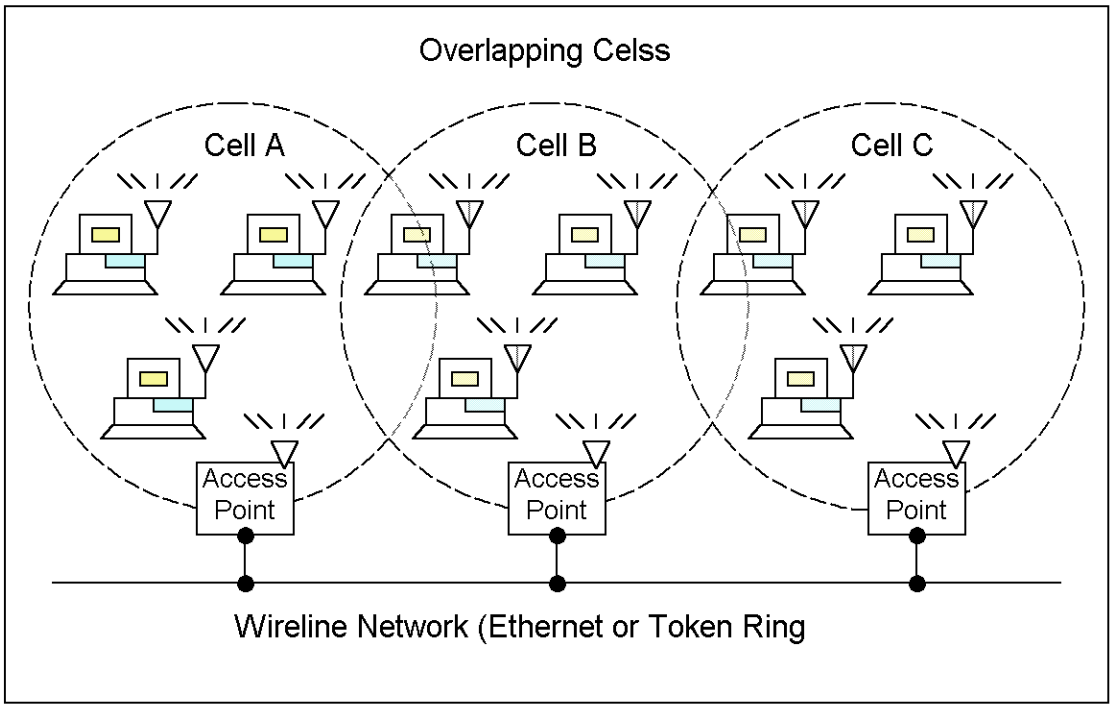

FIGURE 2.9 A multiple-cell wireless LAN [Geiger 1999]

2.1.2 Infrared Light-Based Wireless LANs

The alternative of radio waves for wireless LAN systems is infrared light. The wavelength characteristics of infrared is longer, means lower in frequency, than the spectral colors but much shorter, means higher in frequency than radio waves.

In comparison to radio waves, infrared light offers higher degrees of security and performance. These LANs are more secure than radio waves because infrared light cannot pass through opaque objects, such as walls, so that providing the data signals contained within a room or building. Also, the light signal does not affected from common noise sources such as microwave ovens and radio transmitters so interference with them does not happen. Moreover, in terms of performance, because infrared light has a great deal of bandwidth it can operate at very high data rates. Infrared light, however, is not as suitable as radio waves for mobile applications due to its limited coverage.

An infrared light LAN consists mainly of two components:

• *Adapter card or unit:* The adapter card plugs into the PC or printer via an ISA or PCMCIA slot (or connects to the parallel port).

• *Transducer:* The transducer, similar to the antenna with a radio-based LAN, attaches to a wall or office partition.

The adapter card handles the protocols needed to operate in a shared-medium environment, and the transducer transmits and receives infrared light signals.

There are two types of infrared light LANs:

• Diffused

• Point-to-point

2.1.2.1 Diffused Infrared-Based LAN Technique

When using infrared light in a LAN, the ceiling can be a reflection point as seen figure 2.10. This technique uses carrier sense protocols to share access to the ceiling. For example, there is a room containing four nodes that are using diffused infrared-based LAN technique to communicate. If one node wants to send information, it first looks at the ceiling to notice whether some other is currently transmitting. If a transmission is taking place, the node wanting to send the information waits until the other one stops sending the message. If no one is transmitting, the source node will start to send information. To alert the destination node of an incoming message, the sender transmits the proper sequence of code words that represent the destination node's name (id). All nodes in the room will be constantly surveying the ceiling, waiting for signals containing their addresses. If a

node sees its name, it will pay attention to the rest of the transmission. Through this method, each node can send and receive information.

Diffused infrared light LANs operate at data rates of 1 to 4 Mbps. Due to geometry, diffused infrared light stations are limited in separation distance, typically 30 to 50 feet. The lower the ceiling, the less range between stations. Ceiling heights of 10 feet will limit the range to around 40 feet. To extend the operating range, infrared access points can be used to connect cells together via a wired backbone.

Because they depend on ceilings and walls, diffused infrared LANs will not operate outdoors.

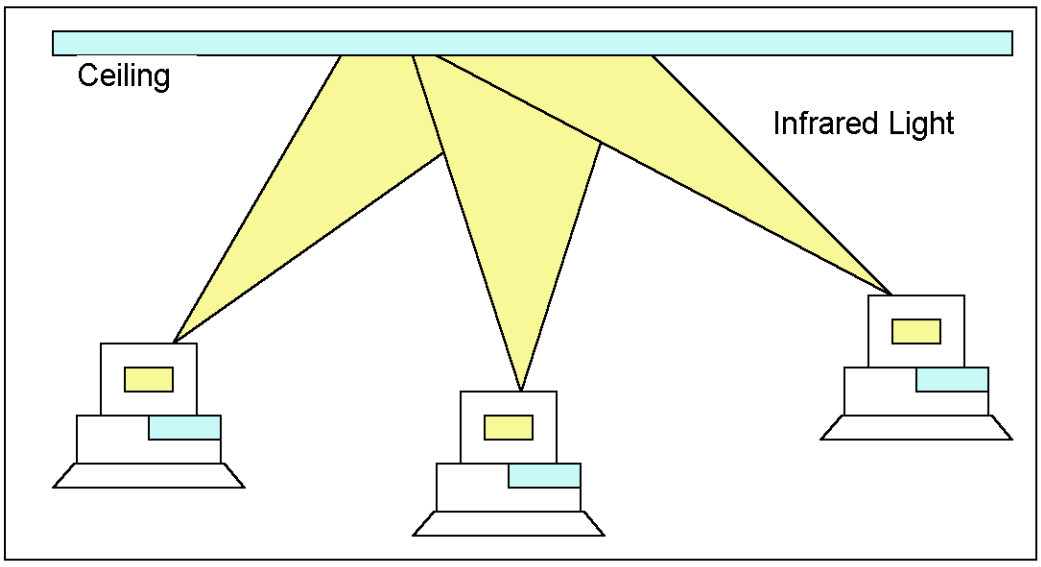

FIGURE 2.10 A diffused infrared-based wireless LAN system [Geiger 1999]

2.1.2.2 Point-to-Point Infrared LAN System

This system just replaces the cable in the token-ring network with infrared light that can reach distances of up to 75 feet. It consists of a pair of transducers, one for transmitting and one for receiving that must be configured, as shown in figure 2.11. The point-to-point infrared LAN system uses a directed light beam to connect token-ring-based computers.

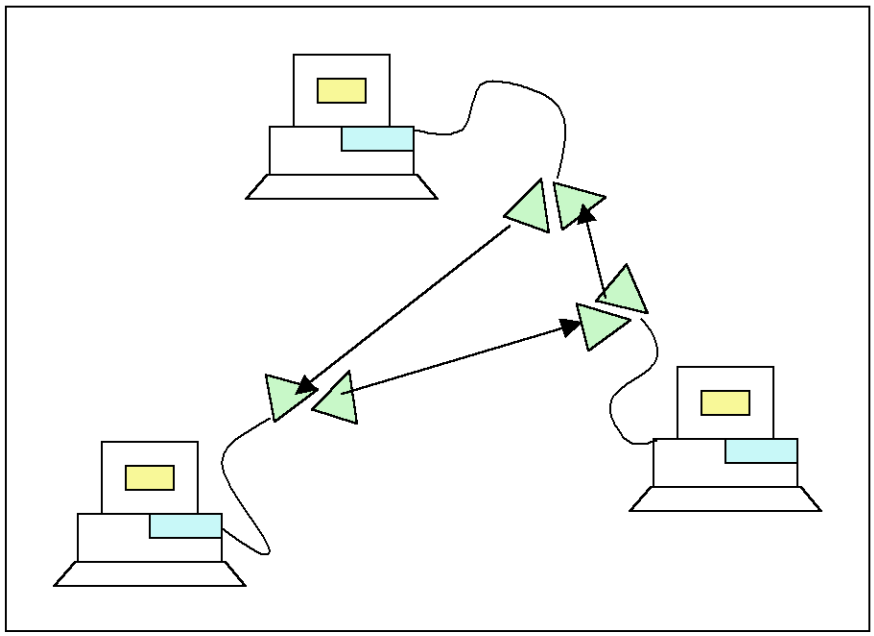

FIGURE 2.11 Point-to-Point Infrared LAN System [Geiger 1999]

At each station, the system interfaces with an IEEE 802.5 (token ring) interface board. Token-ring protocols ensure that only one station transmits at a time through the use of a token. The token, which is a special group of bits, circulates the ring. If a station wishes to transmit data, it must first wait its turn to receive the token, and then transmit its data. The capturing of the token ensures that no other station will transmit. The data circulates the ring and the appropriate destination will sense its address and process the data. Once finished, the sending station will forward the token to the next station on the way.

The advantages of using point-to-point infrared LAN system are the performance and security it offers. Because of the focused infrared beam, the system can provide performance requirements of either 4 or 16 Mbps token-ring protocols. The system is the only wireless LAN system on the market today that can support that type of performance. It is immune to electrical noise and is difficult to tap. Electrical signals do not interfere with the extremely high frequencies of infrared light, and an information thief would have to place himself within the path of the beam to receive the signal.

The disadvantage with this approach, however, is that it does not accommodate mobility. It might be suitable, however, in such environments as conference rooms or factories, where electrical noise would interfere with radio signals. Also, it must be

ensured that mounting the devices will not cause the blockage of the light beams. Because someone setting a plant on a desk or a forklift raising its cargo in line with the path the light travels could disrupt transmission.

2.1.2.3 Carrier-Current LANs

A quasi-wireless LAN technique, called *carrier current,* is the use of power lines as a medium for the transport of data. This technique is very similar to using an analog modem to communicate over telephone wires.

Power-line circuits within home and office provide enough bandwidth to support 1 to 2 Mbps data signals. For instance, at voltages of 110 volts on these circuits can typically carry 60 Hz alternating current. It is possible, then, to have *a power-line* modem that interfaces a computer to the power circuitry (figure 2.12). The interface acts much like a telephone modem and converts the digital data within computer to an analog signal for transmission through the electrical wires.

The 110-volt alternating current in the circuit does not affect the signal (or vice versa) because the signals are at different frequencies. The interface has filters that will prevent the lower 60 Hz frequency from being received.

The advantages of this technique are ease of installation and low-cost products. A disadvantage of the power-line approach is that the presence of electrical transformers, designed to electrically couple signals at 60 Hz, will block higher-frequency data signals. Most homes and smaller facilities will not have this problem because usually only one side of the transformer is available; however, larger buildings, especially industrial centers, will have multiple electrical wire legs connected by transformers. The presence of transformers, therefore, will limit connectivity among sites.

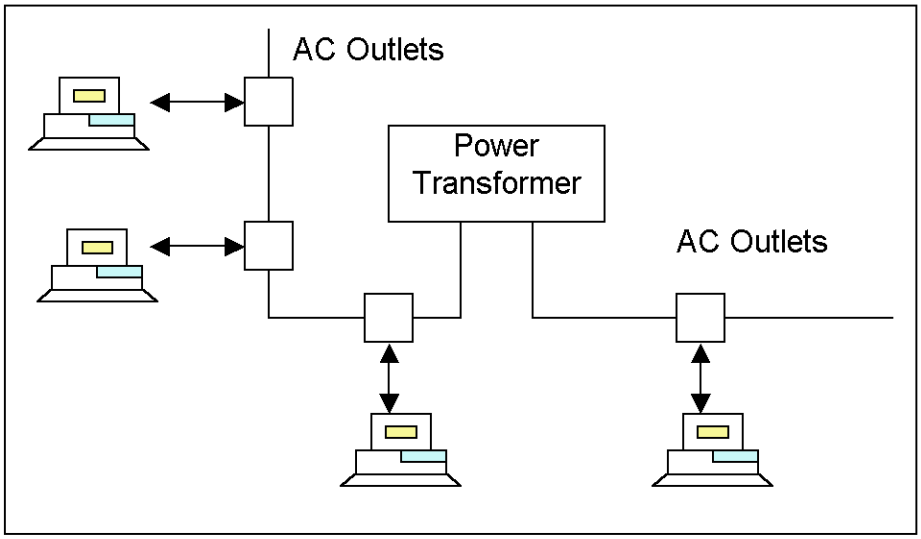

FIGURE 2.12 A carrier current LAN system [Geiger 1999]

2.2 Wireless Metropolitan Area Networks

Organizations generally need for communications between facilities in a local area, such as a city block or metropolitan area. A hospital, for example, might consist of several buildings within the same general area, separated by streets and rivers. Traditionally, companies have a physical media such as metallic wire or optical fiber, or leased 56 Kbps or T1 circuits to provide necessary connections. These forms of media, however, might require a great deal of installation time and can result in expensive monthly service fees. In some cases, leased communications lines might not even be available. A wireless point-to-point network is a flexible way of connecting buildings spread throughout a city:

2.2.1 Wireless Point-To-Point Applications

These networks provide communications links between buildings, avoiding the costly installation of cabling or leasing fees and the downtime associated with system failures. Many organizations, such as hospitals and government centers, use wireless point-to-point network components to avoid the installation of wiring along the roadway, digging trenches and routing cabling around rivers and roads.

Another use of wireless point-to-point network components is to perform a backup function in case a primary leased line is out of order. If a primary link fails, an organization can quickly deploy a wireless link to restore operations.

A wireless point-to-point network, as illustrated in figure 2.13, utilizes either radio waves or infrared light as a transport for the transmission of data up to 30 miles. These systems work in a point-to-point configuration, much like that of leased lines. Wireless point-to-point systems provide required data rates of existing LANs.

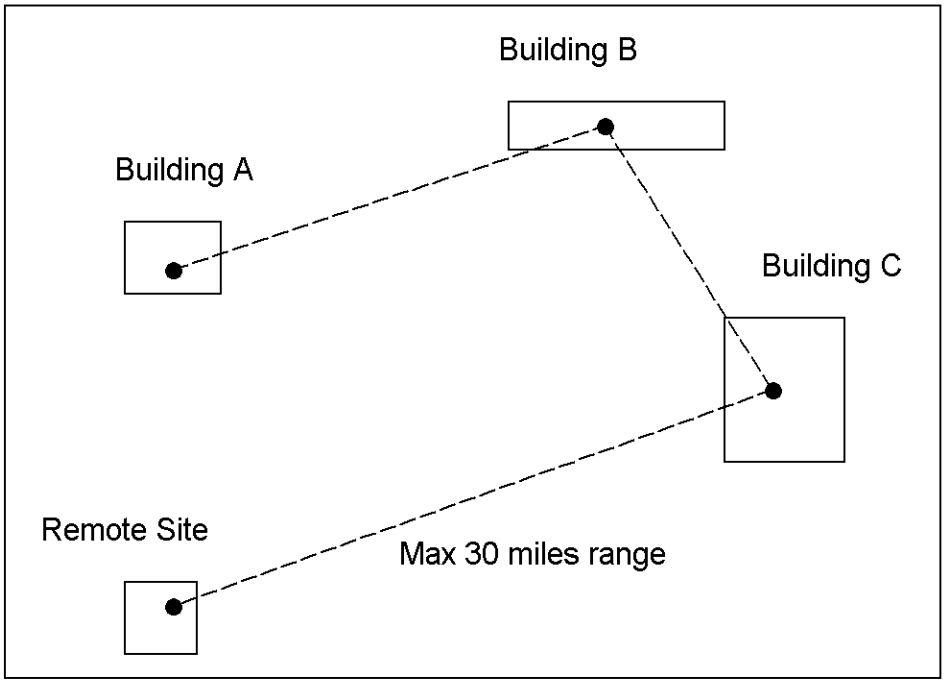

FIGURE 2.13 Point-To-Point Radio Waves or Laser [Geiger 1999]

2.2.2 Radio-Based Wireless Point-To-Point Networks

This type of point-to-point network is the most common method for providing links between the separate facilities of an organization within a metropolitan area. These systems have highly directional antennas that provide the signal power in a narrow beam so as to maximize the transmission distance. As a result, spread spectrum products operating under one watt of power can reach single hop transmission distances of 30 miles. But this data is handled at the production stage but the actual transmission distance of a particular product, however, depends on environmental conditions and earth surface. Rain, for example, causes resistance to

the propagation of radio signals, resulted with a decrease in the effective range. A mountainous area will also lower the transmission range of the signals.

Radio-based, wireless point-to-point network data rates are 4-5 Mbps for the short-range products operating along the two or three miles links. Reasonable products operate over a 30-mile link; however, they will transmit at much lower data rates to obtain the longer range. In addition, these products use either spread spectrum or narrowband modulation.

2.2.2.1 Radio Based Wireless Point-To-Point Network Components

As it can be seen from figure 2.14, radio-based wireless point-to-point networks mainly consist of transceivers and bridges/routers. Transceivers modulate the sent data with a carrier that will propagate the signal to the opposite site. As it happens in wireless LANs, the modulation transforms the computer's digital data into a suitable form that can be transmitted by air. Radio-based, wireless point-to-point network products often include an interface to Ethernet or token-ring networks, as well as bridging or routing functionality.

Wireless point-to-point network bridges, also called *wireless remote network bridges,* segment data traffic by filtering each packet according to its final destination address. This form of segmentation blocks packets from crossing the wireless link unless they need to reach a destination on the opposite side. Same as with local bridges, this makes usage of bandwidth more efficient and increases network performance.

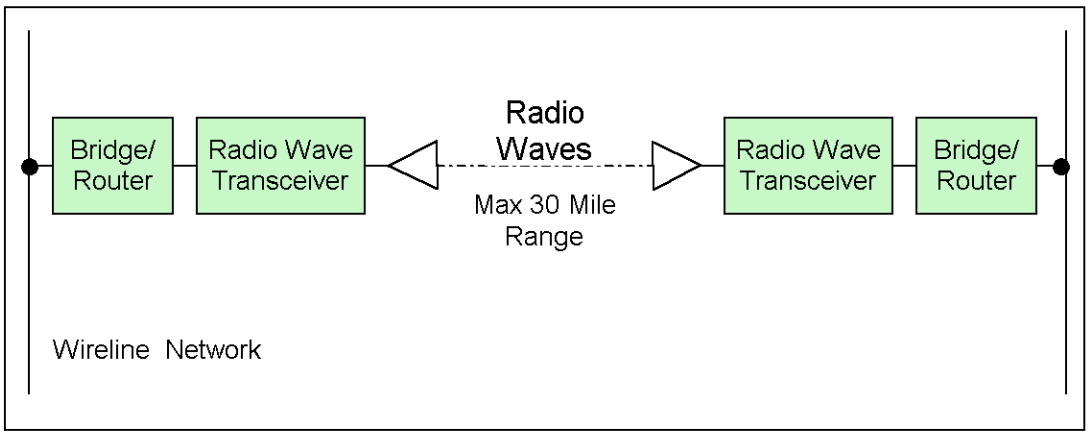

FIGURE 2.14 Radio-based wireless point-to-point network [Geiger 1999]

The routers forward packets according to the final destination address. This makes it possible to create a more intelligent network having alternative routes. In fact, a collection of these components would constitute the functionality of a WAN limited to a large metropolitan area. The difference, however, is that the wireless point-to-point network will not support mobile users-it just provides wireless connections between fixed sites.

2.2.2.2 Spread Spectrum Wireless Point-To-Point Networks

As with wireless LANs, wireless point-to-point networks using spread spectrum in the ISM bands again do not need to get user licensing. This situation results with an advantage of easy and rapid installation. The installation time of spread spectrum products can take a few hours, for instance, saving the two-month wait-time for obtaining FCC licensing.

Spread spectrum resists interference from traditional narrowband radio systems, enabling systems using both modulation techniques to coexist in the same space. The only signals likely to cause serious interference coming from other spread spectrum devices. As a result, the disadvantage is the possible interference with others operating similar wireless point-to-point networks around.

Radio waves traveling between buildings, perhaps across a large city, will be beyond the organization's authority and control, possibly receiving interference from other unknown systems.

2.2.2.3 Narrowband Wireless Point-To-Point Network

There are very few wireless point-to-point network products that operate on narrowband frequencies. These products operate within the 400-512 MHz and 820-960 MHz frequencies and have a range of 30 miles or more. For instance, a point-to-point product, called radio area network (RAN), operates in full-duplex mode ranging in data rates from 9.6 to 125 Kbps. The main applications of RAN are for the replacement of leased lines and wireline modems within metropolitan areas.

2.2.3 Laser-Based Wireless Point-To-Point Networks

Another class of wireless point-to-point networks utilizes laser light as a carrier for data transmission. The laser emits coherent light at a precise wavelength in a narrow beam. Most laser point-to-point networks utilize lasers that produce infrared light.

A laser modem modulates the data with a light signal to produce a light beam capable of transmitting data. With light, these data rates can be extremely high. Most laser links can easily handle Ethernet (10 Mbps), 4/16 Mbps token ring, and higher data rates. Figure 2.15 illustrates a laser point-to-point network. To maintain safe operation, laser links typically range less than a mile. These devices operate at Class III Center for Devices and Radiological Health standards, which can cause eye damage under some circumstances. Much longer distances are possible, but this causes an increase in the power to a level that would damage buildings and injure living things.

Weather is also an influence on the transmission distance of laser systems. A nice, clear day with very little smog will support the one-mile operating distance. Snow, rain, fog, smog, and dust, however, cause attenuation, which could limit the effective range to a half mile or less. As a result, there is a need to plan the link according to potential changes in the weather.

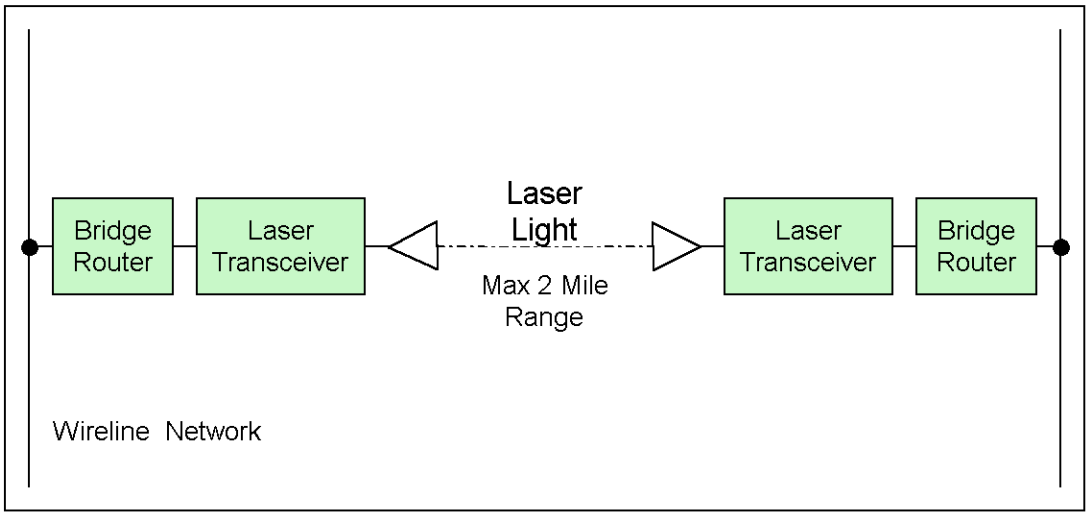

FIGURE 2.15 A laser-based wireless point-to-point network [Geiger 1999]

A laser point-to-point system has some advantages over other systems. It may effectively sustain 10 Mbps and higher data rates which means really high-speed data transmissions. There is no need to obtain FCC licensing because FCC doesn't manage frequencies above 300 GHz. Therefore, a laser system can be established as quickly possible like a license-free spread spectrum radio system.

When using a laser, very few other systems can cause interference. Even at high microwave frequencies, radio signals are far from the spectral location of laser light, which eliminates the possibility of interference from these systems. Also, another laser beam generally cannot interfere the working systems because it would have to be pointed directly at receiving site. But of course, someone might do this to purposely jam the system.

The top of a building or tower is the best place to install the laser link to accommodate a line-of-sight path between source and destination. This avoids objects blocking the beam, which can cause a disruption of operation. Birds are generally not a problem because they can see infrared light and will usually avoid the beam. A bird flying through the beam, however, will cause a momentary interruption. If this occurs, higher-level protocols, such as Ethernet or token ring, will trigger a retransmission of the data. The infrared beam will not harm the bird.

Another interference may be caused by sunlight that contains 60 percent of infrared light. Especially during early morning or late afternoon, the rising or setting sun may releases beams that can be received by transceivers. To overcome this problem it must be considered not to install the laser links on east-west direction.

Laser-based systems offer more privacy than radio links. Someone wanting to receive the laser data signal would have to physically place himself directly in the beam's path. Also, an intruder would have to capture the light to obtain the data, significantly attenuating or completely disrupting the signal at the true destination. This means that he would have to put himself next to the laser modem at either end of the link by standing on top of the building or climbing to the top of a tower. Physical security, such as fences and guards, can effectively eliminate this type of sabotage.

2.2.4 Radio-Based Wireless Point-to-Multipoint Networks

Many service companies are in the process of implementing wireless point-to-multipoint networks to support fixed location and mobile users with needs for accessing the Internet [17]. As it is illustrated in figure 2.16 point-to-multipoint wireless networks configurations offer wider coverage from a single point. In some cases, these companies are using IEEE 802.11 or proprietary technologies as the basis for these implementations.

Two emerging wireless MAN technologies are Multichannel Multipoint Distribution Service (MMDS) and Local Multipoint Distribution Service (LMDS). MMDS and LMDS primarily support fixed broadband wireless access to the Internet. With MMDS, a transmitting tower placed at a high elevation can reach customers with receiving dishes on their buildings within a 35-mile radius. In some cases, repeaters may extend the range into remote areas. MMDS is designed to operate in the 2.1 to 2.7 GHz radio frequencies, at transmission power of 1 to 100 watts, with data rates up to 10 Mbps with a 35-mile range. MMDS doesn't require line-of-sight.

MMDS is likely to prevail as the preferred choice for fixed wireless broadband connectivity in North America. Network service providers are rapidly deploying MMDS technology throughout the U.S. to reach local customers without negotiating access agreements with regional Bell operating companies. The advantage to the customer of using MMDS service is that the service provider will maintain the equipment and connections. Initial capital outlay is minimal and the customer pays only a monthly service fee.

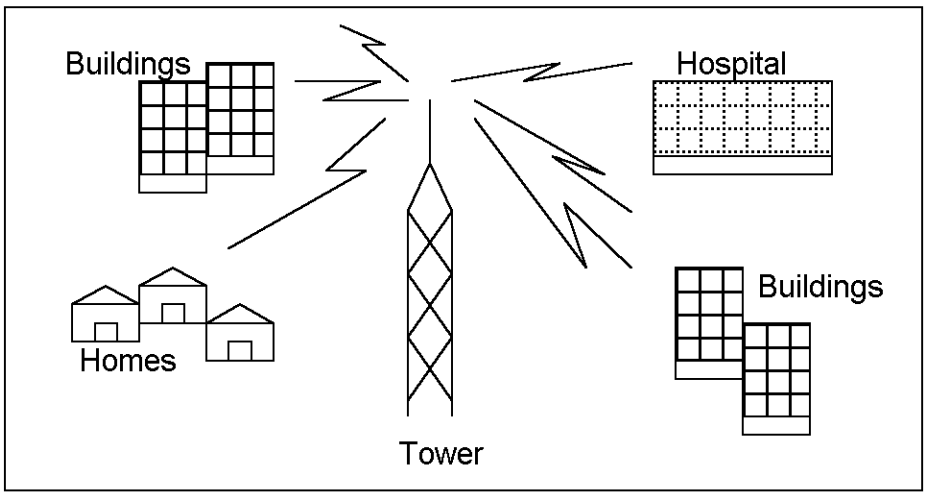

FIGURE 2.16 Point-to-Multipoint wireless networks [Geiger 2001]

An LMDS system consists of a series of cells defined by individual base stations connected to a central control point. An LMDS is designed to operate at 24, 28, 31, 38, and 40 GHz radio frequencies, at transmission power of 1 to 100 watts, with data rates up to 155 Mbps with a 2-mile range. LMDS transmissions are strictly line-of-sight. For this reason, carriers are apt to target business districts where rooftop mounting of subscriber dishes is permissible. Companies will likely subscribe to LMDS services for virtual private networks, packet or ATM telephony, and streaming video (including video broadcasting).

2.3 Wireless WANs

There may always a need for connecting a network to reach information and online services anywhere in the world such as archaeological dig sites or environmental survey sites or even in a city etc. Unfortunately there is no chance to plug a computer into the plain old telephone system all the time. For these situations, a wireless WAN might be the solution for effectively connecting people to the computing resources they need.

2.3.1 Packet Radio WANs

A packet radio WAN uses packet switching technique to transfer information one point to another. The main advantage of packet radio is its capability to economically and efficiently transfer short bursts of data that may be found in systems such as short messaging, dispatch, data entry, and remote monitoring.

2.3.1.1 Packet Radio Architecture

A packet radio network system performs the physical, data link, and network layer functions of OSI Reference Model. Therefore, it provides a physical medium, synchronization, and error control between nodes or routers and also performs routing function. If more than one hop is necessary to transfer data packets from source to destination, the intermediate packet radio nodes relay the data packets closer to the destination, very much like a router does in a traditional wire-based

WAN. When a user wants to utilize a packet radio network, a computer with a radio modem, suitable software, and a lease from service provider are required.

2.3.1.1.1 Packet Radio Modems

A radio modem supplies an interface between end-user appliances and radio relays, using air as the medium. These modems can work up to rates of 20 Kbps user throughputs to transform radio waves. Because they usually do not require licensing, moving them from one location to another is not a big problem. Most of them radiate the data omnidirectionally.

As long as connectivity exists, a pair of radio modems establishes a channel for data transmission between sites. The main condition for proper connectivity is that the destination must be able to correctly receive data from the source at a specified minimum data rate. If the reception of data on a particular channel results in a number of bit errors exceeding the maximum error rate for that link, for example, connectivity is lost. Due to node separation, transmit power, and irregular topography; most packet radio networks cannot maintain full connectivity. Node separation affects the connectivity of a radio network because the power of a radio signal decreases exponentially as the distance between the nodes increases. If the distance becomes too great, the signal-to-noise ratio decreases and produces too many transmission errors, causing the two stations to become disconnected.

The transmit power of the source node affects link connectivity because higher transmit powers will keep the signal-to-noise ratio higher, resulting in fewer errors and connectivity. Some barriers on earth's surface, such as mountains and buildings, can affect connectivity because they will attenuate and sometimes completely block radio waves. The attenuation will decrease the signal power, resulting in shorter transmission distances. A packet radio network, therefore, must perform routing to move data packets from the source user device, through a number of intermediate radio relays, and to the destination user device or network.

2.3.1.1.2 Relay nodes

The radio relay nodes forward transmitting packets closer to the destination. These nodes implement a routing protocol that maintains the optimum routes for the routing tables. The routing table contains a record for each possible destination relay node. Consequently, a relay node uses a routing table to address the packet to the next node that is closer to the destination.

2.3.1.2 Packet Radio Operations

A packet radio network mainly performs two functions to carry packets from source to destination:

1. Transmit data packets
2. Update routing tables at the relay nodes

2.3.1.2.1 Transmitting Data Packets

A packet radio network uses a carrier sense protocol to access the shared air and radio medium. The primary difference from Ethernet and radio-based wireless LANs is that a packet radio network operates in a partially connected rather than fully-connected topology (see figure 2.17). The propagation boundary of each node constitutes that node's operating range. Nodes A and C, for example, can communicate directly with each other.

When a packet radio station wants to send a data packet it must listen to designate whether another station is using the medium. If no other transmission is recognized, the sending station will transmit the packet in a broadcast mode by means of its omnidirectional antenna. The first station to receive the packet will generally be the neighboring relay node. This relay will search its routing table to find where the packet will be send next, according to the final destination address. If the destination can be found in the relay's boundary, the packet will be broadcasted by relay node to be received by destination. If the final destination is not close enough, the relay node will broadcast the packet to the next relay node closer to the destination. This process will continue until the packet reaches the destination.

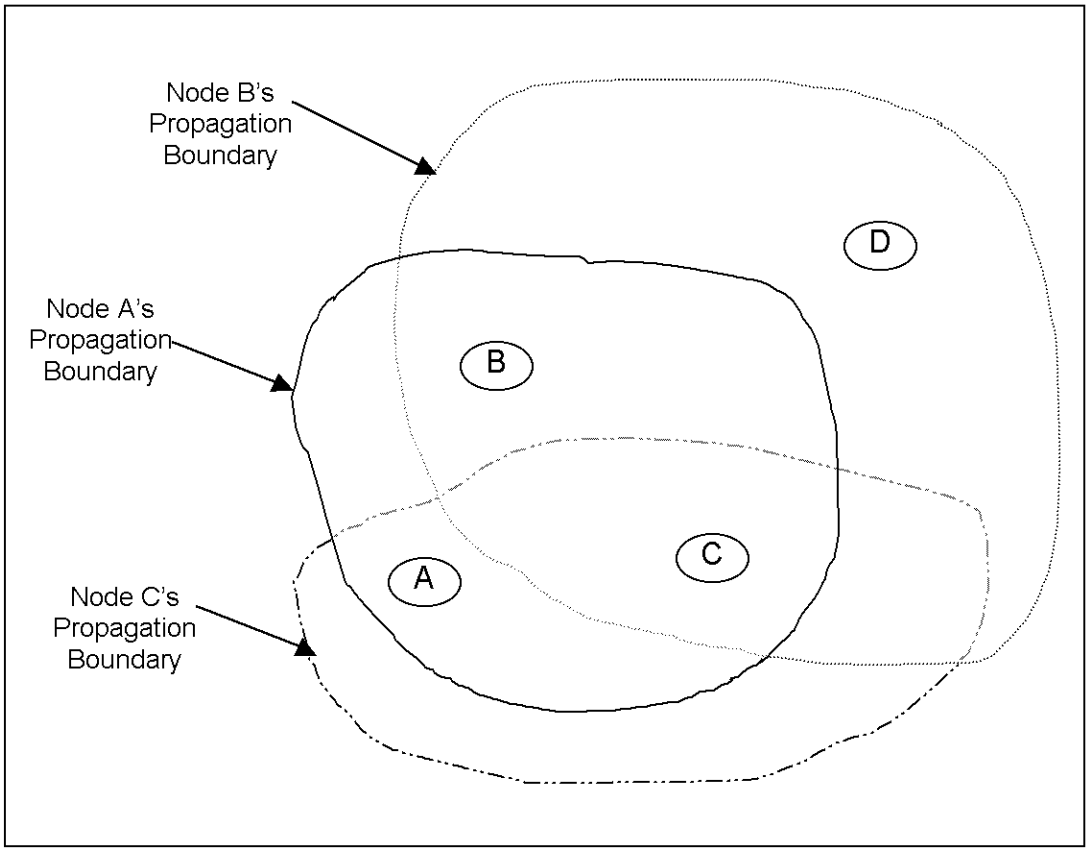

FIGURE 2.17 Partially connected packet radio network topology [Geiger 1999]

2.3.1.2.2 Updating Routing Tables

As it happen in wireline WANs, a packet radio topology may show changes by the time passing. Some relay nodes may be unusable, new ones may be added to the system or weather conditions may disturbs the connectivity channels. The effective usage of the system is depends on the success of the routing protocol. This will occur if the protocol is updated regularly depending on the system changes.

Packet radio routing protocols enable each router within the network to gain a complete picture of the network's topology as it occurs in traditional wireline systems. This function is maintained by providing as follows: Each relay node periodically sends a status packet that informs its presence to all neighboring relay nodes within the nodes coverage area. Therefore, each node learns the presence of its immediate neighbors time by time. A router can also use this information to update its routing table. When a relay node sends its status message, it also sends a copy of

its routing table. Each relay node also sets timers for each neighbor, and if the relay node does not receive a status message within a certain time period, the relay node will delete the neighbor from the routing table. Other relay nodes will hear of the deletion again by means of periodic status messages. All of these processes provide each relay node to obtain a complete map of the network in terms of connectivity.

2.3.1.3 Packet Radio Providers

Several packet radio service providers have constructed networks that implement the radio relay nodes. The process of establishing packet radio networking is to lease the service from one of several packet radio access providers. This service is very economical and the companies usually supply the software for no charge; however, users must purchase a radio modem.

2.3.2 Analog Cellular WANs and Technology

The general idea of an analog cellular WAN is to make use of the cell phone's mobility and employ it as a means of transferring data, much like the use of traditional wire-based plain old telephone system (POTS). The idea of this technology is to connect user computer to a cellular telephone via a modem and then with a remote system through a dial-up connection. This provides a relatively easy way to obtain wireless data transfer wherever cellular telephone service exists, which covers most of the world.

The cellular approach, of course, has some main drawbacks. First of all, the usage costs are relatively high. The cost of sending data is based on the length of the call and the distance to the destination. These factors affect the time need to be stay connected. It may be paid more as roaming from one location to another. Roaming within three different regions in one day, for example, can cost approximately $ 10, not counting the standard air time.

Another problem is the occasional transmission errors that will cause retransmissions to occur. The cellular telephone system was built primarily to transmit voice, which can generally stand more transmission errors than data.

The analog cellular telephone system uses FM (Frequency Modulation) radio waves to transmit voice grade signals. To accommodate mobility, this cellular system switches the radio connection from one cell to another while moving between areas. Every cell within the network has a transmission tower that links mobile callers to a mobile telephone switching office (MTSO). The MTSO, which is owned and operated by the cellular carrier of the area, provides a connection to the public switched telephone network. Each cell covers several miles. Figure 2.18 illustrates the general topology of the cellular telephone system.

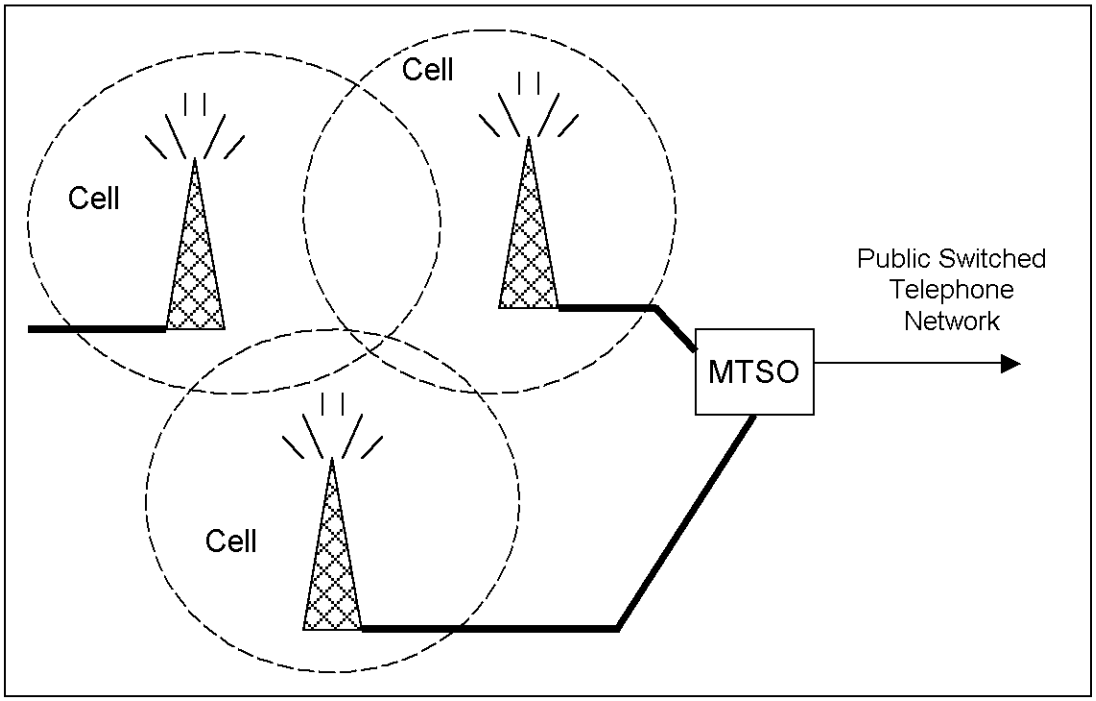

FIGURE 2.18 General topology of a circuit-switched cellular phone system [Geiger 1999]

Most modems that operate over wireline telephone services can also be used to interface and interoperate with cellular phones. But the running software has to be optimized to work with cellular phones to minimize battery usage.

A major problem is that there is no standard connector to interface the portable computer's serial interface to a cellular phone. Therefore, it must be assured to find a cable to connect between the modem and the phone.

2.3.3 Cellular Digital Packet Data (CPDP) WANs and Architecture

A consortium of companies in the United States developed the Cellular Digital Packet Data (CDPD) standard to establish a dedicated wireless data network for mobile users. CDPD overlays the conventional analog cellular telephone system, using a channel-hopping technique to transmit data in short bursts during idle times in cellular channels. CDPD operates full duplex, i.e. there can be simultaneous transmission in both directions, in the 800 and 900 MHz frequency bands. These data transmissions offer rates up to 19.2 Kbps.

The main advantage of the analog cellular system is widespread coverage. Because CDPD overlays on this system, it will also provide nearly worldwide coverage. Moreover CDPD has a great advantage that it uses digital signals, making it possible to enhance the transmission of data. By using digital signals, it is possible to encrypt the data stream and provide easier error control.

CDPD is a robust protocol that is connectionless and utilizes Reed-Salomon forward error correction (FEC). FEC is an error control technique that corrects errors at the receiver without asking the source to retransmit the wrong packet. Security issue in CDPD is accomplished by using an encrypted key-passing technique, which is very good. Also with CDPD, its paid only for the amount of data actually sent, which is less than money required to keep connection alive to data transmission on an analog cellular call if sending the same data.

An architecture of a CDPD system can be shown as figure 2.19. The Mobile Data Base Station (MDBS) defines a radio cell that interfaces the Mobile End System (M-ES), such as a portable computer with a CDPD modem, with the Mobile Data Intermediate System (MD-IS). The MD-ISs provide mobility management services for the CDPD network. The MDBS acts as a bridge between the wireless protocols of the M-ES and the landline protocols of the MD-IS. Therefore, the MDBS decodes the data received from mobile devices, reconstructs the data frames, and transfers them to the MD-IS.

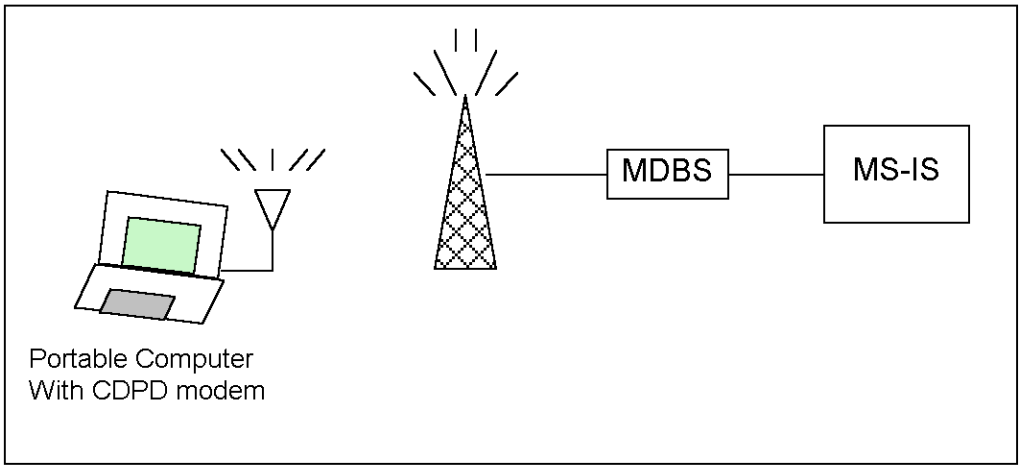

FIGURE 2.19 A CDPD system [Geiger 1999]

At most cellular telephone base sites, digital communications lines tie the MD-ISs back to the cellular telephone system's MTSO. The CDPD architecture includes mobility management and internetworking between separate CDPD network providers: This results with seamless operations while moving between different cells and providers.

An M-ES wanting to send data uses the Digital Sense Multiple Access (DSMA) protocol to share radio channels with other M-ESs. This protocol is similar to the common Ethernet protocol used in LANs. DSMA, however, has both a forward and reverse channel that supports full-duplex operation. MDBSs transmit on the forward band, and M-ESs transmit on the reverse band. To utilize CDPD, it is needed to lease the service through the local provider and purchase a CDPD modem.

2.3.4 Satellite Communications

Satellite communications might be a good alternative for really good coverage area but they provide relatively low data rates. The main issues with satellite systems are high costs and limited support for mobile users. The monthly service costs are relatively low, but initial equipment costs are very high. The portability aspect of satellite requires users to set up the antenna dish and align it with the satellite before sending data.

Satellite systems nowadays support transmission of video, voice, and data for a variety of companies that require global coverage. Figure 2.20 shows the components

that make this possible. The satellite is a platform that hosts a series of transponders acting as signal repeaters. The transponders receive directed signals on the uplink from Earth stations and broadcast the signals back to Earth on a downlink frequency where users over a very wide area are able to receive the signal.

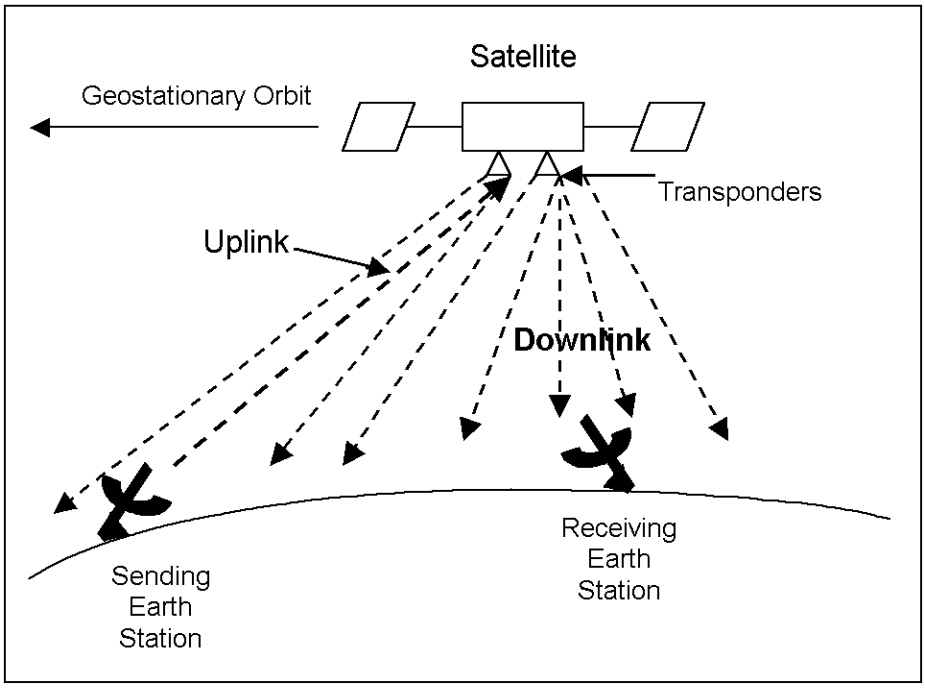

FIGURE 2.20 A satellite system [Geiger 1999]

A satellite in geostationary orbit has a 24-hour period at an altitude of 22,300 miles over the equator. This type of orbit means the satellite takes one full day to orbit the Earth, which makes the satellite appear to look stationary from the Earth's surface. This enables the Earth station antennas to remain fixed, not having to track the satellite. Some satellite systems, however, work at lower altitudes to lessen the amount of propagation delay. These lower-altitude satellites are not geostationary and will appear to move across the sky, requiring Earth stations to have tracking antennas. Newer, lower Earth-orbiting satellite systems, such as Iridium and Globalstar, offer 2,400 to 9,600 bps data throughput from handheld terminals. Future broadband satellite systems will deliver much higher data rates. To utilize a satellite system, there is a need for a satellite station that consists of an antenna, satellite transceiver, and an interface to the computer.

Several satellite projects are in different stages of implementation. Some of these are shown in table 2.2.

TABLE 2.2 Some emerging satellite systems for mobile communications [Varshney 2000].

System Name	Orbit (height)	Satellite (channels)	Frequency of operation	Applications	Coverage	Charges	Start Date
Globalstar	LEO 1400 Km	48 (130,000)	1.6 2.4 GHz users 5GHz up	Voice/data	Worldwide (except poles)	$1000 (terminal) $0.50 airtime	1999
ICO	MEO 10,355 Km	10 (45,000)	7 GHz down 5GHz up	Voice/data	Worldwide	$1000 (terminal) $1 airtime	2000
Teledesic	LEO 1400 Km	288 (unspecified)	7 GHz down 28 GHz	Video/voice data	Worldwide	Unspecified	2003

2.3.5 Meteor Burst Communications

A meteor burst communications system works similar to a satellite system, except the meteors reflect the radio signal instead of a satellite. Actually, everyday almost billions of tiny microscopic meteors goes into the atmosphere. While penetrating the ionosphere, these particles leave a trail of ionized gas. Meteor burst communications uses this ionized gas formation as reflection medium. The system directs a radio wave, modulated with a data signal, to this ionized gas as shown in figure 2.21. The radio signal is reflected from this gas formation and directed back to Earth that covers a large area of the Earth's surface, enabling long-distance operation.

Because it supplies a great coverage area for cellular network packets a meteor burst communications system is really advantageous. Moreover, implementation cost of it generally is less than having a leased satellite service. These benefits make meteor burst systems well suited for remote telemetry, water management, environmental monitoring, pipeline regulation, and oceanographic observation.

The master station is the main component in a meteor burst communications system. It controls the routing of messages and data from hundreds of remote data terminals throughout the system. A remote data terminal collects data from analog and digital sensor inputs. When the remote data terminals receive a beam from a

master station, they can send data containing information obtained from their sensors.

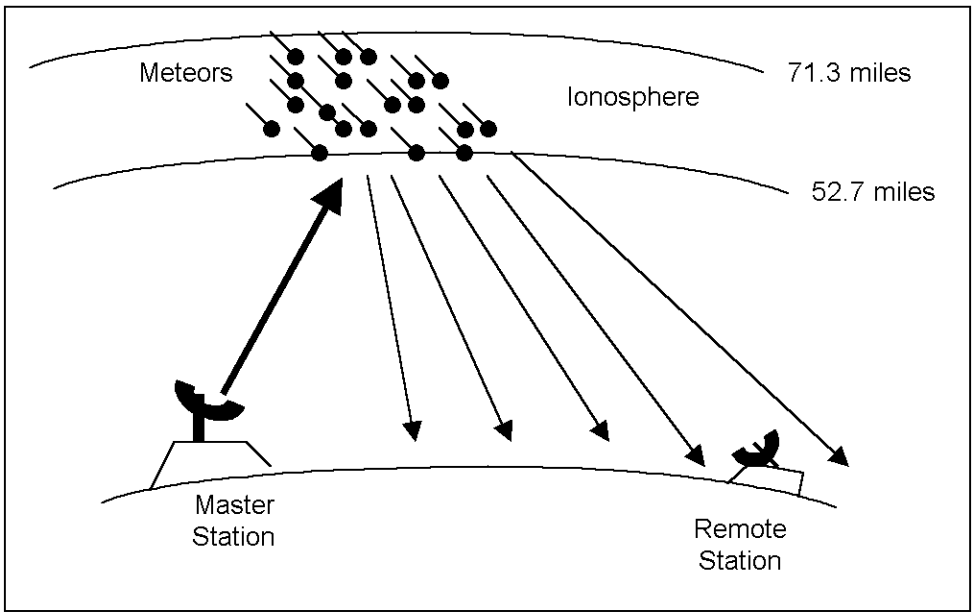

FIGURE 2.21 A meteor burst communications system [Geiger 1999]

2.3.6 Combining Location Devices With Wireless WANs

The aim of location devices is to identify a position on the Earth's surface in terms of latitude and longitude. Nowadays very high prices of these devices show dramatic decrease that they are find a place in people's daily life. These devices are mainly based on Global Positioning System (GPS) technology. GPS is a worldwide, satellite-based radio navigation system providing three-dimensional position, velocity, and time information to users having GPS receivers anywhere on or near the surface of the Earth.

The combination of wireless WAN technologies and location devices gives some valuable results. The joining of these technologies makes it possible for a mobile element to inform its exact location to other elements. Many companies are combining CDPD and paging with the Global Positioning System (GPS) in their products, mainly for vehicle tracking.

2.4 Wireless ATM

Asynchronous Transfer Mode (ATM) has been advocated as an important technology for all types of services and networks [9]. Most people believe that ATM will be the standard for the future B-ISDN (Broadband Integrated Services Digital Network). From the service point of view, ATM combines both the data and multimedia information into the wired networks while scales well from backbones to the customer premises networks.

Due to the success of ATM on wired networks, wireless ATM (WATM) is a direct result of the ATM "everywhere" movement. WATM can be viewed as a solution for next-generation personal communication networks, or a wireless extension of the B-ISDN networks, which will support integrated data transmission (data, voice, video) with guaranteed QoS.

Because of the wide range of services supported by ATM networks, ATM technology is expected to become the dominant networking technology for both public infrastructure networks and LANs [8]. ATM infrastructure can support all types of services, from time-sensitive voice communications and multimedia conferencing to bursty transaction processing and LAN traffic. Extending the ATM infrastr cture with wireless access meets the needs of users and customers who want a unified end-to-end networking infrastructure with high performance and consistent service. Wireless ATM adds the advantages of mobility to the already great service advantages of ATM networks.

2.4.1 Background of ATM

ATM has been advocated as an important technology for the wide area interconnection of heterogeneous networks. In ATM networks, the data is divided into small, fixed length units called cells. The cell is 53 bytes. Each cell contains a 5 byte header, this header contains the identification, control priority, and routing information. The other 48 bytes are the actual data. ATM does not provide any error detection operations on the user payload, inside the cell, and also offers no retransmission services.

ATM switches support two kinds of interfaces: User Network Interface (UNI) and Network Node Interface (NNI). UNI connects ATM end systems (hosts, routers, etc.) to an ATM switch, while a NNI may be imprecisely defined as an interface connection between two ATM switches. The ITU-T Recommendation requires that an ATM connection be identified with connection identifiers that are assigned for each user connection in the ATM network.

At the UNI, the connection is identified by two values in the cell header: Virtual Path Identifier (VPI) and the Virtual Channel Identifier (VCI). Both VPI and VCI can combine together to form a virtual circuit identifier.

The following figure 2.22 shows the UNI and NNI interface to a wireless ATM Network:

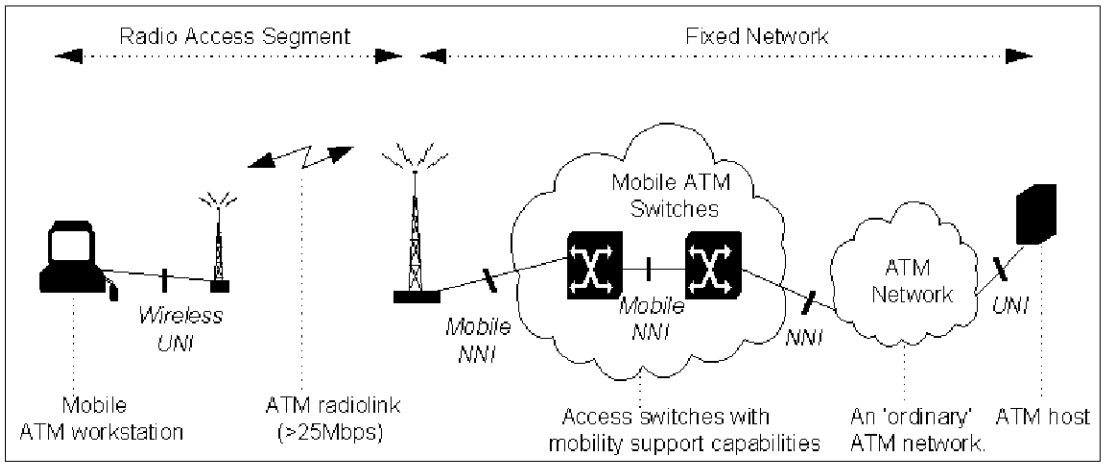

FIGURE 2.22 Wireless ATM reference architecture [Cereceda 1997]

There are two fundamental types of ATM connections:

1. Permanent Virtual Connections (PVC):

A PVC is a connection set up by some external mechanism, typically network management. In this setup switches between a source and destination ATM, are programmed with the appropriate VPI/VCI values. PVCs always require some manual configuration

2. Switched Virtual Connections (SVC):

An SVC is a connection that is set up automatically through a signaling protocol. SVCs do not require the manual interaction needed to set up PVC's and, as such, are likely to be much more widely used. All higher layer protocols operating over ATM primarily use SVCs.

ATM is designed to support both real-time and non–real-time traffic with different delay, loss, and throughput requirements [39]. In addition, ATM has the major advantage of being scalable; therefore ATM can be used in local-area as well as wide-area environments at very high bit rates.

ATM is a connection-oriented technology, so after a mobile user moves to a new location connection rerouting has to be performed. The connection rerouting schemes can be based on (a) setting up a new connection, (b) providing multiple paths to a mobile user, (c) forwarding ATM cells, or (d) dynamically rerouting the connection.

To route or reroute ATM connections, the wireless ATM network should have the information about the current location of mobile hosts. Any change in location information should be reflected in the storage system, usually a location database. And the new location information should be available to the network when a connection to a mobile host needs to be set up (routed) or rerouted. Four major location management schemes are shown in figure 2.23.

When ATM cells are transmitted over wireless links, a high rate of cell loss may occur. Possible ways to counteract the cell loss include the use of forward error-correction algorithms or the use of an error-detection scheme (Cyclic Redundancy Control, for example) followed by buffering and selective retransmission of ATM cells. The retransmission and possible resequencing of ATM cells will require the use of sequence number in ATM cells. It may be possible to package sequence number, error-control overhead, and a 53-byte ATM cell together in a larger WATM cell.

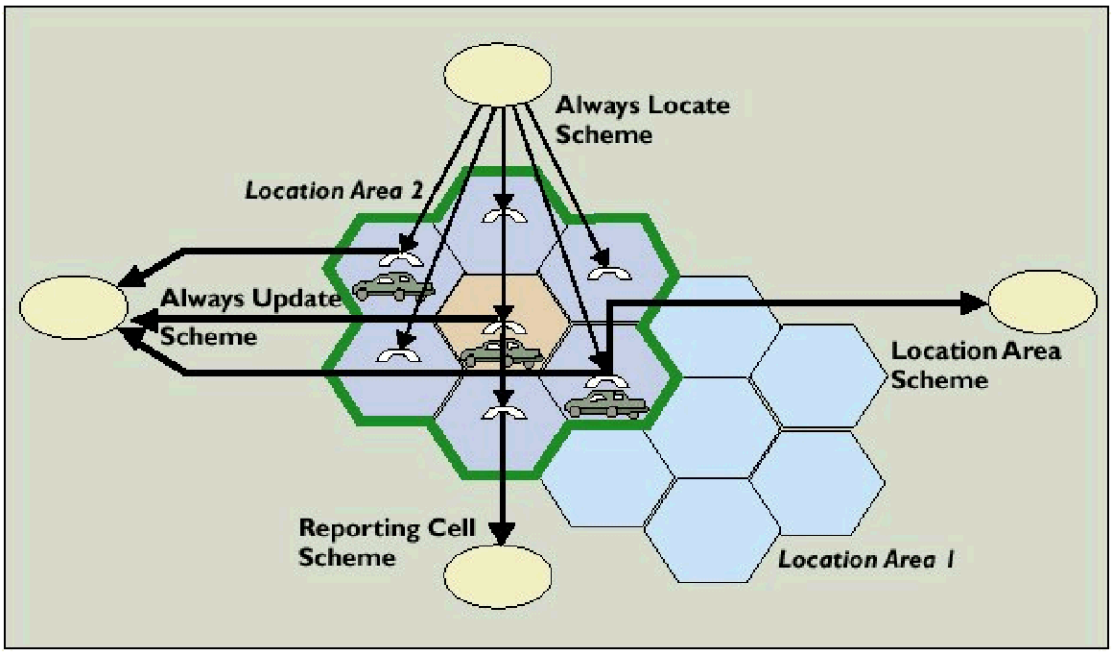

FIGURE 2.23. Four major location update schemes.[Varshney 2000]

2.4.2 Reasons for Wireless ATM

Since the beginning the concept of ATM is for end-to-end communications (i.e. in a WAN environment). The communication protocol will be the same (i.e. ATM), and companies will no longer have to buy extra equipment (like routers or gateways) to interconnect their networks. Also, ATM is considered to reduce the complexity of the network and improve the flexibility while providing end-to-end consideration of traffic performance. That is why researchers have been pushing for an ATM cell-relay paradigm to be adopted as the basis for next generation wireless transport architectures.

There are several factors that tend to favor the use of ATM cell transport for a personal communication network. These are:

- Flexible bandwidth allocation and service type selection for a range of applications
- Efficient multiplexing of traffic from bursty data/multimedia sources
- End-to-end provisioning of broadband services over wireless and wired networks

- Suitability of available ATM switching equipment for inter-cell switching
- Improved service reliability with packet switching techniques
- Ease of interfacing with wired B-ISDN systems that will form the telecommunications backbone

In general, interworking may always be seen as a solution to achieve wireless access to any popular backbone network but the consequence, in this case, is a loss of the ATM quality of service characteristics and original bearer connections. The more interworking there is in a network, the less harmonized the services provided will be. Therefore, it is important to be able to offer appropriate wireless extension to the ATM network infrastructure.

One of the fundamental ideas of ATM is to provide bandwidth on demand. Bandwidth has traditionally been an expensive and scarce resource. This has affected the application development and even the user expectations. So far, application development has been constrained because data transmission pipes cannot support various quality of service parameters, and the maximum data transmission bandwidth that the applications have to interface with is relatively small. Finally, ATM has removed these constraints. Bandwidth has become truly cheap and there is good support for various traffic classes.

The figure 2.24 shows a typical ATM network.

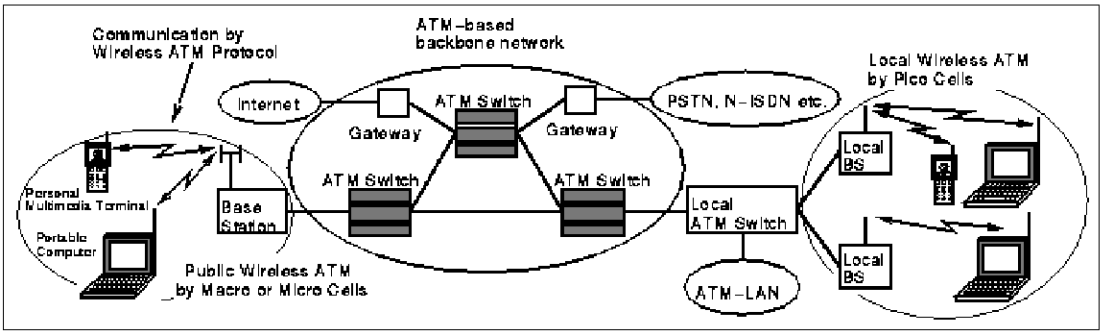

FIGURE 2.24 Typical ATM network [Cereceda 1997]

2.4.3 Wireless ATM Reference Models

A system reference model for WATM is shown in figure 2.25. The overall system consists of a fixed ATM network infrastructure and a radio access segment. In the fixed ATM network, the switches, which communicate directly with wireless station or wireless end user devices, are mobility enhanced ATM switches. These switches setup connections on behalf of the wireless devices. They serve as the "entrance" to the infrastructure wired ATM networks. The other ATM switching elements in the wired ATM networks remain unchanged.

Based on the different types of wireless applications, the radio access segment falls into a number of areas that may need different solutions.

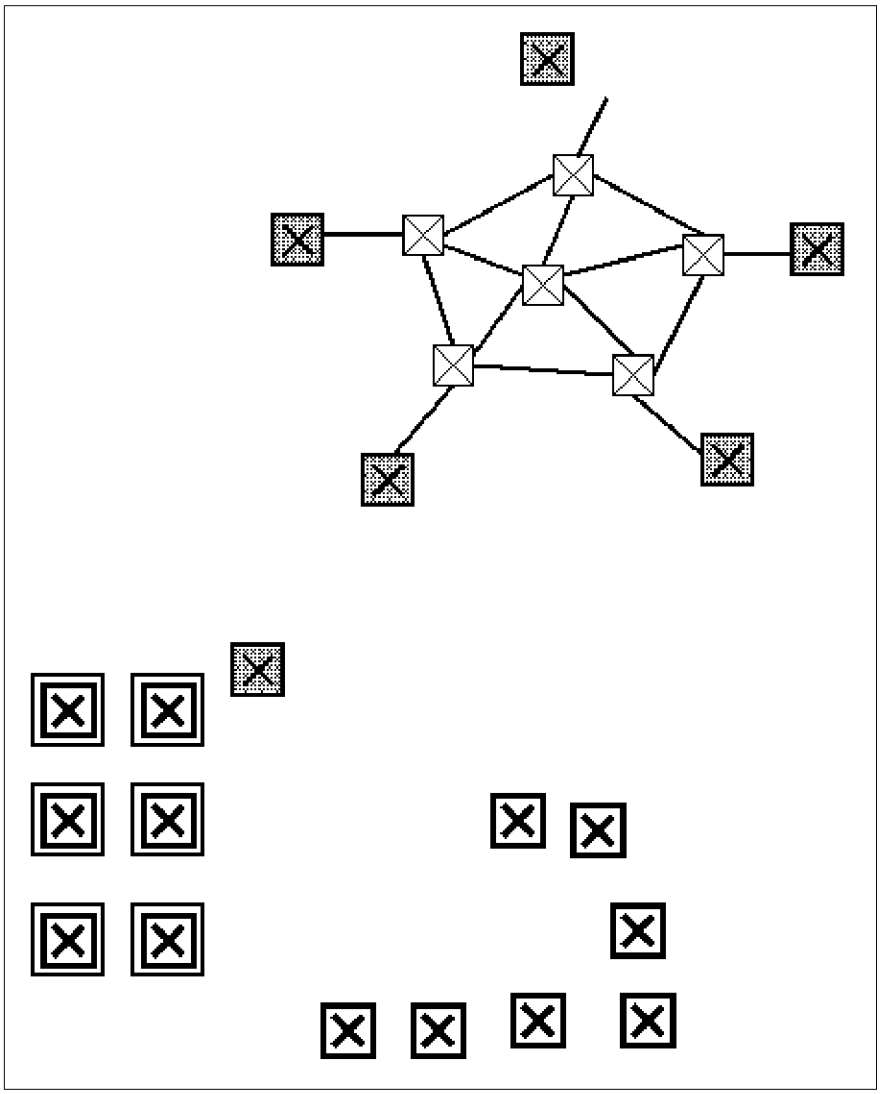

FIGURE 2.25 A reference model for WATM [Cong]

2.4.3.1 Fixed Wireless Components

In fixed wireless LANs, or network interconnection via satellite or microwaves links, the end user devices and switching devices are fixed. They establish connections with each other via wireless channel, not through cable. In these kinds of applications, the data transmissions are wireless, yet without mobility. Since the user devices do not roam around, some design issues, e.g. handover, location management, and re-routing, are not presented.

2.4.3.2 Mobile End Users

In digital cellular, PCS, and wireless Lans, the end user devices, which are mobile, communicate directly with the fixed network switching devices via wired or wireless channels. To support the ATM connections, the end user devices are required to be equipped with a Wireless Terminal Adaptor that communicates with the Wireless Access Point in the fixed switching elements (mobility enhanced ATM switches)

2.4.3.3 Mobile Switches with Fixed End Users

End user devices are connected to switches via wired or wireless channels. The end user device and the switch, as a unit, are mobile. There can be more than one end user devices attach to one switch. An end user device is fixed to one switch instead of roaming around different switches. The switch is responsible to establish connections with the fixed infrastructure network component, either through wired channel or wireless channel. In this case, Wireless Access Points and Wireless Terminal Adapters are needed by the fixed mobility enhanced ATM switches and the mobile switches.

2.4.3.4 Mobile Switches with Mobile End Users

In this case, end user devices are mobile. There are also some mobile switching elements. When the end user wants to establish a connection, it first setups a

connection with a mobile switch, which then setups a connection with the fixed network switches, either directly, or via another mobile switches. Wireless Access Points and Wireless Terminal Adapters are also needed to support the mobility.

2.4.3.5 Interworking with PCS

In PCS networks, the users are PCS terminals. PCS terminals send data to proper PCS base stations via wireless link, which then establish connections to the fixed network switching elements through a base station controller. The base station controller is a logical element which function as the ATM<->PCS translator.

2.4.3.6 Wireless Ad Hoc Networks

An Ad Hoc network is the cooperative engagement of a collections of mobile terminals without the required intervention of any centralized access point. An auto-configuration of a wireless ATM network will be required for this kind of application. In wireless Ad Hoc Networks, an end user can communicate with the mobility enhanced ATM switches either directly, or via a central controller.

2.4.4 Wireless ATM Architecture

The architecture proposed for wireless ATM is composed of a large number of small transmission cells called pico cells. Each pico cell is served by a base station. All the base stations in the network are connected via the wired ATM network. The use of ATM switching for intercell traffic also avoids the crucial problem of developing a new backbone network with sufficient throughput to support intercommunication among large number of small cells. To avoid hard boundaries between pico-cells, the base stations can operate on the same frequency.

Reducing the size of the pico-cells has major advantages in mitigating some of the major problems associated with in-building wireless LANs. The main difficulties encountered are the delay due to multi-path effects and the lack of a line-of-sight path resulting in high attenuation. Pico-cells can also have some drawbacks as compared to larger cells. There are a small number of mobiles, on average, within

range of any base-station, so base-station cost and connectivity is critical. As cell size is reduced, hand-over rate also increases. By using the same frequency, no hand-over will be required at the physical layer. The small cell sizes also give us the flexibility of reusing the same frequency, thus avoiding the problem of running out of bandwidth.

The mobile units in the cell communicate with only the base-station serving that particular cell, and not with other mobile units. The basic role of the base station is interconnection between the LAN or WAN and the wireless subnets, and also to transfer packets and converting them to the wired ATM network from the mobile units.

The figure 2.26 shows a typical ATM to Base Station Connection:

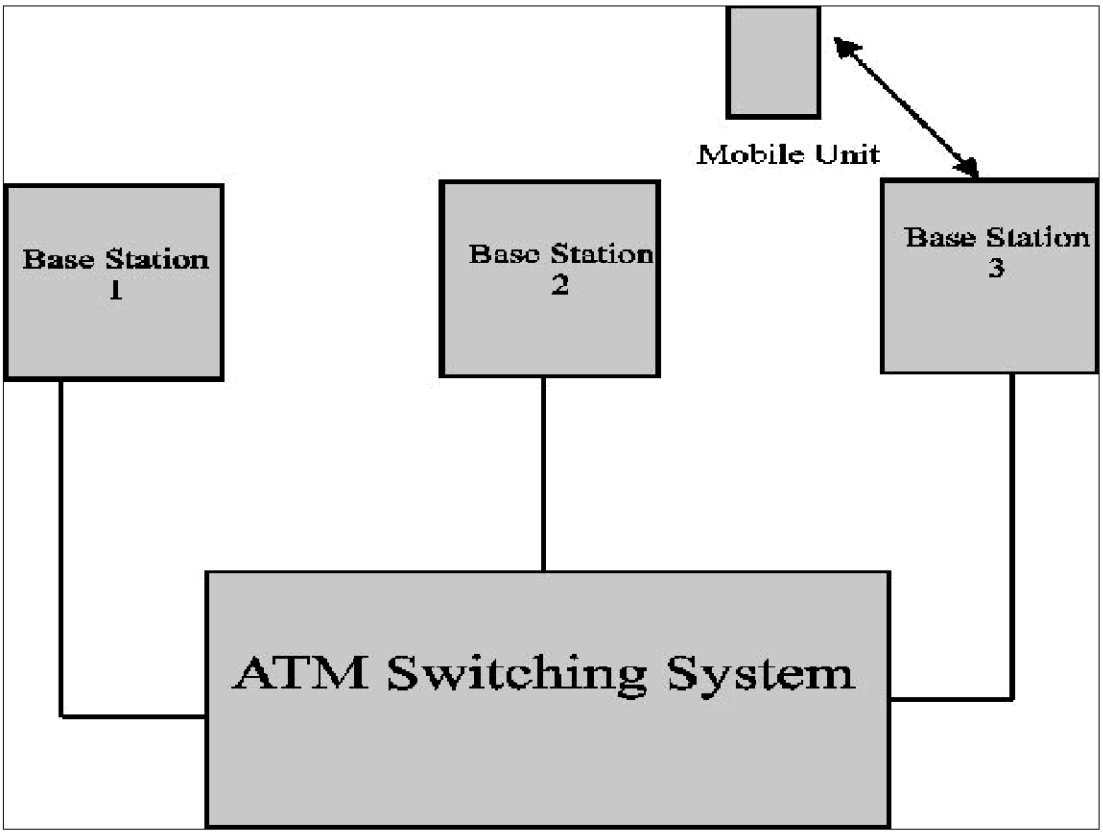

FIGURE 2.26 A typical ATM to base station connection [Cereceda 1997]

When ATM cells are transmitted over wireless links, a high rate of cell loss may occur. Possible ways to counteract the cell loss include the use of forward error-correction algorithms or the use of an error-detection scheme (Cyclic Redundancy

Control, for example) followed by buffering and selective retransmission of ATM cells. The retransmission and possible resequencing of ATM cells will require the use of sequence number in ATM cells. It may be possible to package sequence number, error-control overhead, and a 53-byte ATM cell together in a larger WATM cell.

2.5 Personal Area Networks

A person who carries a watch, pager, cellular phone, personal stereo, personal digital assistant (PDA), and notebook computer is carrying five displays, three keyboards, two speakers, two microphones, and three communication devices [19]. The duplication of I/O components is in part a result of the inability of the devices to exchange data. With proper networking these devices can share I/O, storage, and computational resources.

The problem is all about the inability of all these devices to network with each other seamlessly and transparently. The solution is based on the following considerations:

1. Remove the IO and storage redundancy
2. Achieve an instant and transparent way of interdevice communication
3. Security: The data communication between these devices must be secure and should be limited to the intended set of device
4. The power consumption overhead should be very small or zero.
5. Ability to expand the scope of communication between devices to other devices like a desktop computer etc.

One way of transferring data between two devices is using RF (Radio Frequency). As the growth of wireless services (e.g., cellular phones, pagers, and radio frequency local area networks [RF LANs]) fills up the limited RF spectrum, near-field communication offers an alternative to congesting the airwaves with data. Also with RF communications there would always be the associated issues of security. Far field, RF communications are always susceptible to eavesdropping and interference because the isotropic properties of a radio transmitter. Power consumption is also an issue. There are also infrared (IR) solutions available but IR solutions are not practical for communication between devices hidden in wallets,

pockets etc. Focused IR relies on line-of-sight transmission, which is difficult to maintain with body-based devices that are constantly in motion. Diffused IR relies on a wide-angle beam of high optical power requiring hundreds of milliwatts. Personal area networks, work on the near field, electric field sensing. Electrostatically coupled PAN devices use the body as a "wet wire" and can operate on several milliwatts of power.

The development of the Personal Area Network (PAN) grew out of a meeting between Professor Mike Hawley's Personal Information Architecture Group and Professor Neil Gershenfeld's Physics and Media Group, both at the MIT Media Laboratory. Professor Hawley's group needed a means to interconnect body-borne information appliances, and Professor Gershenfeld's group had been applying electric field sensing to position measurement. A hand placed between the antennas also affected the capacitance, interfering with the position measurement. This interference caused by a hand proved useful. They realized that, by modulation, the electric field being used for position-sensing data could be sent through a body.

Personal area networks (PAN) in that part of this study actually refer to using a near field electric field to send data across various devices using the body as a medium. It should not be confused with networks formed using Bluetooth technology. Bluetooth is a far field radio technology enabling communication between devices in the ISM band. Bluetooth can in fact be used as an enabler to extend the reach of body networks to other devices and networks.

In PAN, to communicate between two devices using body as a medium there is need a PAN Transmitter and PAN receiver, both battery powered. The PAN transmitter capacitatively couples a small displacement current through the human body to a receiver. The Transmitter need not be in direct contact with the skin. A capacitor is a small device with two metal plates separated from each other that can store an electric charge. Whenever an alternating current flows in a circuit with a capacitor in the circuit, a displacement current flows between the two plates of the capacitor, which are electrically isolated from each other. This displacement current is real and is what is transferred from the PAN device to the body. In a PAN, the transmitter electrode facing the body and the skin act as a capacitor. By modulating the electric current, the displacement current between the transmitter and the body can be modulated. As a result, data can be transferred across to the receiver (by

means of current flowing through the body, which also interacts with the body in the same way). As in any electric circuit there is need a return path for the circuit to be completed; this return path is provided by the "earth ground," which includes all conductors and dielectrics in the environment that are in close proximity to the PAN devices. The earth ground needs to be electrically isolated from the body to prevent shorting of the communication circuit. In figure 2.27 this is schematically expressed.

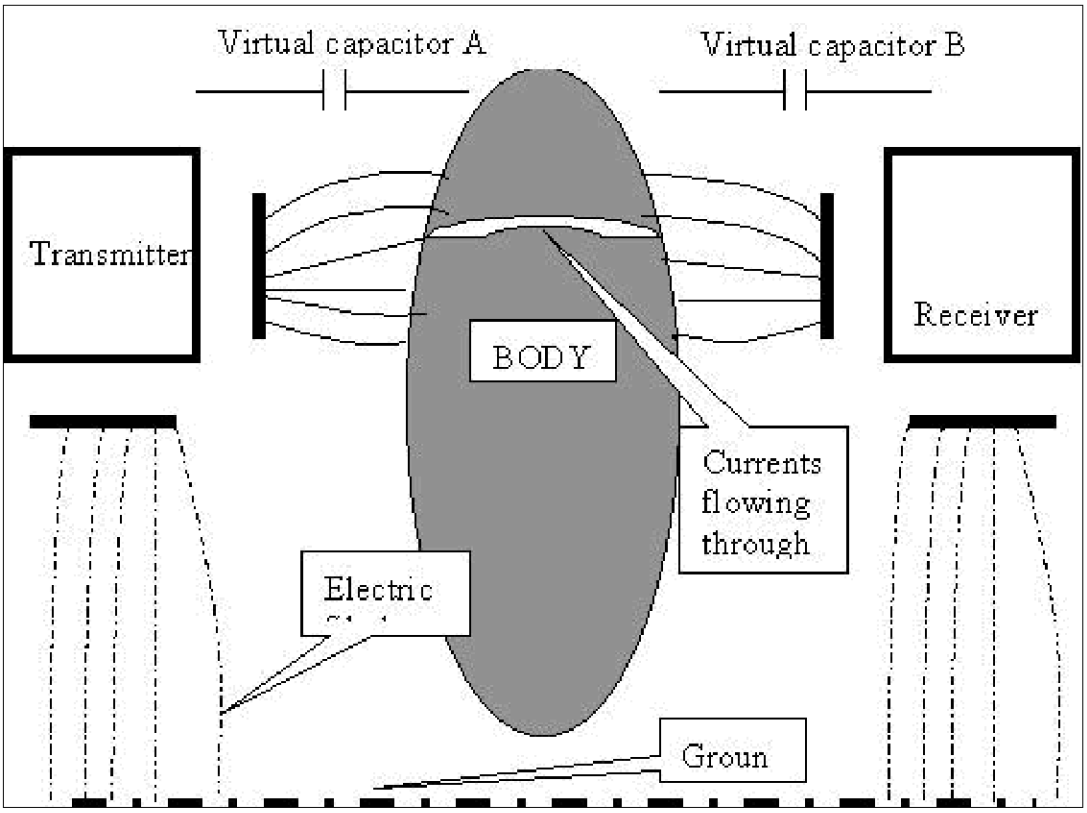

FIGURE 2.27 Basic WPAN [Gupta 2000]

The Transmitter capacitatively couples the electric field to the body. Here the transmitter plate and the body act as a capacitor (A). A normal electric current flows through the body and a part of it reaches the other end where the body and receiver plate act as a capacitor B. Here again, the electric current flows between the body and the receiver as a displacement current. The other electrode of the receiver facing the earth and the ground act as a capacitor C and the ground and the other electrode of the transmitter act as capacitor D. Since the ground is at zero potential (always), electric fields are setup between the ground and the electrodes and thus the return path for the current is formed. Therefore current (and therefore data) can be sent

from the transmitter to the receiver just like any other electric circuit. The transmitters and receivers basically consist of an encoder and/or a decoder followed by the transmitting and receiving circuitry. So, typically the encoder will encode the input data in a suitable form and feed to a transmitting circuitry which converts the data into electric current. At the receiver the electric current is received, amplified, and then converted into data. The decoder then decodes the data into the bits of information that can be processed by the device. The figure 2.28 shows a typical transmitter. A receiver is similar with TRX replaced by a RX and a decoder replacing an encoder.

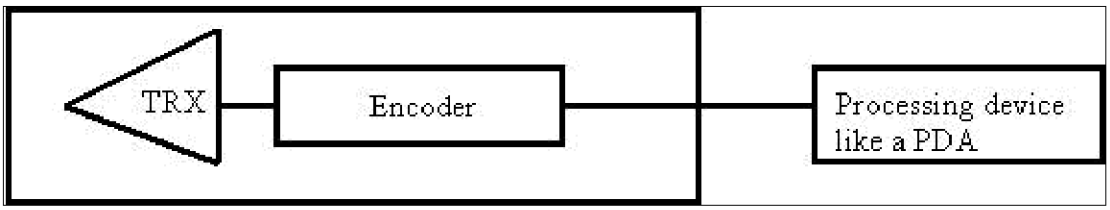

FIGURE 2.28 A typical transmitter [Gupta 2000]

The PAN is based on the seven-layer ISO 7498 network standard of the International Organization for Standardization. Various devices can interact using some form of time multiplexing. Currently time multiplexing is being used. Code division multiplexing could be another exciting alternative.

Electric currents are flowing through the body all the time -nerves, senses and thought patterns all hinge on delicate electric transmissions. The current used in PANs is one-billionth of an amp (i.e. a nanoamp) - lower than the electrical current that flows naturally through our body. Every time combing hair, 1,000 times more electrical charge than a PAN connection is created. The natural salinity of the human body makes it an excellent conductor of electrical current. PAN technology takes advantage of this by creating an external electric field that passes an incredibly tiny current through the body, over which data is carried.

2.5.1 Modulation Strategies

Two modulation strategies have been evaluated for PANs. The on-off keying where data is represented by the presence or absence of electric current. This scheme

is very simple but to improve the signal-to-noise ratio (SNR), higher voltage should be applied. Direct sequence spread spectrum modulates the carrier with a pseudonoise (PN) sequence, producing a broadband transmission much greater than the message bandwidth. Symbol-synchronous PN modulation is used where a message bit one is represented by transmitting the entire PN sequence, and a message bit zero is represented by transmitting the inverted PN sequence. The signal-to-noise performance increases with the length of the PN sequence. For spread spectrum the switches are driven by the PN sequence, and the integrated result, which is the correlation, is compared to two thresholds. If the correlation is greater than a positive threshold, the message bit is one. If the correlation is less than a negative threshold, the message bit is zero. If the correlation is between these thresholds (the dead zone), no message bit is received.

2.5.2 Data Transmission Speeds

Theoretically PAN devices can communicate at 417 Kbits per second, if a robust SNR of 10db is assumed. The PAN transceiver prototype implements a modest 2400 bits-per-second modem. Telephone modems have pushed modulation and digital signal processing techniques to their practical limits. The application of modem telephony techniques to PAN devices may deliver channel capacities of 100 Kbits per second. Data compression will also increase the effective capacity of a PAN communication channel.

2.5.3 Power and Security

The nearfield communication strategy adopted by PANs give them a clear edge over RF based solutions. The extremely small amounts of currents involved make sure that PAN devices would not drain the precious battery. Also using low frequency and low power would ensure that the signal would not propagate very far beyond the body; thus, only devices worn by the user, or by people or devices in direct contact with the user, could detect it. The near-field effect used to make PAN possible has many advantages over other methods of short-range wireless communication. Near-field electrostatic coupling is proportional to electrode surface

area. Far-field transmission efficiency is maximized by matching the impedance of the transmitter to free space, typically by using a half-wavelength antenna. PAN devices 25 to 80 millimeters long would require a carrier of several gigahertz for efficient transmission. Since the energy consumed by electronic components increases with frequency, any increase in the frequency of the carrier beyond that required to contain the information increases energy consumption. Near-field communication can operate at very low frequencies (0.1 to 1 megahertz) that can be generated directly from inexpensive microcontrollers. For example, the prototype PAN transmitter operates at 330 kilohertz (KHz) at 30 volts with a 10-picofarad electrode capacitance, consuming 1.5 milliwatts discharging the electrode capacitance. A majority of this energy is conserved (recycled) by using a resonant inductance-capacitance (LC) tank circuit. Even at low powers, RF waves can be noticed at quite some distance from the source. This is because the RF waves attenuate with distance squared whereas the nearfield electric fields attenuate with distance cubed, providing a distinct advantage as far as security is concerned.

In spite of the short-range, security can still be a problem. Touching a body in PAN could be as good or as bad as tapping into a telephone line, therefore a security method using encryption should be adopted that makes the PAN data look like a stream of random bits to would-be eavesdroppers.

2.5.4 PAN Devices

Any carrying device around can potentially act as a PAN device (the watch, pager, mobile phone, PDA, identification badge, credit card and even the shoe). PAN can help removing the redundancy of IOs and storage capacities mentioned in the beginning. The watch can be a natural choice of a display. The PDA can act as a storage point. The mobile phone/ pager can act as an interface medium to the outside world. With this, not only can the devices become less bulky, but also the cost of owning these devices can also fall dramatically. When getting a paging message on the pager hooked to belt using PAN the pager uploads the message to a watch. The person is alerted by a beep and can read the message from the watch. At the same time pager sends the information to PDA in waist pocket which accesses the address book to find the sender's phone number. The message can also be stored there for

future reference. The PDA sends this information over to mobile phone through the body and the number is already dialed. As a result the mobile doesn't need address books and storage capacity, the pager doesn't need displays. The PDA can act as a server of information and all other devices access it for any information. All these devices form an instant network and talk to each other transparently without any intervention, sharing resources and capabilities and as a result making life much simpler for people.

2.5.5 Issues and Concerns

The biggest issue is security. With the present generation PAN systems, the transfer of data across devices has become quite simple. This increases the risk of transferring data accidentally if person bumps into somebody. It is convenient to transfer the ATM code into the teller machine, but the same should not happen if someone touches the person. So, a lot of work on encryption techniques must be done.

Signal strength and interference play a critical role in deciding the location of the device. The first generation of systems have to be situated at the feet because the signal is strongest there because of the close proximity to the ground. But feet may not be the logical place for credit cards for example. So, a second generation of PAN transceivers need be built that work effectively from wallets and pockets. Also the body must be isolated from ground for the system to work properly.

The next important development that is required is that of monolithic devices. To make carrying of PAN devices feasible, all things like battery, microprocessor and copperplates must be designed as a single compact unit.

Also, to gain wide acceptance, the technology must get out fast from the prototyping stage and cross-industry effort is required to dwell on various higher level issues also (unlike Bluetooth, PAN is an industry initiative (IBM)). Lack of proper application development interfaces, for example, could hinder the acceptance of the technology.

2.5.6 Using The Body to Transfer Power

Recently it was demonstrated that using the body, there cannot only transfer data between devices but power as well. This observation can have great implications. A device can be put into the shoe which can convert the mechanical energy generated while walking into electrical power which can be transmitted through body to some device which can use this to power it's operations.

2.5.7 Application Possibility

Each datum of information received by body has a low but nonzero energy, the excess energy accumulated in receiving and demodulating these bits may itself be used to power circuitry. If a circuit requires only a small amount of current to run, then it is possible by careful design to obtain that current from the data signals coming into the circuit.

It has been shown that under reasonable conditions, an available power of 200mW at 1.0 MHz applied at one hand leads to the recovery of around 20mW of rectified, filtered DC power at one foot.

The scope and effectiveness of PAN, Bluetooth, and IrDA depends on the context and the application. Where high speed inter-device communication is required, PAN can't match the speeds provided by Bluetooth or IrDA.

The success of any technology depends not on what it promises to achieve but on what it is actually able to deliver. The same is true for PANs also. As with other communication and data systems, in PAN there is a trade-off among access, convenience, and security. The technology is in prototyping stage today and most of the work has been done in the lower layers aiming to make transmissions over body work efficiently and reliably. Lots of work needs to be done at the higher layers relating to issues like security, authentication and reliability. Also, The sensitivity and bit rate must be increased in order to realize a watch-sized PAN transceiver. The trade-off among cost, speed, size, power, and operating range must be further studied and quantified in order to engineer practical PAN devices. These devices must shrink in size even further and provide a good development framework to catch the imaginations of developers.

The biggest advantage in support of PANs is that it opens a whole new front in networking. Body networks seem to a very natural evolution in the networking world where wide area networks, metropolitan area networks, local area networks and short range interdevice networks (piconets) using Bluetooth and IrDA. The focus of body networks is different and they are the latest entrants in this field and are (until now) not competing with any other such solutions.

Chapter 3

IEEE 802.11 STANDARD

The lack of standards has been a significant problem with wireless networking at the beginning, but the Institute for Electrical and Electronic Engineers (IEEE) developed the first internationally recognized wireless LAN standard: IEEE 802.11 [14].

There are two main types of standards: official and public. When an *official standard* is published it is open to the public, but it is controlled by an official standards organization, such as IEEE. Government or industry organizations normally sponsor official standards groups. Official standards organizations generally supply coordination at both the international and domestic level.

A *public standard* is similar to an official standard, except it is controlled by a private organization, such as the Wireless LAN Interoperability Forum. Public standards, often called *de facto standards,* are common practices that have not been produced or accepted by an official standards organization. These standards, such as TCP/IP, are the result of widespread proliferation. In some cases, public standards, such as Ethernet, eventually pass through standards organizations and become official standards.

3.1 Introduction to the IEEE Standard

The 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable, and mobile stations moving within a local area. 802.11 standard has the features as:

- Support of asynchronous and time-bounded delivery service
- Continuity of service within extended area by a distribution system, like Ethernet
- Accommodation of transmission rates of 1 and 2 Mbps
- Support of most market applications

• Multicast (including broadcast) services

• Network management services

• Registration and authentication services

The standard has following target environments:

• Inside buildings, such as offices, banks, shops, malls, hospitals, manufacturing plants, and residences

• Outdoor areas, such as parking lots, campuses, building complexes, and outdoor plants

The 802.11 standard clarifies the significant differences between wireless and wired LANs:

• *Power management:* Because almost all wireless LAN NICs are available in PCMCIA Type II format, portable and mobile handheld computing equipment can be easily adopted with wireless LAN connectivity. The problem is that these devices must rely on batteries to power the electronics within them and the addition of a wireless LAN NIC to them can cause rapid decrease in batteries life.

The 802.11 Working Group investigated many solutions to conserve battery power and they found techniques enabling wireless NICs to switch to lower-power standby modes periodically while there is no transmission. This results with longer battery life. The MAC Layer implements power-management functions by putting the radio to sleep when no transmission activity occurs for some specific or user-definable time period. The problem, however, is that a sleeping station can miss critical data transmissions. 802.11 solves this problem by incorporating buffers to queue messages. The standard calls for sleeping stations to awaken periodically and retrieve any applicable messages.

• *Bandwidth:* The ISM spread spectrum bands do not offer a great deal of bandwidth, keeping data rates lower than desired for some applications. The 802.11 Working Group dealt with methods to compress data. These studies enabled the best use of available bandwidth. They also do efforts to increase the data rate of 802.11 to accommodate the growing need for exchanging larger and larger files.

• *Security:* Generally wireless LANs transmit signals over much larger areas than that of wired media, such as twisted-pair, coaxial, and optical fiber cable. In

terms of privacy, therefore, wireless LANs have a much larger area to protect. To employ security, the 802.11 Working Group coordinated their work with the IEEE 802.10 Standards Committee responsible for developing security mechanisms for all 802 series LANs.

• *Addressing:* Because of its natural characteristics the topology of a wireless network is dynamic. Therefore, the destination address does not always correspond to the destination's location. This raises a problem when routing packets through the network to the intended destination. As a result there is a need for using a TCP/IP-based protocol, such as Mobile IP, to accommodate mobile stations.

To satisfy the interoperability with existing standards, the 802.11 Working Group developed the standard to be compatible with other existing 802 standards, such as the following:

- IEEE 802 : Functional Requirements
- IEEE 802.2 : MAC Service Definition
- IEEE 802.1-A : Overview and Architecture
- IEEE 802.1-B : LAN/MAN Management
- IEEE 802.1-D : Transparent Bridges
- IEEE 802.1-F : Guidelines for the Development of Layer Management Standards
- IEEE 802.10 : Secure Data Exchange

3.2 IEEE 802.11 Topology

The IEEE 802.11 topology consists of components, interacting to provide a wireless LAN that enables station mobility transparent to higher protocol layers, such as the LLC. A station is any device that contains functionality of the 802.11 protocol (that is, MAC Layer, PHY Layer, and interface to a wireless medium). The functions of the 802.11 standard reside physically in a radio NIC, the software interface that drives the NIC, and access point. The 802.11 standard supports the following two topologies:

- Independent Basic Service Set (IBSS) networks
- Extended Service Set (ESS) networks

These networks utilize a basic building block the 802.11 standard refers to as a BSS, providing a coverage area whereby stations of the BSS remain fully connected. A station is free to move within the BSS, but it can no longer communicate directly with other stations if it leaves the BSS.

3.2.1 Independent Basic Service Set (IBSS) Networks

An IBSS is a stand-alone BSS that has no backbone infrastructure and consists of at least two wireless stations (see figure 3.1). This type of network is often referred to as an *ad hoc network* because it can be constructed quickly without much planning.

The ad hoc wireless network will satisfy most needs of users occupying a smaller area, such as a single room, a sales floor, or a hospital wing.

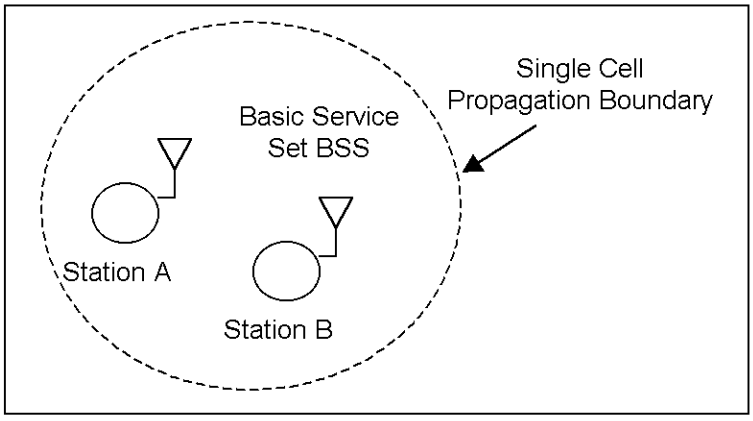

FIGURE 3.1 An independent BSS [Geiger 1999]

3.2.2 Extended Service Set (ESS) Networks

For requirements exceeding the range limitations of an independent BSS, 802.11 defines an Extended Service Set (ESS) LAN, as illustrated in figure 3.2. This type of configuration satisfies the needs of large-coverage networks of arbitrary size and complexity. An Extended Service Set 802.11 wireless LAN consists of multiple cells interconnected by access points and a distribution system, such as Ethernet.

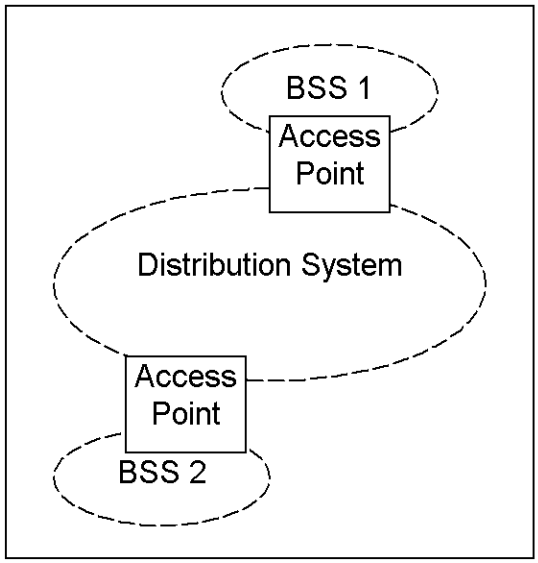

FIGURE 3.2 An Extended Service Set (ESS) [Geiger 1999]

The 802.11 standard recognizes the following mobility types:

• *No-transition:* This type of mobility refers to stations that do not move and those that are moving within a local BSS.

• *BSS-transition:* This type of mobility refers to stations that move from one BSS in one ESS to another BSS within the same ESS.

• *ESS-transition:* This type of mobility refers to stations that move from a BSS in one ESS to a BSS in a different ESS.

The 802.11 standard clearly supports the no-transition and BSS-transition mobility types. The standard, however, does not guarantee that a connection will continue when making an ESS-transition.

The 802.11 standard defines the *distribution system* as an element that interconnects BSSs within the ESS via access points. The distribution system supports the 802.11 mobility types by providing logical services necessary to handle address-to-destination mapping and seamless integration of multiple BSSs. An *access point* is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC Layer.

Within the ESS, the 802.11 standard accommodates the following physical configuration of BSSs:

• *BSSs that partially overlap:* This type of configuration provides contiguous coverage within a defined area, which is best if the application cannot tolerate a disruption of network service.

• *BSSs that are physically disjointed:* For this case, the configuration does not provide contiguous coverage. 802.11 does not specify a limit to the distance between BSSs.

• *BSSs that are physically collocated:* This may be necessary to provide a redundant or higher-performing network.

The 802.11 standard does not constrain the composition of the distribution system; therefore, it may be 802-compliant or some nonstandard network. If data frames need transmission to and from a non-IEEE 802.11 LAN, these frames enter and exit through a logical point called *a. portal.* The portal provides logical integration between existing wired LANs and 802.11 LANs. When the distribution system is constructed with 802-type components, such as 802.3 (Ethernet) or 802.5 (token ring), the portal and the access point become one and the same.

3.3 IEEE 802.11 Logical Architecture

A topology provides a means of explaining necessary physical components of a network, but the *logical architecture* defines the network's operation. As figure 3.3 illustrates, the logical architecture of the 802.11 standard that applies to each station consists of a single MAC and one of multiple PHYs. A single 802.11 MAC Layer supports three separate PHYs: frequency hopping spread spectrum, direct sequence spread spectrum, and infrared light.

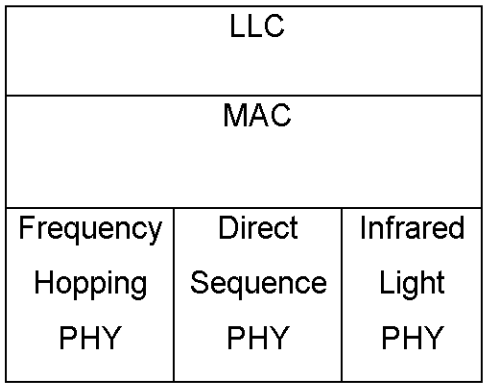

FIGURE 3.3 A basic IEEE 802.11 Logical Architecture [Geiger 1999]

3.3.1 IEEE 802.11 and 802.11b Technology

In September 1999 IEEE ratified the 802.11b "High Rate" amendment to the standard, which added two higher speeds (5.5 and 11 Mbps) to 802.11 [23].

With 802.11b WLANs, mobile users can get Ethernet levels of performance, throughput, and availability. The standards-based technology allows administrators to build networks that seamlessly combine more than one LAN technology to best fit their business and user needs.

Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO model, the physical layer and data link layer (figure 3.4). Any LAN application, network operating system, or protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

The basic architecture, features, and services of 802.11b are defined by the original 802.11 standard. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity.

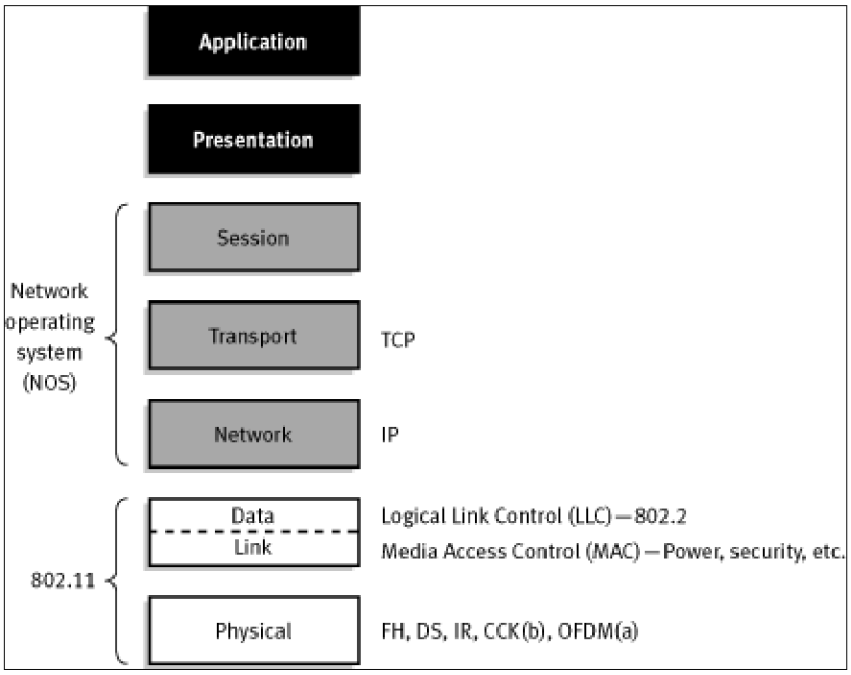

FIGURE 3.4 802.11 and the ISO model [Kawatra]

The original 802.11 DSSS standard specifies an 11-bit chipping—called a *Barker sequence*—to encode all data sent over the air [38]. Each 11-chip sequence

represents a single data bit (1 or 0), and is converted to a waveform, called a *symbol*, that can be sent over the air. These symbols are transmitted at a 1 MSps (1 million symbols per second) *symbol rate* using a technique called *Binary Phase Shift Keying (BPSK)*. In the case of 2 Mbps, a more sophisticated implementation called *Quadrature Phase Shift Keying (QPSK)* is used; it doubles the data rate available in BPSK, via improved efficiency in the use of the radio bandwidth.

To increase the data rate in the 802.11b standard, advanced coding techniques are employed. Rather than the two 11-bit Barker sequences, 802.11b specifies Complementary Code Keying (CCK), which consists of a set of 64 eight-bit code words. As a set, these code words have unique mathematical properties that allow them to be correctly distinguished from one another by a receiver even in the presence of substantial noise and multipath interference (e.g., interference caused by receiving multiple radio reflections within a building). The 5.5 Mbps rate uses CCK to encode 4 bits per carrier, while the 11 Mbps rate encodes 8 bits per carrier. Both speeds use QPSK as the modulation technique and signal at 1.375 MSps. This is how the higher data rates are obtained. Table 3.1 shows the differences.

TABLE 3.1. 802.11b Data Rate Specifications [38]

Data Rate	**Code Length**	**Modulation**	**Symbol Rate**	**Bits/Symbol**
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

To support very noisy environments as well as extended range, 802.11b WLANs use *dynamic rate shifting*, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. Ideally, users connect at the full 11 Mbps rate. However when devices move beyond the optimal range for 11 Mbps operation, or if substantial interference is present, 802.11b devices will transmit at lower speeds, falling back to 5.5, 2, and 1 Mbps. Likewise, if the device moves back within the range of a higher-speed transmission, the connection will

automatically speed up again. Rate shifting is a physical-layer mechanism transparent to the user and the upper layers of the protocol stack.

3.3.1.1 802.11 Operating Modes

802.11 defines two pieces of equipment, a wireless *station*, which is usually a PC equipped with a wireless network interface card (NIC), and an *access point (AP)*, which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface (e.g., 802.3), and bridging software conforming to the 802.1d bridging standard. The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network. Wireless end stations can be 802.11 PC Card, PCI, or ISA NICs, or embedded solutions in non-PC clients (such as an 802.11-based telephone handset).

The 802.11 standard defines two modes: *infrastructure* mode and *ad hoc* mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS) and an *Extended Service Set (ESS)* (figure 3.2) is a set of two or more BSSs forming a single subnetwork as described earlier. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network (figure 3.5). This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).

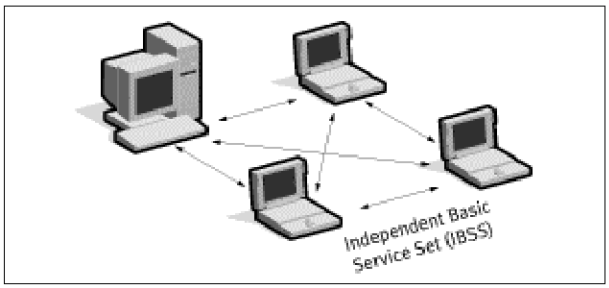

FIGURE 3.5 Ad Hoc mode [Kawatra]

3.3.1.2 IEEE 802.11 Physical Layer

The three physical layers originally defined in 802.11 included two spread-spectrum radio techniques and a diffuse infrared specification. The final standard specifies 2.4 GHz spread spectrum ISM bands for both the direct sequence and frequency hopping PHYs because this band is available license free in most parts of the world [14].

The direct sequence Physical Layer specifies two data rates:

- 2 Mbps using Differential Quaternary Phase Shift Keying (DQPSK) modulation
- 1 Mbps using Differential Binary Phase Shift Keying (DBPSK)

In contrast to direct sequence, the 802.11-based frequency hopping PHY uses radios to send data signals by hopping from one frequency to another, transmitting a few bits on each frequency before shifting to a different one. Frequency hopping systems tend to be less costly to implement and do not consume as much power as their direct sequence counterpart, making them more suitable for portable applications. However, frequency hopping is much less tolerant of multiple-path and other interference sources. The system must retransmit data if it becomes corrupted on one of the hop sequence frequencies.

Using the frequency hopping technique, the 2.4 GHz band is divided into 75 one-MHz subchannels. The sender and receiver agree on a hopping pattern, and data is sent over a sequence of the subchannels. Each conversation within the 802.11 network occurs over a different hopping pattern, and the patterns are designed to minimize the chance of two senders using the same subchannel simultaneously.

FHSS techniques allow for a relatively simple radio design, but are limited to speeds of no higher than 2 Mbps. This limitation is driven primarily by FCC regulations that restrict subchannel bandwidth to 1 MHz. These regulations force FHSS systems to spread their usage across the entire 2.4 GHz band, meaning they must hop often, which leads to a high amount of hopping overhead.

In contrast, the direct sequence signaling technique divides the 2.4 GHz band into 14 channels. In US, only 11 channels are available. For multiple channels to coexist in the same location, they should be 25 MHz apart to avoid interference. This means, that at most 3 channels can coexist in one location. Data is sent across one of these channels without hopping to other channels. To compensate for noise on a given channel, a technique called "chipping" is used. Each bit of user data is converted into a series of redundant bit patterns called "chips." The inherent redundancy of each chip combined with spreading the signal across the channel provides for a form of error checking and correction; even if part of the signal is damaged, it can still be recovered in many cases, minimizing the need for retransmissions.

The infrared Physical Layer describes a modulation type that operates in the 850 to 950 nM band for small equipment and low-speed applications. The basic data rate of this infrared medium is 1 Mbps using 16-PPM (pulse position modulation) and an enhanced rate of 2 Mbps using 4-PPM. Peak power of infrared-based devices is limited to a peak power of 2 watts.

3.3.1.3 802.11b Enhancements to the PHY Layer

The key contribution of the 802.11b addition to the wireless LAN standard was to standardize the physical layer support of two new speeds, 5.5 Mbps and 11 Mbps. To accomplish this, DSSS had to be selected as the sole physical layer technique for the standard since, as noted above, frequency hopping cannot support the higher speeds without violating current FCC regulations. The implication is that 802.11b systems will interoperate with 1 Mbps and 2 Mbps 802.11 DSSS systems, but will not work with 1 Mbps and 2 Mbps 802.11 FHSS systems.

To support very noisy environments as well as extended range, 802.11b WLANs use dynamic rate shifting, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. Ideally, users connect at the full 11 Mbps rate. However when devices move beyond the optimal range for 11 Mbps operation, or if substantial interference is present, 802.11b devices will transmit at lower speeds, falling back to 5.5, 2, and 1 Mbps. Likewise, if the device moves back within the range of a higher-speed transmission, the connection will automatically speed up again. Rate shifting is a physical-layer mechanism transparent to the user and the upper layers of the protocol stack.

3.3.1.4 IEEE 802.11 MAC Layer

The data link layer within 802.11 consists of two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLANs.

The main function of the MAC Layer is to provide access control functions (such as addressing, access coordination, frame check sequence generation and checking, and LLC PDU delimiting) for shared-medium PHYs in support of the LLC Layer.

The 802.11 MAC is very similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it. For 802.3 Ethernet LANs, the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol regulates how Ethernet stations establish access to the wire and how they detect and handle collisions that occur when two or more devices try to simultaneously communicate over the LAN. In an 802.11 WLAN, collision detection is not possible due to what is known as the "near/far" problem: to detect a collision, a station must be able to transmit and listen at the same time, but in radio systems the transmission drowns out the ability of the station to "hear" a collision.

To account for this difference, 802.11 uses a slightly modified protocol known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or the Distributed Coordination Function (DCF). CSMA/CA attempts to avoid collisions by

using explicit packet acknowledgment (ACK), which means an ACK packet is sent by the receiving station to confirm that the data packet arrived intact.

CSMA/CA works as follows: A station wishing to transmit senses the air, and, if no activity is detected, the station waits an additional, randomly selected period of time and then transmits if the medium is still free. If the packet is received intact, the receiving station issues an ACK frame that, once successfully received by the sender, completes the process. If the ACK frame is not detected by the sending station, either because the original data packet was not received intact or the ACK was not received intact, a collision is assumed to have occurred and the data packet is transmitted again after waiting another random amount of time.

CSMA/CA thus provides a way of sharing access over the air. This explicit ACK mechanism also handles interference and other radio-related problems very effectively. However, it does add some overhead to 802.11 that 802.3 does not have, so that an 802.11 LAN will always have slower performance than an equivalent Ethernet LAN.

Frame receipt acknowledgment provides one good example of differences between the 802.11 MAC and the wired Ethernet MAC, along with the advantage the difference affords in a wireless system [38]. Most LANs rely on a receiving node to send an acknowledge message to verify that it received an incoming data frame. In Ethernet and most wired LANs, however, the acknowledge message is handled above the MAC layer.

The 802.11 standard specifies that the MAC layer handle acknowledgment and resend lost frames resulting in more efficient usage of the available bandwidth and quicker acknowledgment. The 802.11 frame format relies on an interframe spacing of 50 ms. The standard requires that the receiving station send an acknowledgment 10 ms after the end of each frame, providing the CRC check is correct. The 10-ms limit ensures that the receiving station can take immediate control of the airwaves rather than competing with other nodes for medium access, as would be required if it waited past the 50-ms interframe spacing. LANs that handle acknowledgment in layers above the MAC canít meet the strict timing requirements and, therefore, essentially compete for medium access and send a standard frame to convey each acknowledgment. The MAC-layer implementation eliminates the latencies of

medium access and allows the acknowledgment to use some of the interframe spacing time period in which no other activity would occur in any case.

Another MAC-layer problem specific to wireless is the "hidden node" issue, in which two stations on opposite sides of an access point can both "hear" activity from an access point, but not from each other, usually due to distance or an obstruction [23]. To solve this problem, 802.11 specifies an optional Request to Send/Clear to Send (RTS/CTS) protocol at the MAC layer. When this feature is in use, a sending station transmits an RTS and waits for the access point to reply with a CTS. Since all stations in the network can hear the access point, the CTS causes them to delay any intended transmissions, allowing the sending station to transmit and receive a packet acknowledgment without any chance of collision. Since RTS/CTS adds additional overhead to the network by temporarily reserving the medium, it is typically used only on the largest-sized packets, for which retransmission would be expensive from a bandwidth standpoint.

Finally, the 802.11 MAC layer provides for two other robustness features: CRC checksum and packet fragmentation. Each packet has a CRC checksum calculated and attached to ensure that the data was not corrupted in transit. This is different from Ethernet, where higher-level protocols such as TCP handle error checking. Packet fragmentation allows large packets to be broken into smaller units when sent over the air, which is useful in very congested environments or when interference is a factor, since larger packets have a better chance of being corrupted. This technique reduces the need for retransmission in many cases and thus improves overall wireless network performance. The MAC layer is responsible for reassembling fragments received, rendering the process transparent to higher-level protocols.

3.3.1.4.1 Association, Cellular Architectures, and Roaming

The 802.11 MAC layer is responsible for how a client associates with an access point. When an 802.11 client enters the range of one or more APs, it chooses an access point to associate with (also called joining a Basic Service Set), based on signal strength and observed packet error rates. Once accepted by the access point, the client tunes to the radio channel to which the access point is set. Periodically it surveys all 802.11 channels in order to assess whether a different access point would

provide it with better performance characteristics. If it determines that this is the case, it reassociates with the new access point, tuning to the radio channel to which that access point is set (figure 3.6).

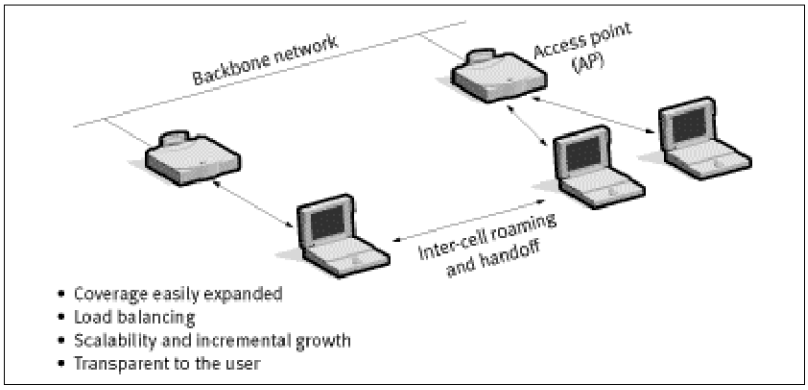

FIGURE 3.6 Access point roaming [Kawatra]

Reassociation usually occurs because the wireless station has physically moved away from the original access point, causing the signal to weaken. In other cases, reassociation occurs due to a change in radio characteristics in the building, or due simply to high network traffic on the original access point. In the latter case this function is known as "load balancing," since its primary function is to distribute the total WLAN load most efficiently across the available wireless infrastructure.

This process of dynamically associating and reassociating with APs allows network managers to set up WLANs with very broad coverage by creating a series of overlapping 802.11b cells throughout a building or across a campus. To be successful, the IT manager ideally will employ "channel reuse," taking care to set up each access point on an 802.11 DSSS channel that does not overlap with a channel used by a neighboring access point (figure 3.7). As noted above, while there are 14 partially overlapping channels specified in 802.11 DSSS, there are only three channels that do not overlap at all, and these are the best to use for multicell coverage. If two APs are in range of one another and are set to the same or partially overlapping channels, they may cause some interference for one another, thus lowering the total available bandwidth in the area of overlap.

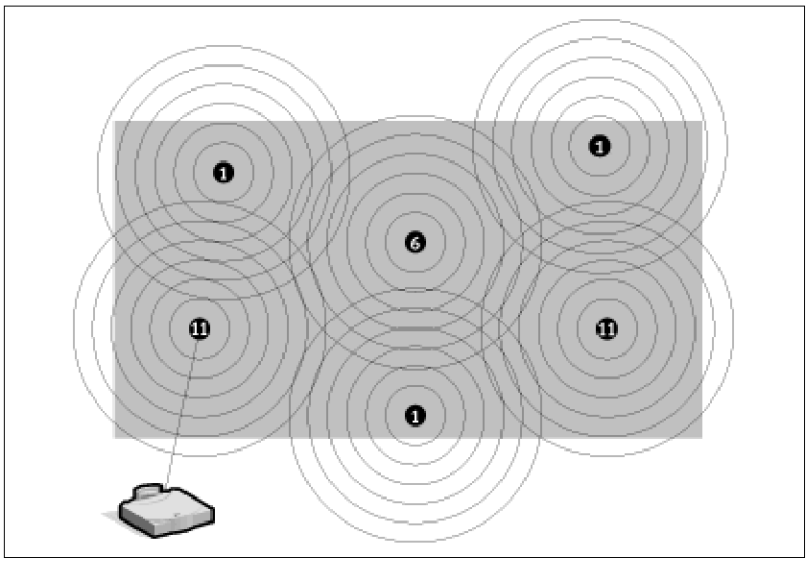

FIGURE 3.7 Unlimited roaming [Kawatra]

3.3.1.4.2 Support for Time-Bounded Data

Time-bounded data such as voice and video is supported in the 802.11 MAC specification through the Point Coordination Function (PCF). As opposed to the DCF, where control is distributed to all stations, in PCF mode a single access point controls access to the media. If a BSS is set up with PCF enabled, time is spliced between the system being in PCF mode and in DCF (CSMA/CA) mode. During the periods when the system is in PCF mode, the access point will poll each station for data, and after a given time move on to the next station. No station is allowed to transmit unless it is polled, and stations receive data from the access point only when they are polled. Since PCF gives every station a turn to transmit in a predetermined fashion, a maximum latency is guaranteed. A downside to PCF is that it is not particularly scalable, in that a single point needs to have control of media access and must poll all stations, which can be ineffective in large networks.

3.3.1.4.3 Power Management

In addition to controlling media access, the 802.11 HR MAC supports power conservation to extend the battery life of portable devices. The standard supports two power-utilization modes, called Continuous Aware Mode and Power Save Polling Mode. In the former, the radio is always on and drawing power, whereas in the latter,

the radio is "dozing," with the access point queuing any data for it. The client radio will wake up periodically in time to receive regular beacon signals from the access point. The beacon includes information regarding which stations have traffic waiting for them, and the client can thus awake upon beacon notification and receive its data, returning to sleep afterward.

3.3.1.4.4 Security

802.11 provides for both MAC layer (OSI Layer 2) access control and encryption mechanisms, which are known as Wired Equivalent Privacy (WEP), with the objective of providing wireless LANs with security equivalent to their wired counterparts. For the access control, the ESSID (also known as a WLAN Service Area ID) is programmed into each access point and is required knowledge in order for a wireless client to associate with an access point. In addition, there is provision for a table of MAC addresses called an Access Control List to be included in the access point, restricting access to clients whose MAC addresses are on the list.

For data encryption, the standard provides for optional encryption using a 40-bit shared-key RC4 PRNG algorithm from RSA Data Security. All data sent and received while the end station and access point are associated can be encrypted using this key. In addition, when encryption is in use, the access point will issue an encrypted challenge packet to any client attempting to associate with it. The client must use its key to encrypt the correct response in order to authenticate itself and gain network access.

Beyond Layer 2, 802.11 HR WLANs support the same security standards supported by other 802 LANs for access control (such as network operating system logins) and encryption (such as IPSec or application-level encryption). These higher-layer technologies can be used to create end-to-end secure networks encompassing both wired LAN and WLAN components, with the wireless piece of the network gaining unique additional security from the 802.11 feature set.

3.4 IEEE 802.11 Services

The LLC Layer is responsible for sending MAC service data units (MSDUs) between two entities on the network. The IEEE 802.11 standard defines services that provide this function of LLC layer. These services are considered mainly in two categories.

3.4.1 Station Services

A station may be found any wireless part of a network. Moreover, all access points apply station services.

3.4.1.1 Authentication

IEEE 802.11 standard provides necessary authentication services to control LAN access by giving the same security level of a wired line. All 802.11 stations, no matter if they are part of an independent BSS or ESS network, must obey the authentication service before establishing a connection with another communicating station.

The IEEE 802.11 standard defines mainly two authentication services:

• *Open system authentication:* This is very simple, two step, 802.11 default authentication process. First of all, the authenticating station sends an authentication management frame containing the sending station's identity an then the receiving station sends back a frame alerting whether it recognizes the identity of the authenticating one.

• *Shared key authentication:* This type of authentication assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key.

3.4.1.2 Deauthentication

When a station wishes to *disassociate* with another station, it invokes the *deauthentication* service. Deauthentication is a notification process that cannot be refused. Deauthenticating stations perform the process by sending an authentication management frame (or group of frames to multiple stations) to *advise* the termination of authentication.

3.4.1.3 Privacy

Because it is an open system, all elements in a wireless network may recognize the data traffic within the range of the network. Again there is a need for to apply security standards of a wired network and the privacy service, applying to all data frames and some authentication management frames, is based on the 802.11 *Wired Equivalent Privacy (WEP)* algorithm that significantly reduces risks if someone eavesdrops on the network. This algorithm performs encryption of messages, as shown in figure 3.8. The Wired Equivalent Privacy (WEP) algorithm produces ciphertext, keeping eavesdroppers from "listening in" on data transmissions. The WEP protects RF data transmissions using a 64-bit seed key and the RC4 encryption algorithm. When enabled, WEC only protects the data packet information. Physical Layer headers are left unencrypted so that all stations can properly receive control information for managing the network.

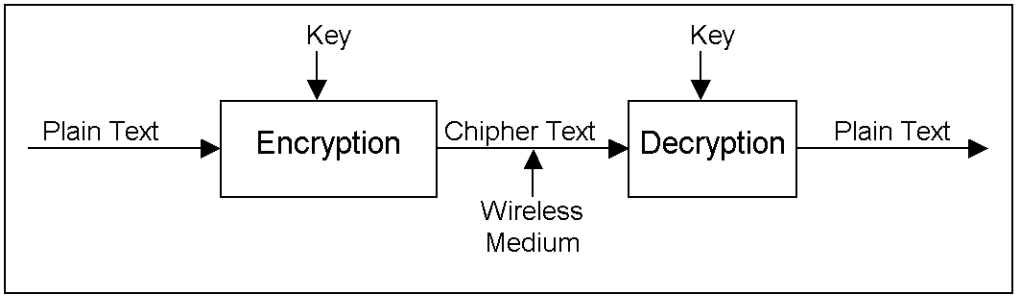

FIGURE 3.8 Wired Equivalent Privacy (WEP) algorithm [Geiger 1999]

3.4.2 Distribution System Services

These services, as defined by 802.11, provide functionality across a distribution system.

3.4.2.1 Association

Before sending information throughout the network, each station must firstly invoke the association service with an access point. The association maps a station to the distribution system by an access point. Each station can associate with only one single access point, but each access point can associate with multiple stations. Association is also a first step to providing the capability for a station to be mobile between BSSs.

3.4.2.2 Disassociation

A station or access point may invoke the *disassociation service* to terminate an existing association. This service is a notification; therefore, no one may refuse termination. Stations should disassociate when leaving the network. An access point, for example, may disassociate all its stations if being removed for maintenance.

3.4.2.3 Distribution

A station uses the *distribution service* every time it sends MAC frames across a distribution system. The 802.11 standard does not specify how the distribution system delivers the data. The distribution service provides the distribution system with only enough information to determine the proper destination BSS.

3.4.2.4 Integration

The *integration service* enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN. The integration function performs all required media or address space translations. The details of an

integration function depend on the distribution system implementation and also these are not business of the 802.11 standard.

3.4.2.5 Reassociation

The *reassociation service* enables a station to change its current state of association. Reassociation provides additional functionality to support BSS-transition mobility for associated stations. The reassociation service enables a station to change its association from one access point to other one. This function always maintains the distribution system informed of the current mapping situations of access points and stations while they are moving from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an already performed association while association continues between the station and the same access point. The mobile station always initiates the reassociation service.

3.4.3 Station States and Corresponding Frame Types

The state existing between a source and destination station governs which IEEE 802.11 frame types the two stations can exchange.

- Class 1 Frames
    - Control Frames
        - Request to send (RTS)
        - Clear to send (CTS)
        - Acknowledgment (ACK)
        - Contention-free (CF)
    - Management Frames
        - Probe request/response
        - Beacon
        - Authentication
        - Deauthentication
        - Announcement traffic indication message (ATIM)
    - Data Frames
- Class 2 Frames

- Management Frames
    - Association request/response
    - Reassociation request/response
    - Disassociation
- Class 3 Frames
    - Data Frames
    - Management Frames
        - Deauthentication
    - Control Frames
        - Power Save Poll

Each station maintains the following two state variables to keep track of station state:

- *Authentication state:* Has values of either unauthenticated and authenticated
- *Association state:* Has values of either unassociated and associated

3.5 Benefits of 802.11 Standard

3.5.1 Appliance Interoperability

Being compatible with the IEEE 802.11 standard makes interoperability possible between various manufacturer devices and the chosen wireless network type. Appliance interoperability avoids the dependence on a single vendor for appliances. Without a standard, for example, a company having a non-standard proprietary type of network would be dependent on the appliances that operate only on that network.

3.5.2 Fast Product Production

The 802.11 standard is a well-tested design that the developers can produce devices without spending time on problems underlying technology. Because standard-forming group has study on all kind of situation to solve the problems of

technology the manufacturers need little time to learn and implement the applicable technology.

3.5.3 Stable Future Migration

Appropriateness with standards provides the protection of investments and also prevents the system being completely unusable in the future when they will be replaced.

3.5.4 Price Reductions

High costs have always caused a barrier on improvements of the wireless LAN industry; however, prices should drop significantly as more vendors and end users comply with 802.11. One of the reasons for lower prices is that vendors will no longer need to develop and support lower-quantity proprietary subcomponents, cutting design, manufacturing, and support costs.

3.5.5 Providing Interoperability

One part of the company, for example, may purchase a wireless network system from one vendor, and then another part of the company may buy a different wireless network. If there isn't a standard, noninteroperable systems will appear within the company, making it very difficult for MIS personnel to plan and support compatible systems.

3.6 IEEE 802.11a Standard

The 802.11b standard was designed to operate in the 2.4-GHz ISM (Industrial, Scientific and Medical) band using direct-sequence spread-spectrum technology. The 802.11a (IEEE Task Group A, part of the IEEE 802.11 Working Group) standard, on the other hand, was designed to operate in the more recently allocated 5-GHz Unlicensed National Information Infrastructure (UNII) band. And unlike 802.11b, the 802.11a standard departs from the traditional spread-spectrum

technology, instead using a frequency division multiplexing scheme that's intended to be friendlier to office environments [10]. This standard specifies the use of Orthogonal Frequency Division Multiplexing (OFDM) for data transmission at rates up to 54 Mbps. This standard is widely accepted by most because the specification of the medium access control (MAC) layer is the same as the one used for 802.11b can also be used for 802.11a [50].

The 802.11a standard, which supports data rates of up to 54 Mbps, is the Fast Ethernet analog to 802.11b, which supports data rates of up to 11 Mbps. Like Ethernet and Fast Ethernet, 802.11b and 802.11a use an identical MAC (Media Access Control). However, while Fast Ethernet uses the same physical-layer encoding scheme as Ethernet (only faster), 802.11a uses an entirely different encoding scheme, OFDM.

The 802.11a standard is designed to operate in the 5-GHz frequency range. Specifically, the FCC has allocated 300 MHz of spectrum for unlicensed operation in the 5-GHz block, 200 MHz of which is at 5.15 MHz to 5.35 MHz, with the other 100 MHz at 5.725 MHz to 5.825 MHz. The spectrum is split into three working "domains". The first 100 MHz in the lower section is restricted to a maximum power output of 50 mW (milliwatts). The second 100 MHz has a more generous 250-mW power budget, while the top 100 MHz is delegated for outdoor applications, with a maximum of 1-watt power output. In contrast, 802.11b cards can radiate as much as 1 watt in the United States. However, most modern cards radiate only a fraction (30 mW) of the maximum available power for reasons of battery conservation and heat dissipation.

Although segmented, the total bandwidth available for IEEE 802.11a applications is almost four times that of the ISM band; the ISM band offers only 83 MHz of spectrum in the 2.4 GHz range, while the newly allocated UNII band offers 300 MHz. The 802.11b spectrum is plagued by saturation from wireless phones, microwave ovens and other emerging wireless technologies, such as Bluetooth. In contrast, 802.11a spectrum is relatively free of interference, at least for now. Only time will tell whether the 5-GHz band will become just as crowded as the 2.4-GHz band.

The 802.11a standard gains some of its performance from the higher frequencies at which it operates. The laws of information theory tie frequency,

radiated power and distance together in an inverse relationship. Thus, moving up to the 5-GHz spectrum from 2.4 GHz will lead to shorter distances, given the same radiated power and encoding scheme. In addition, the encoding mechanism used to convert data into analog radio waves can encode one or more bits per radio cycle (hertz). By rotating and manipulating the radio signal, vendors can encode more information in the same time slice. To ensure that the remote host can decode these more complex radio signals, more power must be used at the source to compensate for signal distortion and fade. The 802.11a technology overcomes some of the distance loss by increasing the EIRP to the maximum 50 mW.

However, power alone is not enough to maintain 802.11b-like distances in an 802.11a environment. To compensate, vendors specified and designed a new physical-layer encoding technology that departs from the traditional direct-sequence technology being deployed today. This technology is called Coded OFDM (COFDM). In addition, to dramatically increase throughput, 802.11a proponents had to solve a major challenge of indoor radio frequency [1]. They had to develop a way to resolve the problem of delay spread in the current 2.4-GHz, single-carrier, delay-spread system. Delay spread is caused by the echoing of transmitted radio frequency. The delay spread must be less than the symbol rate, or the rate at which data is encoded for transmission. If not, some of the delayed signal spreads into the next symbol transmission. This can put a ceiling on the maximum bit rate that can be sustained. With current bit-rate technology, this ceiling tends to be around 10M to 20M bit/sec. The 802.11a standard cleverly solves this challenge by Coded Orthogonal Frequency Division Multiplexing.

COFDM breaks the ceiling of the data bit rate by 1) sending data in a massively parallel fashion, and 2) slowing the symbol rate down so each symbol transmission is much longer than the typical delay spread. A guard interval (sometimes called a cyclic prefix) is inserted at the beginning of the symbol transmission to let all delayed signals "settle" before the baseband processor demodulates the data.

COFDM slows the symbol rate while packing many bits in each symbol transmission, making the symbol rate substantially slower than the data bit rate. It maps the data signal to be transmitted into several lower-speed signals, or subcarriers, which then are modulated individually and transmitted in parallel.

COFDM also uses coding to allow for recovery of errors and to add more interference rejection by spreading information across all carriers. Interferers may jam individual carriers and the data will still get through. The COFDM physical layer allows greater scalability in delivering data over the wireless channel. The larger-spectrum allocation at 5 GHz can, therefore, be exploited for greater data rates.

COFDM was developed specifically for indoor wireless use and offers performance much superior to that of spread-spectrum solutions [10]. COFDM works by breaking one high-speed data carrier into several lower-speed subcarriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide (figure 3.9) and is broken up into 52 subchannels, each approximately 300 KHz wide (figure 3.10). COFDM uses 48 of these subchannels for data, while the remaining four are used for error correction. COFDM delivers higher data rates and a high degree of multipath reflection recovery.

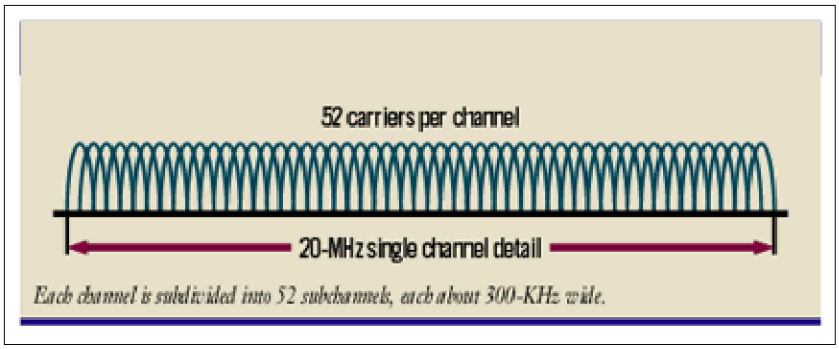

FIGURE 3.9 Subchannels [Conover 2001]

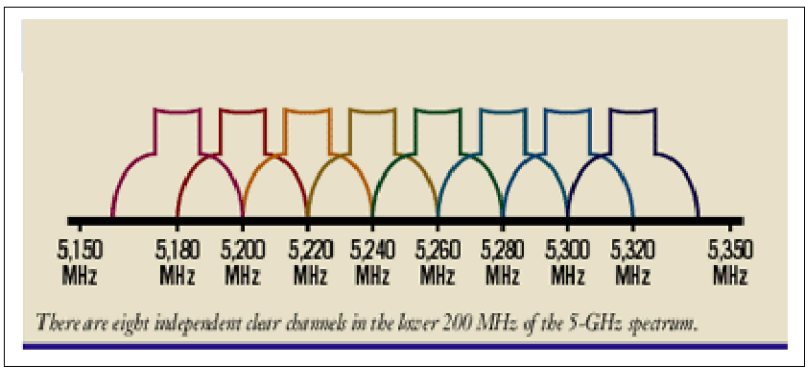

FIGURE 3.10 Independent clear channels [Conover 2001]

Each subchannel in the COFDM implementation is about 300 KHz wide. At the low end of the speed gradient, BPSK (binary phase shift keying) is used to

encode 125 Kbps of data per channel, resulting in a 6,000-Kbps, or 6 Mbps, data rate. Using quadrature phase shift keying, the amount of data encoded to 250 Kbps per channel can be doubled, yielding a 12-Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4 bits per hertz, a data rate of 24 Mbps can be achieved. The 802.11a standard specifies that all 802.11a-compliant products must support these basic data rates. The standard also lets the vendor extend the modulation scheme beyond 24 Mbps. The more bits per cycle (hertz) that are encoded, the more susceptible the signal will be to interference and fading, and ultimately, the shorter the range, unless power output is increased.

Devices using 802.11b enjoy international acceptance because the 2.4-GHz band is almost universally available. Where there are conflicts, the vendor can implement frequency-selection software that prevents a radio from operating at illegal frequencies. However, the 5-GHz spectrum does not share this luxury. In the United States, 802.11a enjoys relatively clear-channel operation. The Japanese market shares only the lower 100 MHz of the frequency spectrum, which means 802.11a applications in Japan will face more contention. In Europe, the lower 200 MHz are common with the FCC's 5-GHz allotment, but the higher 100 MHz, reserved for outdoor applications, are taken. 802.11a needs about 20 MHz of spectrum to operate at 54 Mbps. Thus, users in the United States and Europe will have up to 10 channels from which to choose, while users in Japan will be restricted to five channels.

In Europe, the HiperLAN/2 standard, led by the ETSI (European Telecommunications Standards Institute)'s BRAN (Broadband Radio Access Networks) group, has wide acceptance as the 5-GHz technology of choice. HiperLAN/2 and 802.11a share some similarities at the physical layer: Both use OFDM technology to achieve their data rates, for instance. However, HiperLAN/2 is much more akin to ATM than to Ethernet. In fact, the HiperLAN/2 standard grew out of the effort to develop wireless ATM. HiperLAN/2 shares the 20-MHz channels in the 5-GHz spectrum in time, using TDMA (time division multiple access) to provide QoS (Quality of Service) through ATM-like mechanisms.

In contrast, 802.11a shares the 20-MHz channel in time using CSMA/ CA (carrier sense multiple access with collision avoidance). Logically, HiperLAN/2 uses a different MAC from the one that 802.11a uses. The HiperLAN/2 MAC design has

proven to be problematic and controversial, and the HiperLAN/2 standard is nowhere close to complete. In contrast, 802.11a uses the same MAC as 802.11b, which gives developers only one task to complete: a 5-GHz IEEE 802.11a-compliant radio. No simple task, but easier than redesigning the radio and the MAC controller.

For implementers, 802.11a's use of the same MAC as 802.11b means one less component to design. For adopters, this means that upgrading from 802.11b to 802.11a technology will not have significant impact on network operations. 802.11b's MAC uses CSMA/CA technology and implements a number of options to improve throughput, especially in congested areas.

The only drawback to using the 802.11b MAC is that 802.11a inherits the same inefficiencies hampering 802.11b wireless solutions. The 802.11b MAC is only about 70 percent efficient, so even at 54 Mbps, maximum throughput is closer to 38 Mbps. Factor in driver inefficiencies and some additional overhead at the physical layer, and it can be expected the actual throughput to be about 30 Mbps. This throughput can be estimated as based on the average throughput of 802.11b networks, which is now about 6 Mbps of a possible 11 Mbps for optimal implementations. Unlike 802.11b, 802.11a does not have to transmit its headers at 1 Mbps, so 802.11a will gain some theoretical efficiency over 802.11b; still, it's safe to speculate that throughput won't exceed 35 Mbps.

3.7 IEEE 802.11g Standard

The IEEE's 802.11 Task Group G had been considering two competing modulations that would allow the faster speed [11]. All these wireless devices use spread-spectrum broadcast technology, which distributes information across many frequencies in an alternating pattern, so never continuously occupying any one part of the band. Currently, the FCC (and, by extension, most of the regulatory bodies from other countries) allows only two kinds of spread-spectrum use: frequency hopping (FH), employed by HomeRF and Bluetooth; and direct sequence (DS), used by 802.11b.

Two types of direct sequencing are competing to become the 802.11g standard. Texas Instruments has been promoting a technology called packet binary convolutional code (PBCC), which it said offered better backward compatibility with

earlier versions, ensuring that 802.11b devices would remain useful as organizations upgraded.

Intersil is pushing a modulation called wide-band orthogonal frequency division multiplexing (OFDM), which is used under the same and different acronyms for xDSL transmission and other tasks where a wide band of frequency can achieve higher efficiency through subdivision. Both of these technologies are actually old modulations reinvigorated by the arrival of faster, smaller, and cheaper chips that make them practical for wireless networking.

Recently, the 802.11 Task Group G eliminated Texas Instruments' contender, PBCC, from consideration for the 802.11g protocol. But TI says it will pursue the technology and sell it as a wireless networking chipset compatible with 802.11b up to 11 Mbps. PBCC was already approved for use by the IEEE with 802.11b at 11 Mbps, although it's not what manufacturers agreed to implement.

OFDM isn't the clear winner yet: At least 75 percent of the working group has to approve it, and if it fails, the group can go back to the drawing board for a new 802.11g technology. It has, however, already been approved for use with 802.11a.

IEEE 802.11g is an extension of IEEE 802.11b, meaning, it must be backward compatible with 802.11b [60].

- Frequency Range: 2.4 GHz ISM band
- Medium Access: Carrier-Sense Multiple Access (CSMA)/Collision Avoidance (CA)
- Air Access: Not yet determined. Either Orthogonal Frequency Division Multiplexing (OFDM) or Packet Binary Convolution Coding (PBCC)
- Data Rates: up to 54 Mbps if OFDM is used. Much less if PBCC is used.

3.8 Others

In the meantime, there are more lettered subgroups dealing with problems inherent in existing WLANs. 802.11i, for example, is working on plugging security holes in the 802.11 standard.

The 802.11e group, meanwhile, is working on quality-of-service issues in the media access control layer of the 802.11 protocol, which will ensure that streaming video and audio will work well over WLANs.

Chapter 4

OTHER STANDARDS

4.1 HIPERLAN/1

HIPERLAN/1 is compatible with ISO/IEC 15802-1 MAC service definition and ISO/IEC 15802-3 MAC bridges specifications [24]. It may provide coverage beyond the radio range limitation of a single node via multihop relaying and it supports node mobility. HIPERLAN/1 devices may be operated in Europe in the 5,15-5,30 GHz frequency band. Five HIPERLAN/1 channels may be accommodated in the 5,15-5,30 GHz band. Channels 0, 1, 2 are the mandatory default channels. The availability of channels 3, 4 is subject to national administrations.

The HIPERLAN/1 specifications cover the Physical layer and the MAC layer, i.e. layers 1 and 2 of the OSI model.

4.1.1 HIPERLAN PHY

Adaptive equalisation was chosen as the HIPERLAN multipath counter-measure to facilitate high transmission rates [44]. It is envisaged that the system will use a DFE (Decision Feedback Equaliser) although this is not specified in the standard.

HIPERLAN transmission can be at one of two data rates. The high data rate is 23.5Mbit/s. The modulation is pre-coded non-differential GMSK (Gaussian Minimum Shift Keying) with a BT (bandwidth bit-period product) of 0.3. This is transmitted in a channel of 23.5MHz bandwidth. There are five channels in the 5GHz band.

The low data rate is 1.5Mbit/s, 1/16 of the high data rate. This will be transmitted using the same modulation and direct sequence spread spectrum. This can be detected with a matched filter or correlator.

The HIPERLAN data packet consists of three parts a low date rate header, a synchronisation and training sequence, and the data. This is shown in figure 4.1

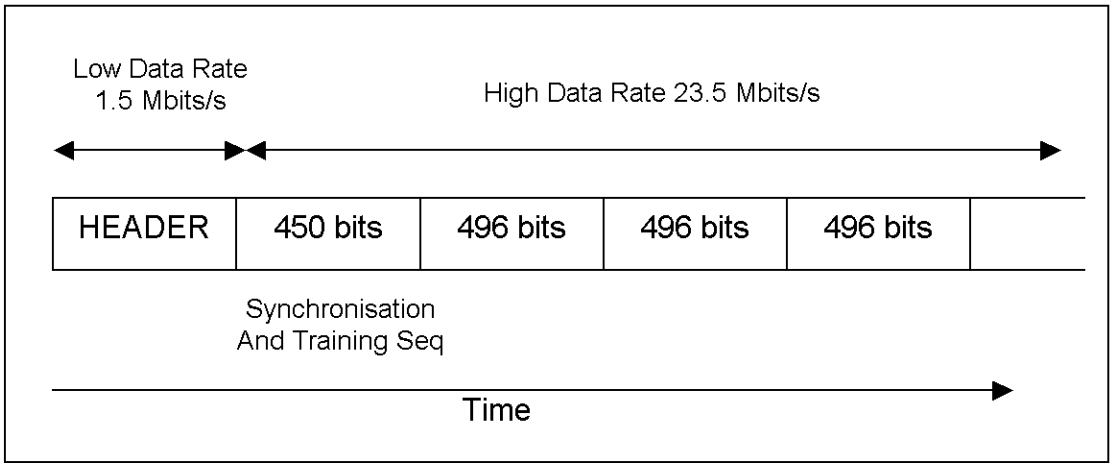

FIGURE 4.1 HIPERLAN packet [Wilkinson 1995]

The low data rate header contains a truncated version of the destination 48bit MAC address, which is transmitted at 1.5Mbit/s. This can be demodulated without equalisation. This is to facilitate power saving strategies where the receiver is only activated when the MAC address is detected in the low data rate header.

The synchronisation and training sequence is 450 bits long.

The data consists of m data blocks of 496 bits where m is from 1 to 47 (the maximum packet length of 47 blocks is calculated for a relative velocity of 1,4m/s). The packet is designed in this way to make it compatible with Ethernet. A block of 416 bits is divided into 16 segments and FEC (Forward Error Correction) encoded with a BCH (31,26) code to give a block of 496 bits.

The H1PERLAN acknowledgement packet is also transmitted at the low data rate so that it can be demodulated without equalisation.

There are three classes of transmitter 30dBm, 20dBm and 10dBm EIRPEP. Antenna diversity is an option and directional antennas can be used but the transmit power must be scaled accordingly. If antenna diversity is used, the antenna used for CCA (Clear Channel Assessment) must also be used for transmitting.

The MAC protocol CCA uses an adaptive threshold based on the signal strength measured in the environment. To enable the MAC protocol to function efficiently, the TX to RX turn around time must be less than 5μs.

Concerns have been expressed about the complexity of the HIPERLAN PHY and the associated power consumption. These concerns can only be investigated with HIPERLAN hardware demonstrators.

4.1.2 HIPERLAN MAC

The only workable way to implement a distributed MAC protocol was to use a variant of CSMA (Carrier Sense Multiple Access] or listen-before-talk that is used to great effect in Ethernet. The difficulty with implementing this on a radio link is that the large dynamic range between transmit and receive signal strengths makes CD (Collision Detection) or listen-while-talk very difficult. Hence, most radio versions of CSMA use CA (Collision Avoidance), which is a randomisation of the collision probability rather than actual avoidance. The HIPERLAN MAC protocol uses a form of listen-before-talk with a random listen-talk sequence prior to data packet transmission.

The protocol also has priority capability designed to ensure delivery times of isochronous traffic. The MAC protocol mechanism is shown in figure 4.2.

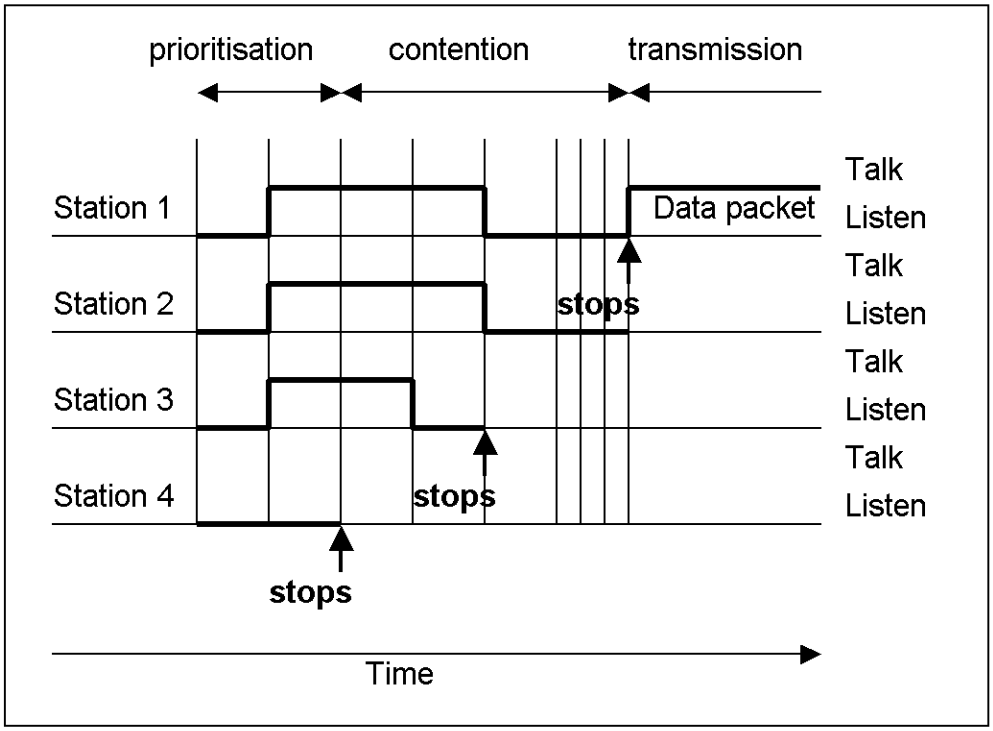

FIGURE 4.2 HIPERLAN MAC protocol mechanism [Wilkinson]

There are three phases in packet transmission; these are, the prioritisation phase, the contention phase and the transmission phase, all of which are of variable duration. If no activity has been sensed on the channel for 1700 bit periods, transmission can take place immediately. Otherwise, it is assumed that all stations wishing to transmit will synchronise to the end of the last transmission and execute the three phases.

The prioritisation phase exists to prioritise transmissions. The prioritisation phase consists of a maximum of 5 slots of 10μs (256bits) duration. Priority is asserted by transmitting in a slot, 1 to 5, 1 for highest priority, and 5 for lowest priority. Stations listen until they transmit. The priority phase ends when one or more stations assert their priority and listening stations with lower priority hear this and defer.

Packet priority is related to the residual lifetime of the packet, number of hops to final destination and application assigned priority. So asynchronous traffic such as file transfer will have a long lifetime and low priority, whereas isochronous traffic such as audio or video will have a short lifetime and high priority. The priority for a packet increases until the lifetime expires and then the packet is discarded. When this happens the MAC informs the higher layers. This has interesting implications for multimedia applications.

The contention phase exists to resolve contention between stations with the same priority. The contention phase consists of an elimination phase and a yield phase. The elimination phase consists of a maximum of 12 slots of 10μs (256bits). Stations entering the elimination phase after the prioritisation phase will continue to transmit in successive slots with probability 0.5 then listen for a single slot. If they hear nothing, they then enter the yield phase. The duration of this phase is 1 to 12 slots. The yield phase consists a maximum of 14 slots of 2.5μs (64bits). Stations entering yield phase from elimination phase will continue to listen in successive slots with probability 0.9. If they hear nothing they then enter the transmission phase.

The transmission phase simply consists of packet transmission. Packet reception is acknowledged by transmission of an acknowledgement.

Figure 4.2 shows four stations contending for the channel. Station four has a lower priority packet than the other stations and is eliminated in the prioritisation

phase. Station 3 is eliminated in the elimination part of the contention phase. Station 2 is eliminated in the yield part of contention phase and station four gets the channel.

The HIPERLAN standard has other elegant features. HIPERLAN has multi-hop relaying capability facilitated by neighbour tables. These are updated periodically when hello packets are transmitted by neighbour stations. There is also a power saving strategy involving wake sleep cycles specified.

4.2 HIPERLAN/2

HiperLAN/2 is a new, high-speed standard for Wireless LANs [58]. HiperLAN/2 allows for increased speed, performance and mobility while retaining the security that customers have come to expect from Wireless LANs

Operating on the unlicensed 5 GHz band, HiperLAN/2 has assigned frequencies in Europe, the USA and Japan. The allocated frequencies provide a true broadband environment that allows large networks to be deployed without compromising performance.

The HiperLAN2 standard is developed by ETSI-BRAN, the European Telecommunication Standards Institute-Broadband Radio Access Network, project.

The spectrum at 5 GHz increases the overall capacity of Wireless LANs. HiperLAN/2 has unique features that distinguish it from other Wireless LAN standards. These functions allow the deployment of HiperLAN/2 in cellular or ad-hoc type networks in a variety of different environments, all while retaining full coverage and high data rates.

HIPERLAN/2 provides a flexible platform for a variety of business and home multimedia applications that can support a set of bit rates up to 54 Mbit/s [25]. In a typical business application scenario, a mobile terminal gets services over a fixed corporate/public network infrastructure. In addition to QoS, the network will provide mobile terminals with security and mobility management services when moving. In an exemplary home application scenario, a low-cost and flexible networking is supported to interconnect wireless digital consumer devices.

To fulfill these goals, HIPERLAN/2 relies on cellular networking topology combined with an ad-hoc networking capability. It supports two basic modes of operation: centralized mode and direct mode. The centralized mode is used in the

cellular networking topology where each radio cell is controlled by an access point covering a certain geographical area. In this mode, a mobile terminal communicates with other mobile terminals or with the core network via an access point. This mode of operation is mainly used in business applications, both indoors and outdoors, where an area much larger than a radio cell has to be covered. The direct mode is used in the ad-hoc networking topology, mainly in typical private home environments, where a radio cell covers the whole serving area. In this mode, mobile terminals in a single-cell home "network" can directly exchange data.

4.2.1 The HiperLAN2 Network

A HiperLAN2 network typically has a topology as depicted in figure 4.3 below [22]. The Mobile Terminals (MT) communicate with the Access Points (AP) over an air interface as defined by the HiperLAN2 standard. There is also a direct mode of communication between two MTs, which is still in its early phase of development. The user of the MT may move around freely in the HiperLAN2 network, which will ensure that the user and the MT get the best possible transmission performance. An MT, after association has been performed (can be viewed as a login), only communicates with one AP in each point in time. The APs see to that the radio network is automatically configured, taking into account changes in radio network topology, i.e. there is no need for manual frequency planning.

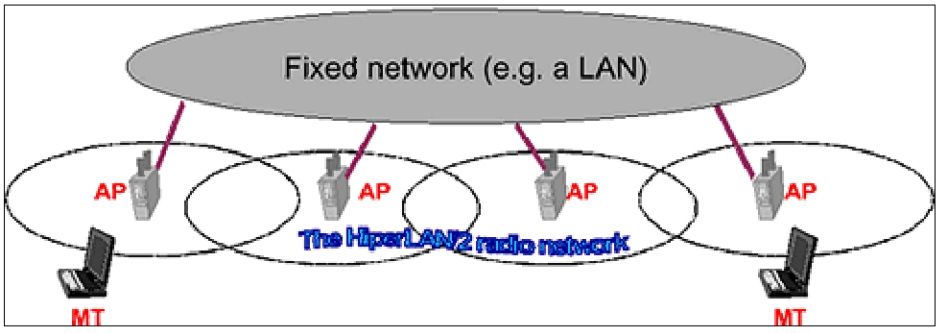

FIGURE 4.3 A HIPERLAN/2 network [Jhonsson 1999]

4.2.2 Features of HiperLAN2

4.2.2.1 High-Speed Transmission

HiperLAN2 has a very high transmission rate, which at the physical layer extends up to 54 Mbit/s and on layer 3 up to 25 Mbit/s. To achieve this, HiperLAN2 makes use of a modularization method called Orthogonal Frequency Digital Multiplexing (OFDM) to transmit the analogue signals. OFDM is very efficient in time-dispersive environments, e.g. within offices, where the transmitted radio signals are reflected from many points, leading to different propagation times before they eventually reach the receiver. Above the physical layer, the Medium Access Control (MAC) protocol is all new which implements a form of dynamic time-division duplex to allow for most efficient utlilization of radio resources.

4.2.2.2 Connection-Oriented

In a HiperLAN2 network, data is transmitted on connections between the MT and the AP that have been established prior to the transmission using signaling functions of the HiperLAN2 control plane. Connections are time-division-multiplexed over the air interface. There are two types of connections, point-to- point and point-to-multipoint. Point-to-point connections are bi-directional whereas point-to-multipoint are unidirectional in the direction towards the Mobile Terminal. In addition, there is also a dedicated broadcast channel through which traffic reaches all terminals transmitted from one AP.

4.2.2.3 QoS Support

The connection-oriented nature of HiperLAN2 makes it straightforward to implement support for QoS. Each connection can be assigned a specific QoS, for instance in terms of bandwidth, delay, jitter, bit error rate, etc. It is also possible to use a more simplistic approach, where each connection can be assigned a priority level relative to other connections. This QoS support in combination with the high

transmission rate facilitates the simultaneous transmission of many different types of data streams, e.g. video, voice, and data.

4.2.2.4 Automatic Frequency Allocation

In a HiperLAN2 network, there is no need for manual frequency planning as in cellular networks like GSM. The radio base stations, which are called Access Points in HiperLAN2, have a built-in support for automatically selecting an appropriate radio channel for transmission within each AP's coverage area. An AP listens to neighboring APs as well as to other radio sources in the environment, and selects an appropriate radio channel based on both what radio channels are already in use by those other APs and to minimize interference with the environment.

4.2.2.5 Security Support

The HiperLAN2 network has support for both authentication and encryption. With authentication both the AP and the MT can authenticate each other to ensure authorized access to the network (from the AP's point of view) or to ensure access to a valid network operator (from the MT's point of view). Authentication relies on the existence of a supporting function, such as a directory service, but which is outside the scope of HiperLAN2.

The user traffic on established connections can be encrypted to protect against for instance eavesdropping and man-in-middle attacks.

4.2.2.6 Mobility Support

The MT will see to that it transmits and receives data to/from the "nearest" AP, or more correctly speaking the MT uses the AP with the best radio signal as measured by the signal to noise ratio. Thus, as the user and the MT move around, the MT may detect that there is an alternative AP with better radio transmission performance than the AP, which the MT is currently associated to. The MT will then order a hand over to this AP. All established connections will be moved to this new

AP resulting in that the MT stays associated to the HiperLAN2 network and can continue its communication. During handover, some packet loss may occur.

If an MT moves out of radio coverage for a certain time, the MT may loose its association to the HiperLAN2 network resulting in the release of all connections.

4.2.2.7 Network & Application Independent

The HiperLAN2 protocol stack has a flexible architecture for easy adaptation and integration with a variety of fixed networks. A HiperLAN2 network can for instance be used as the "last hop" wireless segment of a switched Ethernet, but it may also be used in other configurations, e.g. as an access network to 3 rd generation cellular networks. All applications, which today run over a fixed infrastructure, can also run over a HiperLAN2 network.

4.2.2.8 Power Save

In HiperLAN2, the mechanism to allow for an MT to save power is based on MT-initiated negotiation of sleep periods. The MT may at any time request the AP to enter a low power state (specific per MT), and requests for a specific sleep period. At the expiration of the negotiated sleep period, the MT searches for the presence of any wake up indication from the AP. In the absence of the wake up indication the MT reverts back to its low power state for the next sleep period, and so forth. An AP will defer any pending data to an MT until the corresponding sleep period expires. Different sleep periods are supported to allow for either short latency requirement or low power requirement.

4.2.3 Protocol Architecture and Layers

In figure 4.4 below, the protocol reference model for the HiperLAN2 radio interface is depicted. The protocol stack is divided into a control plane part and a user plane part following the semantics of ISDN functional partitioning; i.e. user plane includes functions for transmission of traffic over established connections, and the control plane includes functions for the control of connection establishment,

release, and supervision. The HiperLAN2 protocol has three basic layers; Physical layer (PHY), Data Link Control layer (DLC), and the Convergence layer (CL).

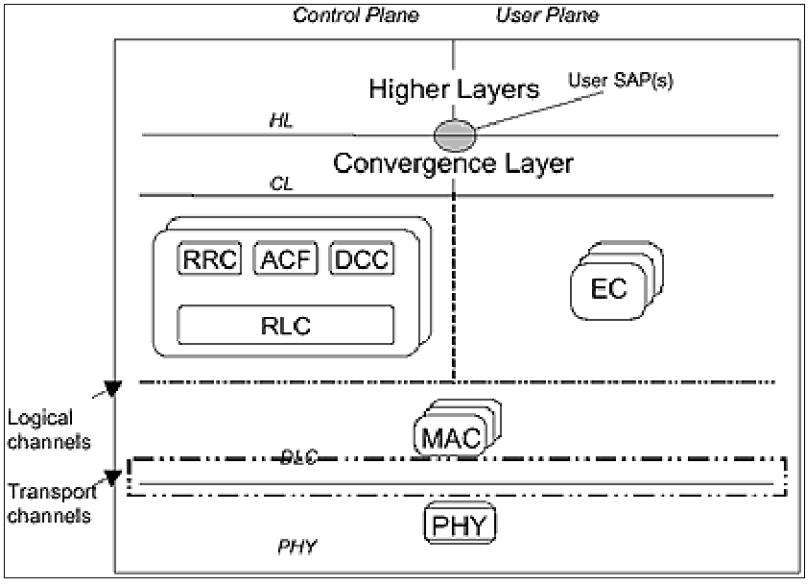

FIGURE 4.4 HiperLAN/2 protocol reference model [Jhonsson 1999]

4.2.3.1 Physical Layer

The transmission format on the physical layer is a burst, which consists of a preamble part and a data part, where the latter could originate from each of the transport channels within DLC. Orthogonal Frequency Division Multiplexing (OFDM) has been chosen due to its excellent performance on highly dispersive channels. The channel spacing is 20 MHz, which allows high bit rates per channel but still has a reasonable number of channels in the allocated spectrum (e.g. 19 channels in Europe). 52 subcarriers are used per channel, where 48 subcarriers carry actual data and 4 subcarriers are pilots which facilitate phase tracking for coherent demodulation. The duration of the guard interval is equal to 800 ns, which is sufficient to enable good performance on channels with delay spread of up to 250 ns. An optional shorter guard interval of 400 ns may be used in small indoor environments.

The basic idea in OFDM (Orthogonal Frequency Division Multiplex), which is a special form of multicarrier modulation, is to transmit broadband, high data rate information by dividing the data into several interleaved, parallel bit streams, and let

each one of these bit streams modulate a separate subcarrier. In this way the channel spectrum is passed into a number of independent non-selective frequency subchannels. These sub channels are used for one transmission link between the AP and the MTs. OFDM is efficiently realized by the use of effective signal processing, fast-fourier transform, in the transmitter and receiver. This significantly reduces the amount of required hardware compared to earlier FDM-systems. One of the benefits of OFDM is the robustness against the adverse effects of multipath propagation with respect to intersymbol interference. It is also spectrally efficient because the subcarriers are packed maximally close together. OFDM also admits great flexibility considering the choice of and realization of different modulation alternatives.

ODFM requires a properly designed system. Of special importance is the design of frequency synchronization and power amplifier back-off in the receiver. Also the number of subcarriers has to be chosen in an appropriate way. So far OFDM has been standardised for several applications. Under the name there is discrete multitone (DMT) which is the world standard for asymmetric digital subscriber lines (ADSL). As an example of a wireless broadcast application, OFDM has been standardized for DAB, the European Digital Audio Broadcasting.

A key feature of the physical layer is to provide several modulation and coding alternatives. This is to both adapt to current radio link quality and to meet the requirements for different physical layer properties as defined for the transport channels within DLC. BPSK, QPSK and 16QAM are the supported subcarrier modulation schemes (64QAM is optional). Forward error control is performed by a convolutional code with rate 1/2 and constraint length seven. The three code rates 1/2, 9/16 and 3/4 are obtained by puncturing. Seven physical layer modes (PHY modes) are specified in table 4.1.

TABLE 4.1 PHY modes defined for HiperLAN2

Mode	Modulation	Code rate	PHY bit rate	Bytes/OFDM symb
1	BPSK	½	6 Mbps	3.0
2	BPSK	¾	9 Mbps	4.5
3	QPSK	½	12 Mbps	6.0
4	QPSK	¾	18 Mbps	9.0
5	16QAM	9/16	27 Mbps	13.5
6	16QAM	¾	36 Mbps	18.0
7	64QAM	¾	54 Mbps	27.0

4.2.3.2 Data Link Control Layer

Includes functions for both medium access and transmission (user plane) as well as terminal/user and connection handling (control plane). Thus, the DLC layer consists of a set of sublayers:

- Medium Access Control (MAC) protocol.
- Error Control (EC) protocol
- Radio Link Control (RLC) protocol with the associated signaling entities DLC Connection Control (DCC), the Radio Resource Control (RRC) and the Association Control Function (ACF)

4.2.3.2.1 MAC Protocol

The MAC protocol is the protocol used for access to the medium (the radio link) with the resulting transmission of data onto that medium. The control is centralised to the AP which inform the MTs at which point in time in the MAC frame they are allowed to transmit their data, which adapts according to the request for resources from each of the MTs.

The air interface is based on time-division duplex (TDD) and dynamic time-division multiple access (TDMA). I.e. the time-slotted structure of the medium allows for simultaneous communication in both downlink and uplink within the same time frame, called MAC frame in HiperLAN2. Time slots for downlink and uplink communication are allocated dynamically depending on the need for transmission resources. The basic MAC frame structure on the air interface has a fixed duration of 2 ms and comprises transport channels for broadcast control, frame control, access control, downlink (DL) and uplink (UL) data transmission and random access. All data from both AP and the MTs is transmitted in dedicated time slots, except for the random access channel where contention for the same time slot is allowed. The duration of broadcast control is fixed whereas the duration of other fields is dynamically adapted to the current traffic situation. The MAC frame and the transport channels form the interface between DLC and the physical layer.

4.2.3.2.2 The Error Control Protocol

Selective repeat (SR) ARQ is the Error Control (EC) mechanism that is used to increase the reliability over the radio link. EC in this context means detection of bit errors, and the resulting retransmission of U-PDU(s) if such errors occur. EC also ensures that the U-PDU's are delivered in-sequence to the convergence layer. The method for controlling this is by giving each transmitted U-PDU a sequence number per connection. The ARQ ACK/NACK messages are signaled in the LCCH. An errored U-PDU can be retransmitted a number of times (configurable). To support QoS for delay critical applications such as voice in an efficient manner, a U-PDU discard mechanism is defined. If the data becomes obsolete (e.g. beyond the playback point), the sender entity in the EC protocol can initiate a discard of a U-PDU and all U-PDUs with lower sequence number and which haven't been acknowledged. The result is that the transmission in DLC allows for "holes" (missing data) while retaining the DLC connection active. It is up to higher layers, if there is a need, to recover from missing data.

4.2.3.2.3 Signaling and Control

The Radio Link Control (RLC) protocol gives a transport service for the signaling entities Association Control Function (ACF), Radio Resource Control function (RRC), and the DLC user Connection Control function (DCC). These four entities comprise the DLC control plane for the exchange of signaling messages between the AP and the MT.

4.2.3.3 Convergence Layer

The convergence layer (CL) has two main functions: adapting service request from higher layers to the service offered by the DLC and to convert the higher layer packets (SDUs) with variable or possibly fixed size into a fixed size that is used within the DLC. The padding, segmentation and reassembly function of the fixed size DLC SDUs is one key issue that makes it possible to standardize and implement a DLC and PHY that is independent of the fixed network to which the HiperLAN2

network is connected. The generic architecture of the CL makes HiperLAN2 suitable as a radio access network for a diversity of fixed networks, e.g. Ethernet, IP, ATM, UMTS, etc. There are currently two different types of CLs defined; cell-based and packet-based as depicted in figure 4.5. The former is intended for interconnection to ATM networks, whereas the latter can be used in a variety of configurations depending on fixed network type and how the interworking is specified.

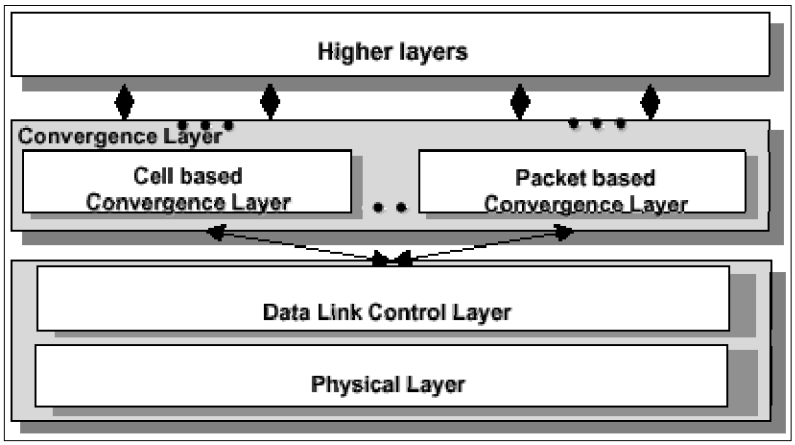

FIGURE 4.5 The general structure of the Convergence Layer.[Jhonsson 1999]

The structure of the packet-based CL with a common and service-specific part allows for easy adoption to different configurations and fixed networks. From the beginning though, the HiperLAN2 standard specifies the common part and a service specific part for interworking with a fixed ethernet network. The packet-based CL is depicted in figure 4.6.

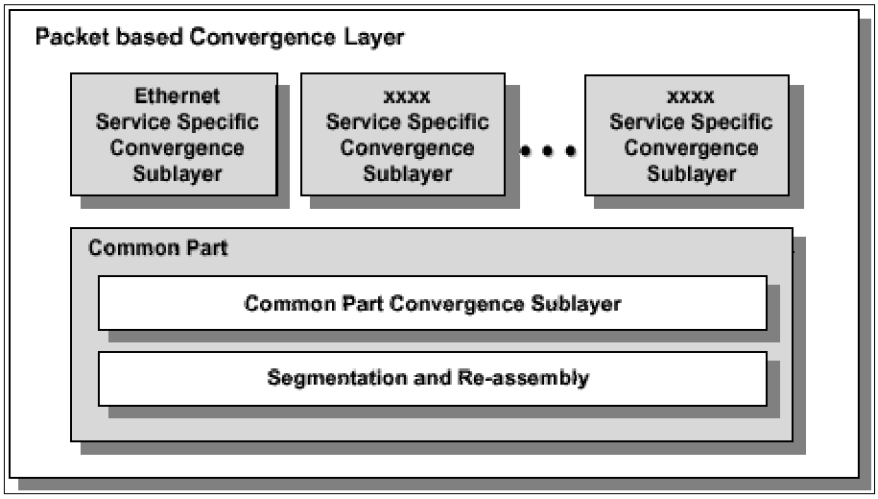

FIGURE 4.6 The general structure of the packet-based CL.[Jhonsson 1999]

The main function of Common Part of the Convergence layer is to segment packets received from the SSCS, and to reassemble segmented packets received from the DLC layer before they are handed over to the SSCS. Included in this sublayer is also to add/remove padding octets as needed to make a Common Part PDU being an integral number DLC SDUs.

The Ethernet SSCS makes the HiperLAN2 network look like wireless segments of a switched Ethernet. Its main functionality is the preservation of Ethernet frames. Both, IEEE 802.3 1 frames and tagged IEEE802.3ac 2 frames are supported. The Ethernet SSCS offers two Quality of Service schemes: The best effort scheme is mandatory supported and treats all traffic equally. The IEEE 802.1p based priority scheme is optional and separates traffic in different priority queues as described in IEEE 802.1p. As a benefit the DLC can treat the different priority queues in an optimised way for specific traffic types.

4.2.4 Radio Network Functions

The HiperLAN2 standard defines measurements and signaling to support a number of radio network functions. These are currently defined as dynamic frequency selection, link adaptation, radio cell handover, multi beam antennas and power control. All algorithms are vendor specific.

4.2.4.1 Dynamic Frequency Selection

The HiperLAN2 radio network shall automatically allocate frequencies to each AP for communication. This is performed by the Dynamic Frequency Selection (DFS) function, which allows several operators to share the available frequency spectrum and can be used to avoid the use of interfered frequencies. The frequency selection made by each AP is based on filtered interference measurements performed by the AP and its associated MTs.

4.2.4.2 Link **Adoption**

To cope with the varying radio quality, in terms of signal to interference ratio (C/I), a link adaptation scheme is used. The range of C/I levels varies depending on location where the system is deployed and also changes over time depending on the traffic in surrounding radio cells. The link adaptation scheme adapts the PHY robustness based on link quality measurements. Thus, the PHY mode is dynamically selected for the SCH and LCH in each transmitted MAC frame.

4.2.4.3 Antennas

Multi beam antennas are supported in H/2 as a means to improve the link budget and increase the C/I ratio in the radio network. The MAC protocol and the frame structure in H/2 allow up to 7 beams to be used.

4.2.4.4 Handover

The handover scheme is MT initiated, i.e. a MT performs the necessary measurements on surrounding APs and selects appropriate APs for communication. The handover measurements are not defined in the standard, i.e. a vendor can chose to base the handover on signal strength or some other quality measurement. The standard defines necessary signaling to perform the handover.

4.2.4.5 Power control

Transmitter power control is supported in both MT (uplink) and AP (downlink). MT power control is mainly used to simplify the design of the AP receiver, e.g. no AGC is needed. AP power control is part of the standard out from regulatory reasons, i.e. to decrease the interference to satellite systems.

4.2.5 Spectrum allocation & area coverage

In Europe, 455 MHz is suggested to be allocated for Hiperlan systems. The different parts of the bands have different operational conditions set by CEPT to allow coexistence with other services. A draft ERC decision is made and is expected to be approved during autumn -99.

In US, 300 MHz is allocated to wireless LANs in the so-called National Information Infrastructure (NII) In Japan, 100 MHz is allocated for Wireless LANs, and more spectrum allocation is under investigation. The ITU-R has also started activities to recommend a global allocation for Wireless LANs.

A cell of a HiperLAN2 AP typically extends to approximately 30 (office indoor) – 150 meters.

Figure 4.7 and 4.8 shows the current status regarding frequency allocation in USA, Europe, and Japan.

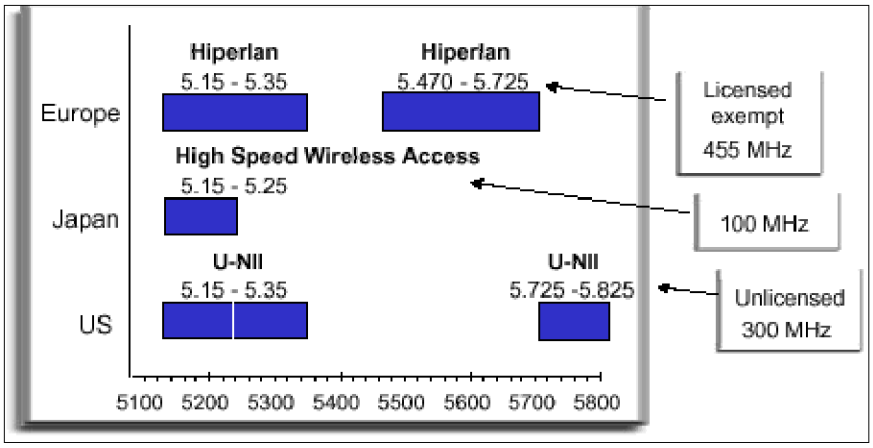

FIGURE 4.7 Spectrum allocation in 5 GHz.[Jhonsson 1999]

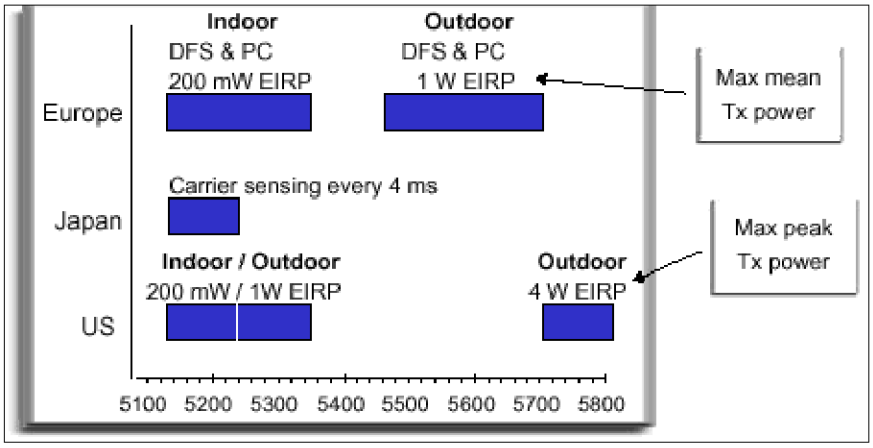

FIGURE 4.8 Spectrum rules on 5 GHz.[Jhonsson 1999]

4.2.6 How It All Works

Figure 4.9 shows a scenario with an MT, three APs which are connected to a fixed ethernet supporting the Q-tag with priority indications.

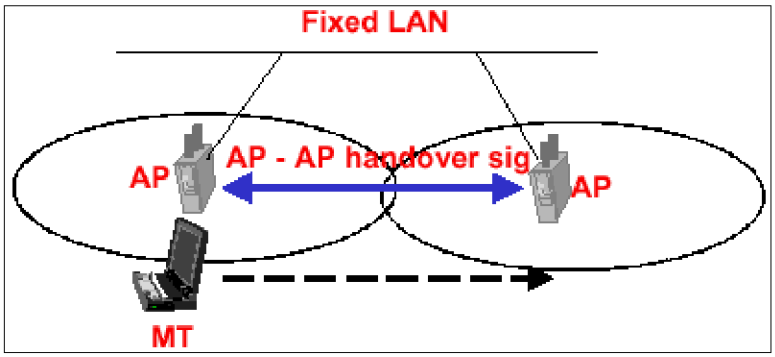

FIGURE 4.9 Sample HiperLAN2 network connected via a fixed LAN. [Jhonsson 1999]

The APs have each selected appropriate frequencies with the DFS algorithm.

The MT starts by measuring signal strength and select the appropriate AP to which it wants to get associated. From the selected AP the MT receives a MAC-ID. This is followed by exchange of link capabilities to decide upon, among other things, the authentication procedure to use and encryption algorithm as well as which convergence layer to use for user plane traffic. After a possible key exchange and authentication, the MT is associated to the AP. Finally, the DLC user connections are established over which the user plane traffic is transmitted.

The MT will send and receive data on two established connections (default in HiperLAN2) supporting two different priority queues onto which the Q-tag priorities are mapped (but more priority queues can be supported). The Ethernet CL ensures that the priorities for each Ethernet frame is mapped to the appropriate DLC user connection according to the predefined mapping scheme

The MT may subsequently decide to join one or more multicast groups. The HiperLAN2 network may be configured to use N*unicast for optimal quality, or reserve a MAC-ID for each joined group for the sake of conserving bandwidth. If a separate MAC-ID is used for a multicast group, the mapping is:

IP address -> IEEE address -> MAC-ID

As the MT moves, it may decide to perform a handover if it detects that there is an AP better suited for communication (e.g. with higher signal strength). All established connections as well as possible security associations would be automatically handed over to the new AP using AP – AP signaling via the fixed LAN. When the MT (or more correct the user) wants to get disconnected from the LAN, the MT will ask for disassociation, resulting in the release of all connections between the MT and the AP. This may also be the result if the MT happens to move out from radio coverage for a certain time period.

The comparison table of 802.11 and HiperLAN/2 can be seen in table 8.5

4.3 HomeRF

HomeRF, as the very name suggests, was developed from the beginning to bring wireless networking to the consumer using radio frequency (RF) devices [62]. A typical HomeRF network for a Broadband Internet home consists of multiple device types as shown in figure 4.10. HomeRF is unique among wireless networking standards in its ability to simultaneously provide Broadband speed Internet access and resource sharing, multiple streaming media sessions, and multiple toll-quality voice connections.

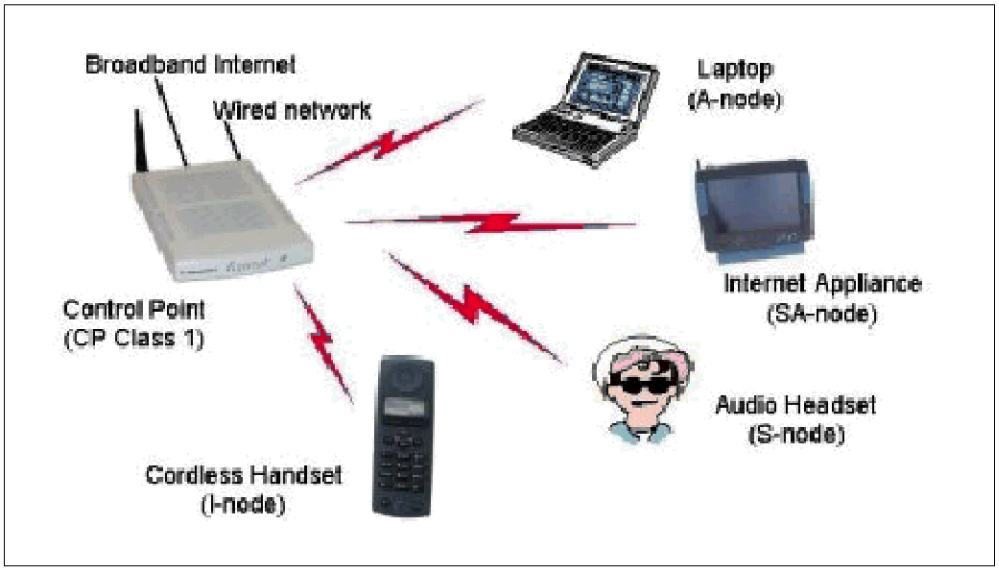

FIGURE 4.10 HomeRF Network Device Types [HomeRf WG 2001]

Although originally designed for a home network, HomeRF is the best choice for teleworkers because working from home or while on the road introduces networking requirements that enterprise wireless LANs still can't address [6]. IEEE 802.11 variants such as Wireless Fidelity (Wi-Fi) fail to provide toll-quality voice services and compare poorly in such critical aspects as cost, power consumption, reliability, and support for high-network-density environments such as apartment buildings.

HomeRF is fast, with a 10M bit/sec peak data rate in 2001 products and sufficient range for most residential applications, even in the presence of severe interference from microwave ovens, cordless phones, Bluetooth devices and nearby neighbors. The data rates back off to 5M bit/sec or slower if necessary to extend the range or to operate with older HomeRF products. By 2002, HomeRF proponents expect to achieve a data rate of 20M bit/sec or faster with full backward compatibility.

Because HomeRF was originally designed for home consumers, "certified HomeRF" products are generally simpler, more secure, more reliable and more affordable than Wi-Fi products. For example, Proxim's Symphony-HRF products make it easy to move between offices and homes – or between wired Ethernet in the home office and wireless HomeRF on the sofa, kitchen table or patio without changing network or Internet settings.

HomeRF also enables low-cost roaming for access to wireless networks in public places such as coffee shops, libraries and shopping malls. Due to its frequency-hopping technology, HomeRF offers superior scalability in larger installations, with support for up to 15 overlapping networks compared with three for Wi-Fi. Frequency hopping also makes HomeRF less susceptible to interference and more secure than Wi-Fi. And with Proxim's CompactFlash HomeRF adapter, teleworkers can even use a personal digital assistant as an Internet terminal rather than carrying a PC.

Although Wi-Fi has gained some momentum in retail channels, most deployments have been in industry vertical applications, corporate offices and schools. HomeRF continues to dominate the home wireless networking market and remains the choice of broadband carriers for their integrated services. That's because HomeRF integrates voice, data and entertainment – including cordless phones,

prioritized media streaming, wireless speakers and Dolby Surround. HomeRF is included in the leading cable modems, the top TV set-top boxes and a growing number of home gateways, music and TV devices, and information appliances.

Unlike Wi-Fi, HomeRF already has quality-of-service support for streaming media and is the only wireless LAN to integrate voice. In fact, HomeRF has a chance to become the worldwide standard for cordless phones. It is a 2.4-GHz extension of the European digitally enhanced cordless telephony standard, with added data and entertainment support and features such as call waiting, caller ID, forwarding to individual handsets, distinctive ringing, and 911 breakthrough.

HomeRF networks provide a range of up to 150-feet, sufficient to cover the typical home, garage, and yard [61]. A recent ruling by the FCC allowed increased data rates for HomeRF networks, and products based on the second-generation HomeRF 2.0 specification will take advantage of this ruling. HomeRF 2.0 enables the introduction of new types of devices, applications, and services including high-speed applications such as whole house CD quality audio distribution to wireless speakers and streaming video. At the same time, backward compatibility ensures that all current HomeRF products will operate with future products.

4.3.1 Integrated Voice & Data

In addition to the expected benefits of home networking, such as shared Internet access, PCs, data files, and printers, HomeRF also opens up a new world of applications by supporting high-quality voice and data. Consumers can look forward to innovative new services from telephone companies, cable companies and others. New information appliances and other devices will emerge that take advantage of the integrated voice and data capabilities. As services and devices evolve, HomeRF networks will support home entertainment, home automation, and even telemedicine applications.

An integrated network offers a simple, low cost solution and makes it easy to add voice or data devices to the network whenever needed. Additionally, it improves access to and utilization of both traditional telephone lines and high-speed Internet connections.

4.3.2 Voice Applications

The HomeRF specification incorporates the DECT (Digital Enhanced Cordless Telephony) standard. This standard supports all the telephony features consumers expect plus a full range of enhanced features useful in both home and small business applications. Cordless handsets using HomeRF will offer even more convenience than traditional cordless telephones, including more flexible phone placement. Today, cordless phones must be connected to telephone jacks in locations that may not be ideal to the end user. And since many homes include only two or three phone jacks, traditional cordless phones are confined to certain rooms.

With HomeRF there is no need for multiple base units to be tied to individual phone jacks. Only one connection to a single telephone jack is required, and additional cordless handsets can be purchased and placed wherever convenient. The ability to expand the voice network by simply adding handsets offers savings over purchasing multiple cordless phones.

Users also benefit from the convenience of sharing the same, rich set of telephone features. Multiple handsets can also be used to enable users to place both external and intercom calls at the same time. HomeRF technology also provides superior voice quality and security. Using 2.4GHz technology, the HomeRF avoids interference from other cordless phones, remote controls, and baby monitors. Using Frequency Hopping Spread Spectrum (FHSS) technology, the voice channel changes fifty times every second, ensuring conversations are not overheard.

4.3.3 Emerging HomeRF Applications

While today's home networks typically connect multiple PCs to enable Internet and printer sharing, home networks of tomorrow will enable sharing of unified voice, data and video services. Users will realize new benefits and conveniences by including everything from new digital entertainment devices to traditional household appliances in the home network. As services and devices evolve, HomeRF networks will support a variety of home entertainment, home automation, and even telemedicine applications. Further, HomeRF support of both voice and data will allow speech-enabled applications for increased user convenience.

Some examples of what users will be able to do with the availability of products that adhere to the HomeRF specification include:

- Set up a wireless home network to share voice and data between PCs, peripherals, PC-enhanced cordless phones, and new devices such as portable, remote displays or "Web" pads
- Access the Internet from anywhere in and around the home from portable display devices
- Share a single ISP connection between PC's and other new devices
- Intelligently forward incoming telephone calls to multiple cordless handsets, FAX machines and voice mailboxes
- Review incoming voice, FAX and e-mail messages from a small PC-enhanced cordless telephone handset
- Activate other home electronic systems by simply speaking a command into a PC-enhanced cordless handset
- Play multi-player games, toys and gaming consoles based on PC or Internet resources
- Download MP3 and other audio files using audio streaming
- Enjoy streaming audio and video from networked devices anywhere in the home.

4.3.4 Technical Overview

The HomeRF specification, like most networking interface standards, describes fundamentally the lowest two layers of the seven-layer OSI network stack model as shown in figure 4.11 [62]. The lowest layer, the physical (PHY) layer, sets most of the cost, data rate and range characteristics. The second layer, the data link control (DLC) or as used here the media access control (MAC) layer, defines the types of data services such as voice or prioritized streaming as well as other attributes like security, roaming and mapping to standard upper layers. In HomeRF the PHY and MAC layers are optimized together to provide superior interference immunity and high network density.

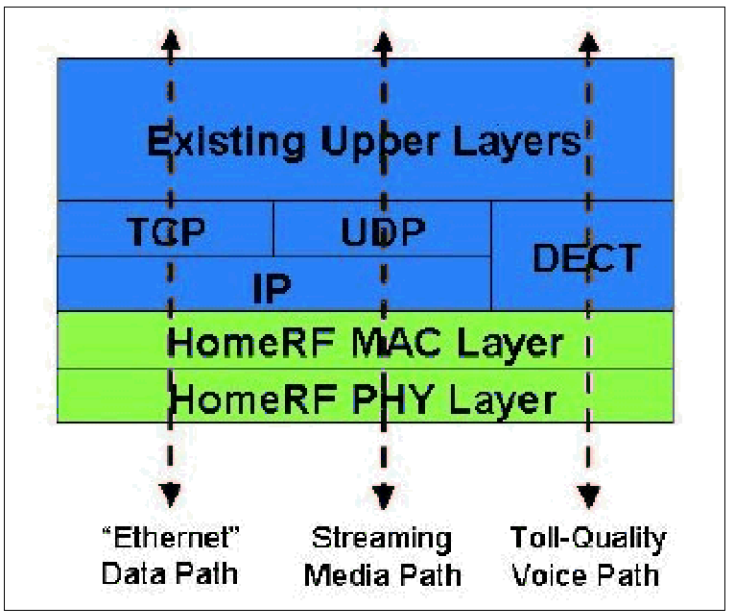

FIGURE 4.11 HomeRF Network Stack Model [HomeRF WG 2001]

4.3.4.1 PHY Layer

The HomeRF PHY layer enables low cost, low power, and small size products. The HomeRF PHY layer of figure 4.11 is common to all data service flow types shown in figure 4.10. HomeRF products operate in the globally available 2.4 GHz band using frequency hopping spread spectrum at 50-100 hops/s. The radios are extremely simple - in fact they require only the same basic circuits as Bluetooth - such that very low cost, low power and highly integrated solutions are feasible today. First generation HomeRF products which as of this writing have captured over 90% of home wireless networking market share have peak data rates of 1.6 Mb/s and readily cover virtually all homes and small offices with 150 feet typical indoor range. Second generation HomeRF products due to ship mid-2001 use 10 Mb/s peak data rates while still providing whole home coverage. Both generations provide stellar low power consumption (<10 mW standby with full TCP/IP connectivity) and small size (world's only Compact Flash WLAN). Third generation HomeRF devices are planned to be faster yet (~ 20 Mb/s).

4.3.4.2 MAC Layer

As indicated by figure 4.11, the HomeRF MAC layer provides three distinct service flow categories:

- An asynchronous, connectionless packet data service (or "wireless Ethernet") typically used for TCP/IP traffic
- A prioritized and repetitive connection-oriented data service typically used for streaming media sessions using UDP/IP flows
- An isochronous, full-duplex, symmetric, two-way voice service typically used to map multiple toll-quality voice connections as defined by the DECT protocol

A very basic description of how the HomeRF MAC layer operates in the time domain is shown in figure 4.12. Within each repeating frame, either 10 or 20 ms long depending on the presence of active voice calls, the bulk of the time (or bandwidth) is typically available for asynchronous data. However, within this asynchronous data period the first available opportunities to send packets are reserved sequentially for the prioritized streaming media sessions. Up to 8 sequentially prioritized simultaneous sessions are allowed but if fewer than 8 are present, the reservations are cancelled and the time (or bandwidth) is fully available for asynchronous data services.

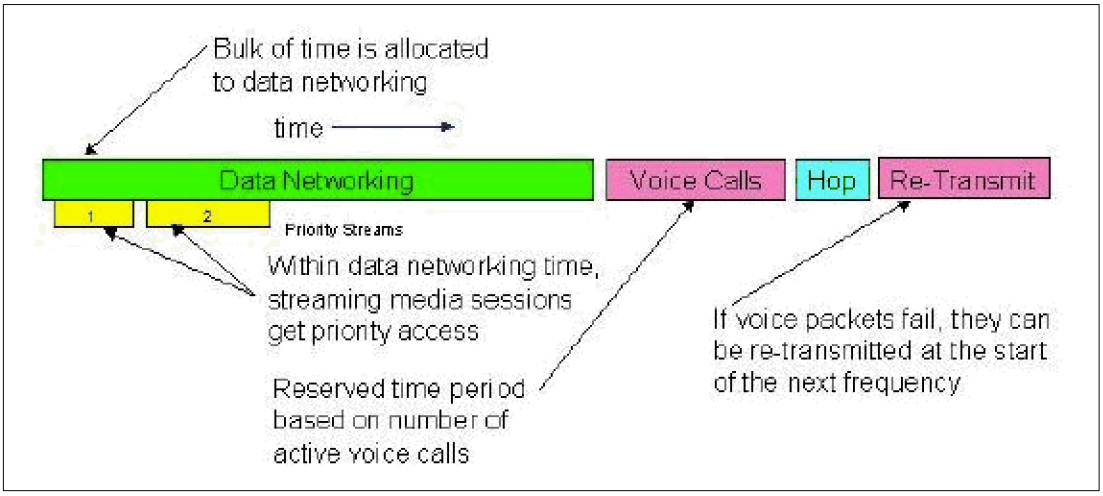

FIGURE 4.12 HomeRF MAC Layer Timing [HomeRF WG 2001]

Continuing with figure 4.12, the last part of the repeating frame structure is divided into a series of fixed-length slots that are assigned as full-duplex pairs for two-way toll-quality voice communications based entirely upon the DECT upper-layer protocol. DECT, the Digital Enhanced Cordless Telecommunications system, is the world's most successful multi-line cordless telephony system in history with over 50M units in the field today and over 200M predicted by 2003. By designing the HomeRF MAC layer to map directly into DECT upper layers, HomeRF leverages not only thousands of thoroughly debugged protocol specification pages but also fifth generation custom DECT silicon and over 100 certified DECT handset suppliers that can easily convert to HomeRF. Note again that the time reserved for voice calls is directly proportional to the number of active connections and is adjusted dynamically as calls are added or dropped. Thus time (or bandwidth) available for data communications is always maximized. First generation HomeRF voice/data systems support 4 active handsets with a subjective voice quality score of 4.1 out of 5 (versus 4.3 for landline or 3.2 for digital cell phones). Second generation HomeRF voice/data systems will allow up to 8 active handsets at identical voice quality as landline.

The last "event" shown in figure 4.12 is the voice connection re-transmits period. This is unique to HomeRF and provides excellent voice quality even in the presence of severe interference because the re-transmissions occur at a different frequency channel. The re-transmit feature is applied only to those rare voice packets that are actually lost in order to once again maximize the bandwidth available for asynchronous data traffic.

4.4 IrDA (Infrared Data Association)

IrDA is a standard defined by the IrDA consortium (**Infra**red **D**ata **A**ssociation) [28]. It specifies a way to wirelessly transfer data via infrared radiation. The IrDA specifications include standards for both the physical devices and the protocols they use to communicate with each other. The IrDA standards have arisen from the need to connect various mobile devices together.

As infrared data communications, based on standards from the Infrared Data Association (IrDA), become widely available on personal computers and peripherals, a timely opportunity exists for effective and inexpensive short range wireless

communications on embedded systems and devices of all types [42]. The IrDA standards were developed rapidly (compared to most standards organizations), and information on the IrDA protocols has not yet reached every corner of the embedded systems universe.

The Infrared Data Association (IrDA) is an industry-based group of over 150 companies that have developed communication standards especially suited for low cost, short range, cross-platform, point-to-point communications at a wide range of speeds. These standards have been implemented on various computer platforms and more recently have become available for many embedded applications. Because of their wide acceptance, the IrDA specifications are now on an accelerated track for adoption as ISO standards.

In general, IrDA is used to provide wireless connectivity technologies for devices that would normally use cables for connectivity [41]. IrDA is a point-to-point, narrow angle (30° cone), ad-hoc data transmission standard designed to operate over a distance of 0 to 1 meter and at speeds of 9600 bps to 16 Mbps.

IrDA devices conforming to standards IrDA 1.0 and 1.1 work over distances up to 1.0m with BER (**B**it **E**rror **R**atio - number of incorrectly transferred bits over number of correctly transferred bits) 10^{-9} and maximum level of surrounding illumination 10klux (daylight) [28]. Values are defined for a 15 degree deflection (off-alignment) of the receiver and the transmitter; output power for individual optical components is measured at up to 30 degrees. Directional transmitters (IR LEDs) for higher distances exist; however, they don't comply with the required 30 degree radiation angle. Speeds for IrDA v. 1.0 range from 2400 to 115200 kbps. In addition, IrDA v. 1.1 defines speeds 0.576 and 1.152 Mbps.

4.4.1 Protocol Stack

Communications protocols deal with many issues, and so are generally broken into layers, each of which deals with a manageable set of responsibilities and supplies needed capabilities to the layers above and below [42]. When placing the layers on top of each other, it can be get what is called a protocol stack, rather like a stack of pancakes or a stack of plates. An IrDA protocol stack is the layered set of protocols particularly aimed at point-to-point infrared communications and the

applications needed in that environment. Figure 4.13 is a picture of the IrDA protocol layers.

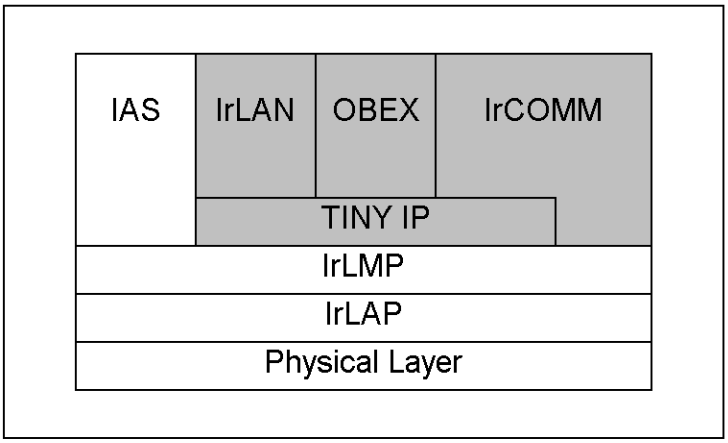

FIGURE 4.13 IrDA Protocol Layers [Suvak]

The layers within this stack can be divided into two groups: required and optional protocols.

4.4.1.1 Required IrDA Protocols

The required layers of an IrDA protocol stack are in unshaded boxes in the diagram above and include the following:

- Physical Layer: Specifies optical characteristics, encoding of data, and framing for various speeds.
- IrLAP: Link Access Protocol. Establishes the basic reliable connection.
- IrLMP: Link Management Protocol. Multiplexes services and applications on the LAP connection.
- IAS: Information Access Service. Provides a "yellow pages" of services on a device.

4.4.1.2 Optional Protocols

The optional protocols are shown above in shaded boxes. The use of the optional layers depends upon the particular application. The optional protocols are:

- TinyTP: Tiny Transport Protocol. Adds per-channel flow control to keep things moving smoothly. This is a very important function and is required in many cases.
- IrOBEX: The Object Exchange protocol. Easy transfer of files and other data objects.
- IrCOMM: Serial and Parallel Port emulation, enabling existing apps that use serial and parallel communications to use IR without change.
- IrLAN: Local Area Network access, enabling walk-up IR LAN access for laptops and other devices.

When the stack layers shown figure 4.13 are integrated into an embedded system, the picture may look more like the figure 4.14:

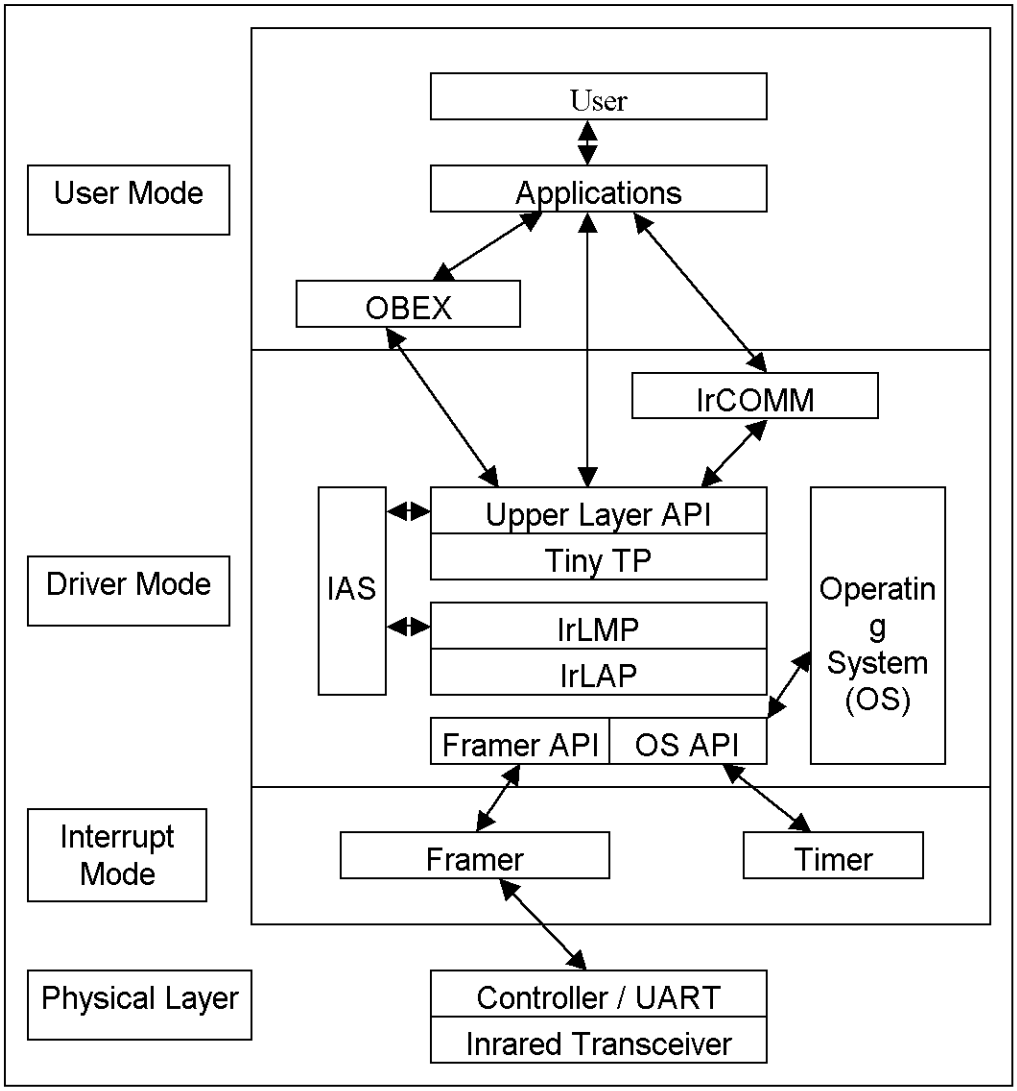

FIGURE 4.14 The stack layers integrated into an embedded system [Suvak]

4.4.2 Physical Layer and the Framer

The Physical layer includes the optical transceiver, and deals with shaping and other characteristics of infrared signals including the encoding of data bits, and some framing data such as begin and end of frame flags (BOFs and EOFs) and cyclic redundancy checks (CRCs). This layer must be at least partially implemented in hardware, but in some cases is handled entirely by hardware.

In order to isolate the remainder of the stack from the ever-changing hardware layer, a software layer called the framer is created. Its primary responsibility is to accept incoming frames from the hardware and present them to the Link Access Protocol layer (IrLAP). This includes accepting outgoing frames and doing whatever is necessary to send them. In addition, the framer is responsible for changing hardware speeds at the bidding of the IrLAP layer, using whatever magic incantations the hardware designer invented for that purpose (these signals have not yet been standardized).

4.4.3 IrLAP -Link Access Protocol

Immediately above the framer we encounter the IrLAP layer, also known as the Link Access Protocol, or LAP for short. IrLAP is a required IrDA protocol corresponding to OSI layer 2 (data link protocol). It is based on High-Level Data Link Control (HDLC) and Synchronous Data Link Control (SDLC) with extensions for some unique characteristics of infrared communications.

IrLAP provides reliable data transfer using the following mechanisms:

- Retransmission.
- Low-level flow control. (TinyTP provides high-level flow control and should almost always be used in place of IrLAP flow control.)
- Error detection.

By dealing with reliable data transfer at a low level, upper layers are free from this concern and can be assured that their data will be delivered (or at least that they will be informed if it was not). Data delivery might fail if the beam path were blocked. For instance, someone could put a coffee cup in the path of the infrared beam. IrLAP alerts the upper layer so that higher-level layers can deal with the

problem appropriately. As an example, an application sitting on the stack could be alerted of an interruption in data flow, allowing it to alert the user through some interface. The user could then potentially remedy the problem (by moving the coffee cup) without dropping the connection or losing the data transferred to that point.

4.4.4 IrLMP -Link Management Protocol

The IrLMP layer depends upon the reliable connection and negotiated performance provided by the IrLAP layer. IrLMP is a required IrDA layer, and provides the following functionality:

- Multiplexing -LMP allows multiple IrLMP clients to run over a single IrLAP link.
- Higher level discovery, consisting of:
- Address conflict resolution on IrLAP Discovery. Handles the case of multiple devices with the same IrLAP address by telling them to generate new addresses.
- Information Access Service (IAS). A "yellow pages" describing the services available on a device.

4.4.4.1 IrLMP Terminology

In order to have multiple IrLMP connections on a single IrLAP connection, there must be some higher level addressing scheme. The following terminology is used to describe this addressing:

- LSAP (Logical Service Access Point): The point of access to a service or application within IrLMP (for example, a printing service).It is referenced with a simple one byte number, the LSAP-SEL.
- LSAP-SEL (LSAP Selector): A one byte number that corresponds to an LSAP. Think of this as the address of a service within the LMP multiplexor.

Given the limited number of LSAP-SEL values, services are not assigned fixed "port addresses" as in TCP/IP. Instead, services have fixed published names, and the LMP IAS (yellow pages) is used to look up the LSAP-SEL for a desired service.

4.4.4.2 IrLMP Services

Not all services are necessary in all devices, and the specification (along with the IrDA Lite standard) describes the minimum requirements. Notice that this set is identical to the set listed in the IrLAP section; it is a common feature of protocol stacks for operations to propagate upward like this, with each layer adding its particular contribution.

- Device Discovery: Finds out additional information about devices in the IR space.
- Connect: Establishes a connection between a pair of services at the LMP level.
- Data -send the data back and forth
- Disconnect: Closes this LMP connection. Note that this does not necessarily close the LAP connection other LMP connections may still be open.

4.4.5 IAS -The Information Access Service

The IAS, or Information Access Service, acts as the "yellow pages" for a device. All of the services/applications available for incoming connections must have entries in the IAS, which can be used to determine the service address (LSAP-SEL). The IAS can also be queried for additional information about services.

A full IAS implementation consists of client and server components. The client is the component that makes inquiries about services on the other device using the Information Access Protocol (IAP, used only within the IAS). The server is the component that knows how to respond to inquiries from an IAS client. The server uses an information base of objects supplied by the local services/applications. In fixed-purpose embedded systems this may be a hard-coded collections of objects, while in a PDA there may be APIs for registering and de-registering services. Note that devices, which never initiate LMP connections, might include an IAS server only.

4.4.6 TinyTP -the Tiny Transport Protocol

To put TinyTP in its proper perspective, it would help to review the layers covered so far:

- Physical layer defines the hardware requirements and low-level framing of the data.
- IrLAP provides reliable, sequenced data, and trouble-free connection at agreed upon parameters with automatic negotiation to best common parameters.
- IrLMP provides multiplexing of services onto the LAP connection and the IAS "yellow pages" of services available for incoming connection.

TinyTP (TTP for short) is an optional IrDA layer, although it is so important that it should generally be considered a required layer (except in the case of current printing solutions). TTP provides two functions:

- Flow control on a per-LMP-connection (per-channel) basis.
- SAR (segmentation and reassembly)

TTP adds one byte of information to each IrLMP packet to perform its task.

4.4.7 IrDA Lite

This section briefly describes a specification which does not create a new layer, but which modifies layers already described.

The IrDA Lite specification describes a set of design and implementation strategies that together yield the smallest possible implementation that will still perform connection-oriented communications with a full IrDA implementation.

Naturally, the ultimate size of the stack will depend heavily on the hardware, the software tools available, and the experience and skills of the development team. However, the experience suggests that primaries under 10 Kbytes code size and secondaries under 5K are feasible on common CISC processors used in embedded systems. RAM usage can be as low as a few hundred bytes, most of which is needed to buffer incoming frames.

The IrDA Lite specification is composed of a number of strategies. A developer may choose to implement all of them, or only the ones appropriate to a particular

device. For instance, some of the strategies severely limit the performance of the stack:

- Speeds restricted to 9600 bps.
- LAP packet size restricted 64 bytes

While the most severely constrained devices (watches, for instance) may both need and tolerate these constraints, many devices (such as digital cameras) need high performance. Some strategies do not affect performance at all, so a judicious choice is in order to balance the needs for performance, functionality, and size.

4.4.8 IrOBEX -Object Exchange Protocol

IrOBEX is an optional application layer protocol designed to enable systems of all sizes and types to exchange a wide variety of data and commands in a resource-sensitive standardized fashion. It addresses one of the most common applications on either PCs or embedded systems: take an arbitrary data object (a file for instance), and send it to whoever the infrared device is pointing to. It also provides some tools to enable the object to be recognized and handled intelligently on the receiving side. The potential range of objects is wide, encompassing not only traditional files, but also pages, phone messages, digital images, electronic business cards, database records, hand-held instrument results, or diagnostics and programming. The common thread is that the application doesn't need or want to get involved in managing connections or dealing with the communications process at all. Just take the object and ship it to the other side. It is very similar to the role that HTTP serves in the Internet protocol suite, although HTTP is very "pull"-oriented in its fundamental design, while OBEX is more evenly balanced [42].

4.4.9 IrCOMM -Serial and Parallel Port Emulation and Service Types

When the IrDA standards were developed, there was a strong desire to allow existing PC applications that use serial and parallel ports to operate via infrared without change. These applications, collectively known as "legacy applications", included printing, file transfer applications such as LapLink or Carbon Copy, and modem communications.

However, IrDA infrared communications differs significantly from serial and parallel communications. For instance, both serial and parallel cables have individual circuits over which signals can be sent independently and concurrently. By contrast, infrared has a single beam of light, and all information must be fitted into LMP or higher layer packets in a serial stream.

The IrCOMM standard was developed to solve these problems and allow legacy applications to be used over infrared with a minimum of hassle. The key feature of IrCOMM is the definition of a so-called control channel to carry the non-data circuit information. In the stack picture, IrCOMM rests on top of IrLMP and TinyTP.

IrCOMM is an optional IrDA protocol that applies only to certain applications .In general, new applications are better served if they avoid IrCOMM and use other IrDA applications protocols such as IrOBEX, IrLAN, or TinyTP directly. This is because IrCOMM masks some of the useful features built into the lower protocols. After all, its job is to make IrDA look like serial and parallel media that do not have handy features like automatic negotiation of best common parameters and a "yellow pages" of available services.

Because different applications use the non-data circuits of serial and parallel communications to varying degrees, four service types are defined in IrCOMM:

- 3-Wire Raw (Parallel and Serial Emulation): Sends data only, no non-data circuit information and hence no control channel. Runs directly on IrLMP.
- 3-Wire (Parallel and Serial Emulation): Minimal use of control channel. Uses Tiny TP.
- 9-Wire (Serial emulation only): Uses control channel for status of standard RS-232 non-data circuits. Uses Tiny TP.
- Centronics (Parallel emulation only): Uses control channel for status of Centronics non-data circuits. Uses Tiny TP.

4.4.10 IrLAN -LAN Access

The final optional protocol discussed is IrLAN. It is mentioned only briefly because it is not an approved standard at this time, nor is its use widespread in the

world of embedded systems it primarily serves as an extremely convenient connection between portable PCs and office LANs.

IrLAN offers three models of operation:

- Enable a computer to attach to a LAN via an Access Point Device (sometime called an IR LAN Adapter). The Hewlett Packard NetBeam IR is an example of this type of device.
- Enable two computers to communicate as though attached on a LAN in effect an instant LAN between a pair of machines, with access to the other machines' directories and other LAN capabilities.
- Enable a computer to attach to a LAN through a second computer already attached.

4.4.11 Some Applications

- Synchronizing data (contacts, schedule, arbitrary data bases) between PDA and PC.
- Walking up to a printer or copier and printing a document from a laptop, PDA, phone, or camera.
- Exchanging electronic business cards between PDA and someone's smart cell phone.
- Beaming a potential client some literature and sample code at a trade show.
- Internet/network access in meeting rooms, public phones (already widespread in Japan).
- Sending a digital photo from a camera to a PC, printer, slide viewer, or development kiosk.
- Making a payment at point of sale with all record keeping automated.
- Field repair of electronics/machinery using a laptop as a service/debugging console.

4.5 OpenAir

OpenAir is the proprietary protocol from Proxim [37]. As Proxim is one of the largest Wireless LAN manufacturer, they are trying to push OpenAir as an alternative to 802.11 through the WLIF (Wireless LAN Interoperability Forum).

OpenAir is a pre-802.11 protocol, using Frequency Hopping and 0.8 and 1.6 Mb/s bit rate (2FSK and 4FSK). The radio turnaround (size of contention slots and between packets) is much larger than in 802.11, which allow a cheaper implementation but reduces performance.

The OpenAir MAC protocol is CSMA/CA with MAC retransmissions, and heavily based on RTS/CTS, each contention slot contains a full RTS/CTS exchange, which offers good robustness but some overhead. A nice feature of the protocol is that the access point can send all its traffic contention free at the beginning of each dwell and then switch the channel back to contention access mode.

OpenAir doesn't implement any encryption at the MAC layer, but generates Network ID based on a password (Security ID). This provides some security only because Proxim controls the way all the implementation behave (they don't provide a way to synchronise to any network as 802.11 manufacturers do). OpenAir also provide coarse power saving.

4.6 IEEE 802.15

The 802.15 Wireless Personal Area Network (WPAN) effort focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks [60]. These WPANs address wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics; allowing these devices to communicate and interoperate with one another. The goal is to publish standards that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

4.7 IEEE 802.16

The mission of Working Group 802.16 is to develop standards and recommended practices to support the development and deployment of fixed broadband wireless access systems. IEEE 802.16 is a unit of the IEEE 802 LAN/MAN Standards Committee .

Chapter 5

BLUETOOTH

5.1 Introduction

Bluetooth is a new standard developed by a group of electronics manufacturers that will allow any sort of electronic equipment -- from computers and cell phones to keyboards and headphones -- to make its own connections, without wires, cables or any direct action from a user. It will enable users to connect a wide range of computing and telecommunications devices easily and simply, without the need to buy, carry, or connect cables. It delivers opportunities for rapid ad hoc connections, and the possibility of automatic, unconscious, connections between devices. It will virtually eliminate the need to purchase additional or proprietary cabling to connect individual devices. Because Bluetooth can be used for a variety of purposes, it will also potentially replace multiple cable connections via a single radio link [49].

Bluetooth is intended to be a standard that works at two levels:

- It provides agreement at the physical level -- Bluetooth is a radio-frequency standard.
- It also provides agreement at the next level up, where products have to agree on when bits are sent, how many will be sent at a time and how the parties in a conversation can be sure that the message received is the same as the message sent.

The standard defines a uniform structure for a wide range of devices to communicate with each other, with minimal user effort. Its key features are robustness, low complexity, low power and low cost. The technology also offers wireless access to LANs, PSTN, the mobile phone network and the Internet for a host of home appliances and portable handheld interfaces (figure 5.1).

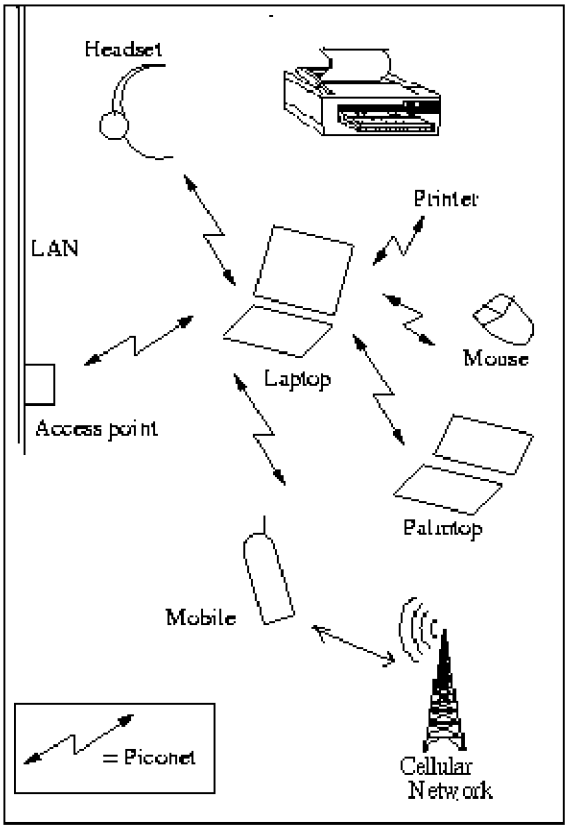

FIGURE 5.1 Wireless connectivity over Bluetooth [Handy Tel 2001]

The Bluetooth system has both the point-to-point connection and a point-to-multipoint connection. In point-to-multipoint connection, the channel is shared among several Bluetooth units. Two or more units sharing the same channel form a piconet (figure 5.2). There is one master unit and up to seven active slave units in a piconet. These devices can be in either of the states: active, park, hold and sniff. Each of the active slaves has an assigned 3-bit Active Member address (AM_ADDR) [3]. There can be additional slaves which remain synchronized to the master, but do not have a Active Member address. These slaves are not active and are referred to as parked. For the case of both active and parked units, all channel access is regulated by the master. A parked device has an 8-bit Parked Member Address (PM_ADDR), thus limiting the number of parked members to 256. A parked device remains synchronized to the master clock and can very quickly become active and begin communicating in the piconet. Multiple piconets with overlapping coverage areas form a scatternet. Any slave in one piconet can participate in another piconet as either a master or slave [3]. This is accomplished through time division multiplexing. In a scatternet, the two (or more) piconets are not synchronized in either time or

frequency. Each of the piconets operates in its own frequency hopping channel while any devices in multiple piconets participate at the appropriate time via time division multiplexing.

The standard is aimed at achieving global acceptance such that any Bluetooth device, anywhere in the world, can connect to other Bluetooth devices in its proximity, regardless of brand. Bluetooth enabled electronic devices connect and communicate wirelessly via short-range, ad hoc networks which are piconets. Each unit can simultaneously communicate with up to seven other units per piconet. Moreover, each unit can simultaneously belong to several piconets. These piconets are established dynamically and automatically as Bluetooth devices enter and leave the radio proximity.

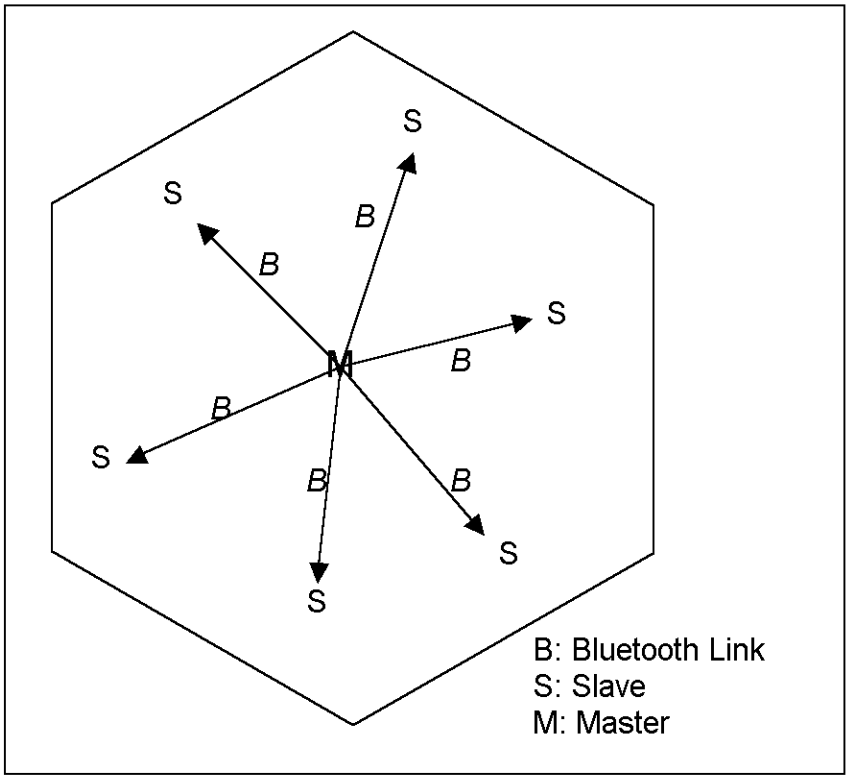

FIGURE 5.2 A Bluetooth Piconet [Blankenbeckler 2000]

Bluetooth was not designed for full WAN connectivity [33]. At best, the technology can be used for ad hoc networking when needed, but it is not designed for more than limited use. While other standards, like 802.11b, are designed for wide-reaching applications, Bluetooth simply does not have the bandwidth to handle full

network demands. Bluetooth is not meant to be a replacement for wireless LAN networks, but a cable replacement and ad hoc network.

Bluetooth is a good, low-power data/voice transmission standard that will be a real boon for certain applications. Imagine a cell phone or pager that automatically transfers to vibrate mode when entering a restaurant or theater. Or a laptop and GPS (global positioning system) that automatically feed a display in a car for directions. One of Bluetooth's design strengths is its low cost. The Bluetooth SIG says integrating this technology should add only $5 to the cost of a unit.

5.1.1 Specifications

Bluetooth operates in the 2.4-GHz Industrial, Scientific and Medical (ISM) band and uses a fast frequency-hopping technology to minimize interference to and from non-Bluetooth sources. This frequency hopping occurs nominally at 1,600 hops per second. The system has 78 possible channels. Channel spacing is 1 MHz in every industrialized country but France. (In France, it is limited to 22 possible channels on which to hop.)

Bluetooth has three power classes for transmitting: 100 milliwatt, 2.5 milliwatt and 1 milliwatt. The range for 100 milliwatt is 100 meters, 2.5 milliwatt is 10 meters and 1 milliwatt is 10 centimeters. But these ranges are variable and difficult to calculate. Materials, walls and interference from other 2.4-GHz sources all can change the range achieved.

By default, Piconets transmit up to 10 meters (about 30 feet) [31]. However, it can be increased to 100 meters by increasing the power output of 100 mW (milliwatts), as opposed to the 1 mW of default Bluetooth. However, compared to Global System for Mobile communications (GSM), which consumes between 1.5 and 2 Watts, this is still a weak signal. Manufacturers are working to make Bluetooth devices that adapt to the necessary proximity, so as not to consume more energy than is necessary.

Throughput for Bluetooth is rated at 1 Mbps under optimal conditions. With error correction overhead and other environmental factors, however, the real throughput should be about 700 Kbps to 800 Kbps. This should be more than enough for the Bluetooth cable-replacement designation.

Several other factors can influence Bluetooth's speed. The presence of other 2.4-GHz devices, such as an 802.11b WAN, can degrade performance of a Bluetooth piconet. Bluetooth traffic is separated into two types: data and voice.

Voice traffic has a much lower tolerance for interference than does data traffic. Ericsson conducted a study of interference from 802.11b on Bluetooth and found that when 802.11b is operating at normal traffic conditions, the more sensitive voice operation of Bluetooth is not affected when the transmitter and receiver are less than two meters apart. At a range of 10 meters, the probability of noticeable interference increases to eight percent.

The data link gets more interference than the voice link but is less susceptible to it. At a 10-meter range, throughput loss of more than 10 percent can occur with a 24 percent probability. The Ericsson study reports that the total loss of throughput due to interference from 802.11 WANs cannot exceed 22 percent. The 801.11 networks take up 17 channels at 2.4 GHz, and Bluetooth has 79 available channels. The IEEE's 802.15 working group is developing standards to let Bluetooth and 802.11b function better in shared space.

5.1.2 The Personal Area Network

Bluetooth's promoters are positioning it as the technology for the Personal Area Network (PAN), and are targeting appliances that don't require large flows -- like printers, personal computers, and mobile phones [31]. One concept that's been put forward is the mobile PAN: a communication device clipped to a belt could contain a GSM transceiver that communicates with the wider world. Meanwhile, the same device has a Bluetooth transceiver that communicates with the headset (replacing the mobile phone), the PDA, the MP3 player, allowing all these devices to communicate with each other and the larger world.

Since it is not a very expensive technology (between $5 and $20 per chip), it can easily be placed in many devices. Also, Bluetooth doesn't require an access point, unlike the traditional radio operator networks. It's well suited for mobile devices, since it can join a local Piconet quickly, as soon as the two devices are in a sufficient perimeter. And unlike infrared networks (like two Palm computers beaming each other), Bluetooth doesn't require to align objects for communication.

5.2 Bluetooth History

The name of "Bluetooth" comes from a Dutch ruler " Harald Bluetooth " in late 900 A.D. who ruled greater part of Denmark and Norway during his reign [53].

Bluetooth was invented in 1994 by L. M. Ericsson of Sweden. The Bluetooth Special Interest Group (SIG) was founded by Ericsson, IBM, Intel, Nokia and Toshiba in February 1998, to develop an open specification for short-range wireless connectivity. The group is now promoted by 3COM, Microsoft, Lucent and Motorola also. More than 1900 companies have joined the SIG.

5.3 System Challenges

Although, originally conceived to enable the design of universal wireless connections for laptops, computers and cellular telephones, it quickly became apparent that there were many other applications for the Bluetooth standard. Thus, the Bluetooth standard not only tries to overcome the limitations of the wired networks but also offers a variety of other services and creates opportunities for new usage models.

5.3.1 System Requirements

The Bluetooth system is now recognized more than just a cable replacement technology. Various innovative usage models have opened up new areas where Bluetooth can be used. These also impose many requirements on the system, some of them are:

- The most important requirement from the wireless link is that there should be a universal framework that offers means to access information across a diverse set of devices (for example, PDA's, laptops, PC's, mobile phones, home appliances etc.) in a seamless, user friendly and efficient manner.
- In the practical scenario all devices are not expected to be capable of all functionalities and users too may expect their familiar devices to perform their basic functions in the usual way. So Bluetooth must offer the facility for collaboration between devices, in the proximity of one another, where every device provides its

inherent function based on its form, user interface, cost and power, but additional services emerge due to the synergy resulting out of the collaboration.

- The standard must enable the devices to establish ad hoc connections. Also, introduced is the "unconscious connectivity" paradigm, where devices can connect to those in proximity almost without any user command or interaction. This shall allow utilization of various information recourses for the benefit of the user.
- Support for both data and voice is expected, as these are two most important kinds of information being transmitted over networks today. (The requirements of video and streaming multimedia are also being imposed on the future versions of Bluetooth).
- The standard should be able to incorporate new usage models without requiring any registration of the new service with a central authority.
- The communications should offer similar protection as in cables. There should not be any compromises on security in switching over to wireless.
- The implementations of the standard should be simple, small and power efficient for easy mobile usage.

It is necessary for the rapid deployment of the system and for the Bluetooth benefits to actually reach the users that a large number of devices be enabled with the Bluetooth standard. The devices to be enabled comprise a highly non-uniform set and no single company can have the expertise to manufacture all these. For this and other reasons, the Bluetooth standard has been made royalty free and its worldwide acceptance should be facilitated.

5.3.2 Technical Challenges

The above requirements involve great technical complexity not only in terms of the functionalities to be provided but also in terms of the power and size requirements. The technology designed to meet the above requirements must face the following technical challenges:

1. The system has to use an unlicensed band for universal acceptance and usage. Thus the Industrial, Scientific and Medical (ISM) band has been selected for Bluetooth. The challenge here is to make the system robust to interference from other sources in this band, which include not only ISM band communication systems but

also microwave ovens. Preferably, each transmitter itself should use the minimum power required so as not to increase the noise for other users.

2. The transceivers should be able to adapt to a rapidly changing environment, as the devices will usually be mobile. The well-known problems in wireless systems such as multipath fading must be handled. Also, the connection establishment and routing protocols have to operate in an environment where the number, location and variety of Bluetooth devices will change dynamically with fair amount of rapidity.

3. The size of the implementation should be small for easy integration into handheld and mobile devices.

4. The power consumption should not be more than a small fraction of the host device into which the Bluetooth capability is to be introduced.

5. The technology should be adaptable to devices of varying computing power and memory recourses. This will ensure that more and more devices can inter operate.

6. Automatic and unconscious connection establishment must be provided. The number and identity of devices in proximity will change quite frequently and it will be very inconvenient to establish connections manually each time. Also, the number of devices will be too large for most users to be able to remember or search the device address of the device they need to connect to.

7. Synchronization of clocks among the communicating units will have to be achieved. As each unit will have its own free running clock with its own drift, carrying out successful communication, especially CDMA, is a challenge in itself.

8. Security considerations have to be satisfied. The Bluetooth devices will be part of people's personal usage and will contain and communicate their personal information, sensitive business information or other data, which must be protected from being spoofed or mutilated. Encryption facility must thus be provided among other security features.

9. There are some existing wireless applications in personal and office area networks, which provide services similar to the ones provided by Bluetooth, like the IrDA OBEX and HomeRF. These services though similar, have certain differentiating features, which make them more suitable to certain classes of applications. Thus, to achieve complete integration, Bluetooth must provide means to inter operate with these other technologies in at least those services for which they

are better suited. It will be advantageous for the standard to be amenable to existing higher layer protocols such as TCP-IP and WAP for speeding up development.

The products should provide a good out of the box experience, that is, they should provide high value with existing applications.

5.4 The Basic Bluetooth System Architecture

As it seen from figure 5.3 that the protocol stack consists of a radio layer at the bottom, which forms the physical connection interface. The baseband and Link Manager Protocol (LMP) that reside over it are basically meant to establish and control links between Bluetooth devices. These three bottom layers are typically implemented in hardware/firmware. The Host Controller layer is required to interface the Bluetooth hardware to the upper protocol- Logical Link Control and Adaptation Protocol (L2CAP). The host controller is required only when the L2CAP resides in software in the host. If the L2CAP is also on the Bluetooth module, this layer may not be required as then the L2CAP can directly communicate with the LMP and baseband. Applications reside above L2CAP. Above the data link layer, RFCOMM and network level protocols provide different communication abstractions [20]. RF-COMM provides serial cable emulation using a subset of the ETSI GSM 07.10 standard.

5.5 Link Manager

The Link Manager (LM) software entity carries out link setup, authentication, link configuration, and other protocols.

The Link Manager discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).

The basic functions of LMP can be classified as:

1. Piconet management
2. Link configuration
3. Security functions

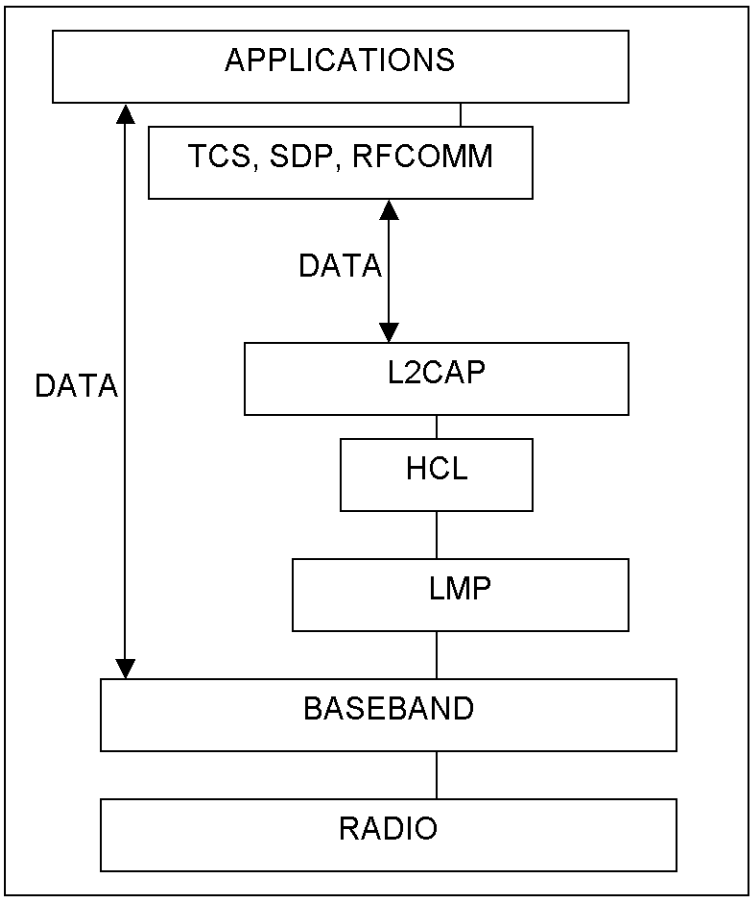

FIGURE 5.3 The Bluetooth Protocol Stack

Any two or more devices that need to communicate must establish a piconet among themselves. Devices can be part of many piconets at the same time (figure 5.4). In this figure

a) A piconet between two devices,

b) A piconet between many devices,

c) A scatternet, a combination of piconets with some devices common to the piconets are illustrated.

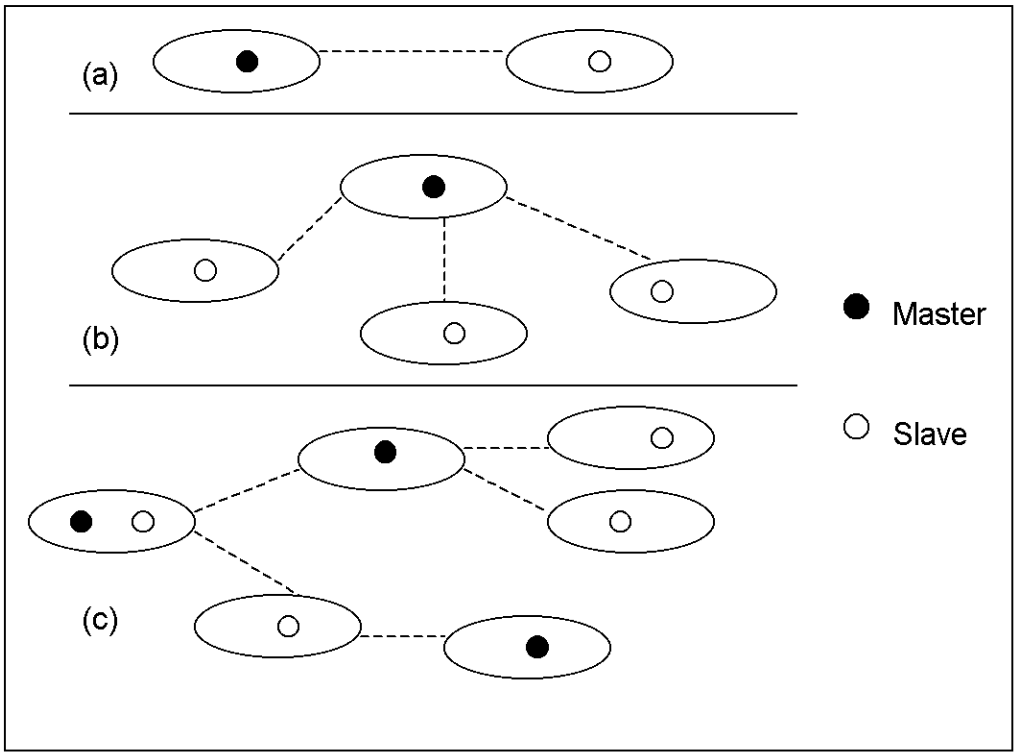

FIGURE 5.4 Piconets and Scatternets

LMP provides below services:

- Sending and receiving of data,
- Name request (the Link Manager has an efficient means to inquire and report a name or device ID up to 16 characters in length),
- Link address inquiries,
- Connection set-up,
- Authentication,
- Link mode negotiation and set-up, e.g. data or data/voice (this may be changed during a connection. The Link Manager decides the actual frame type on a packet-by-packet basis),
- Setting a device in sniff mode (in sniff mode, the duty cycle of the slave is reduced: it listens only every M slot where M is negotiated at the Link manager. The master can only start transmission in specified time slots spaced at regular intervals),
- Setting a link device on hold (in hold mode, turning off the receiver for longer periods saves power. Any device can wake up the link again, with an average latency of 4 seconds. This is defined by the Link Manager and handled by the Link Controller),

• Setting a device in park mode when it does not need to participate on the channel but wants to stay synchronized. It wakes up at regular intervals to listen to the channel in order to re-synchronize with the rest of the piconet, and to check for page messages.

5.6 Bluetooth Baseband

The baseband describes the specifications of the digital signal processing part of the hardware - the Bluetooth link controller, which carries out the baseband protocols and other low-level link routines. The baseband is the layer that controls the radio. The frequency hop sequences are provided by this layer. Baseband also takes care of lower level encryption for secure links. The packet handling over the wireless link is the responsibility of baseband.

The baseband provides the functionalities required for devices to synchronize their clocks and establish connections. Inquiry procedures for discovering the addresses of devices in proximity are also provided. Error correction for packets is provided depending on the type of packet. Various packet types are specified for some common applications, differing in their data capacity and error correction overheads. Five different channel types are provided for control information, link management information, user synchronous data, user asynchronous data and isosynchronous data. Data whitening is also carried out at this layer. The functions required for generating encryption keys and link keys are defined.

5.6.1 Baseband Link And Packet Types

The link type defines what type of packets can be used on a particular link. The Bluetooth baseband technology supports two link types:

- Synchronous Connection Oriented (SCO) type (used primarily for voice),
- Asynchronous Connectionless (ACL) type (used primarily for packet data).

Both link types use a Time Division Duplex (TDD) scheme for full-duplex transmissions.

5.6.2 Error Correction

There are three error-correction schemes defined for Bluetooth baseband controllers:

1. 1/3 rate forward error correction code (FEC),
2. 2/3 rate forward error correction code,
3. Automatic repeat request (ARQ) scheme for data.

The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However, in a reasonably error-free environment, FEC creates unnecessary overhead that reduces the throughput. Therefore, the packet definitions have been kept flexible as to whether or not to use FEC in the payload. The packet header is always protected by a 1/3 rate FEC; it contains valuable link information and should survive bit errors.

An unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot. For a data transmission to be acknowledged both the header error check and the cyclic redundancy check must be okay; otherwise a negative acknowledge is returned.

5.7 AD-HOC Connectivity

Most wireless communication systems like the public cellular phone networks-GSM, DAMPS, IS-95 or other private networks like Hiperlan-II, DECT or Personal Handyphony system, use a network architecture in which the radio units: base stations and mobile terminals are strictly distinct. This is advantageous in design as channel access, channel allocation, traffic control, interference minimization etc. can be taken care by the base stations, making the design of mobile terminals simpler. In ad hoc networks, there is no difference between radio units. Communication is peer to peer with no central controller. Conventionally in ad hoc wireless networks, all devices sharing a common space will share the same channel, and will mutually coordinate in it's sharing. In Bluetooth usage models however, even this is not sufficient as the number of Bluetooth devices in a given region of space may be very large and only a few of them may need to communicate among themselves, making mutual coordination among them very difficult and unlikely. This has led to the

concept of scatternets: a group of networks in the same space but communicating over different channels, with some overlapping devices. There need not be any coordination among devices belonging to different networks within the scatternet. In figure 5.5 three different networks are illustrated:

(a) A cellular network with squares representing stationary base stations

(b) A conventional ad hoc system

(c) Scatter ad hoc network

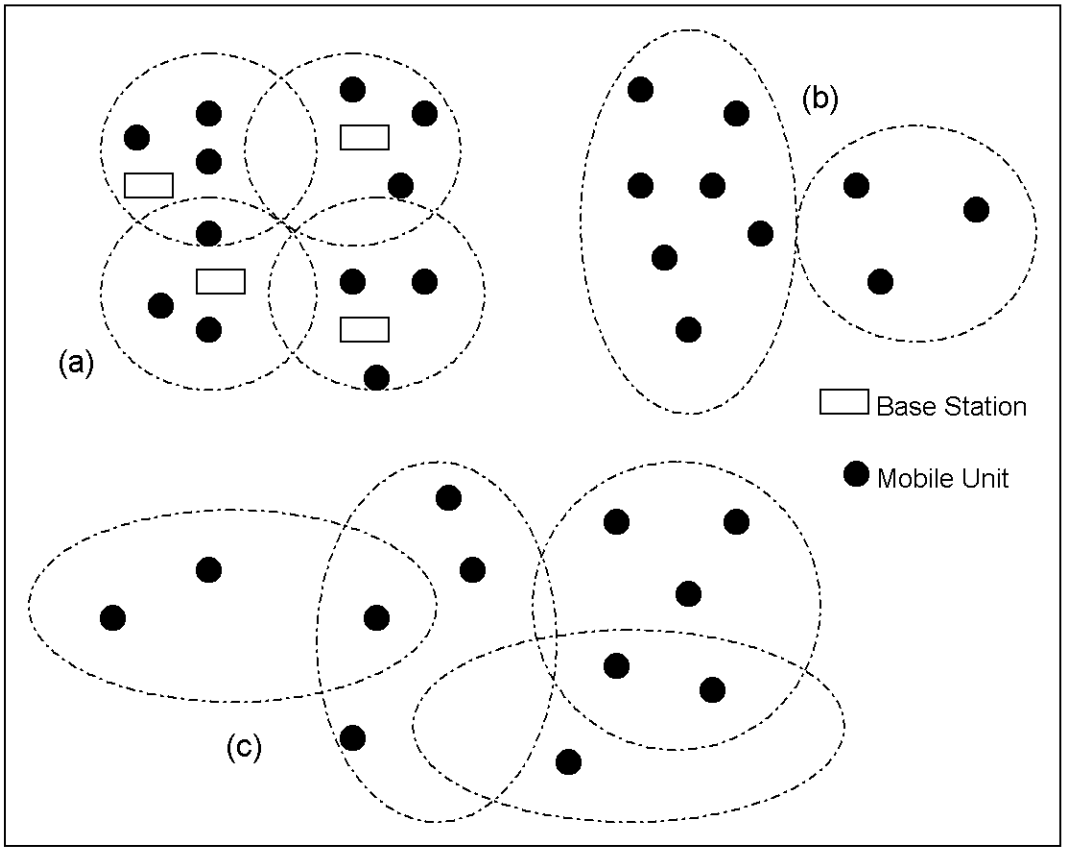

FIGURE 5.5 Different networks within the scatternet

Thus it is clear that the Bluetooth system due to its very nature of application will have to use scatternet kind of ad-hoc connectivity. The major considerations in this design are:

- Choice of the radio spectrum.
- Connection establishment, and determining units in range that can be connected.
- Choice of the multiple access scheme.
- Channel allocation.
- Medium Access control.
- Service prioritization; voice may have higher priority over data.
- Interference, mutual and from other sources.
- Power consumption.
- Protection of data over the channel.

5.7.1 The Choice of The Radio Spectrum

The issues to be considered here are:

1. There will not be any coordination between operators as in a cellular network.
2. The spectrum must be available worldwide without the need for licenses. This will make the interoperability truly global. This is important as mobility is one main advantage for Bluetooth devices.

These considerations encourage the adoption of the ISM band (around 2.45GHz.) that is globally available. It is governed by different regulations in different parts of the world and hence the system must be designed considering the minimum common availability.

5.7.2 Medium Access Control

The choice of the Medium access scheme must take into account the lack of coordination among devices in the ISM band. Frequency Division Multiple Access (FDMA) cannot be used, as it does not satisfy the frequency spreading characteristics of the ISM spectrum. Time Division Multiple Access (TDMA) requires strict timing synchronization, which is rather cumbersome for ad hoc connections. Code Division Multiple Access (CDMA) is the clear choice as it fulfils the spreading requirements

and can work with uncoordinated systems. The next question is Direct Sequence (DS) or Frequency Hopping (FH). DS suffers from certain disadvantages like the requirement of a common timing reference, which is not a good idea in the scatternet ad-hoc scenario. Further, due to the near far problem, a coordinated power control is required. Finally, high data rates will require higher chip rates-which is not advisable due to the wide bandwidth and the resulting interference, and due to excessive current drain. FH, apart from taking care of these problems, offers other advantages. The average signal is spread over a large bandwidth but the instantaneous signal is only in a narrow band, making it easy to filter out a lot of potential interference. Bluetooth thus uses FH-CDMA. To keep interference effects minimal and to make the data robust, very short packets are used and the frequency hop rate is kept high-1600 hops per second.

5.7.3 Connection Establishment

The environment of a Bluetooth device will change dynamically with fair amount of rapidity. Further the number of devices will be quite large and new devices will usually be have to accessed whenever the user takes his device outside his usual workplace. Then some questions arise about finding the devices each other and establishing links over the CDMA channel. It is important that the devices should not depend on manual commands to establish connections. So the standard must provide for procedures using which a device can discover the addresses of other Bluetooth devices in its proximity without any user support. Further there should be some mechanism to start a link. This will require some synchronization to be achieved between the two devices.

When first establishing a network or adding components to a piconet, the units must be identified [20]. Units can be dynamically connected and disconnected from the piconet at any time. Two available options lead to connection times of typically 0.64 and 1.28 seconds respectively. This applies when the unit address is known and not more than about 5 hours have elapsed since the previous connection. A unit does not need to be connected at all times since only a typical delay of under one second is required to start a transaction. Hence, when not in use, the unit can be in a sleep state

(STANDBY) most of the time where only a Low Power Oscillator (LPO) is running. This is, of course, beneficial for battery operation.

Before any connections are made, all units are in standby mode. In this mode, an unconnected unit will only listen to messages every 1.28 seconds or 2.56 seconds depending on the selected option. Each time a unit wakes up, it will listen on one of 32 hop frequencies defined for this unit.

The connect procedure is initiated by one of the units, the master. A connection is made either by a PAGE message if the address is already known, or by the INQUIRY message followed by a subsequent PAGE message if the address is unknown. In the initial PAGE state, the paging unit (which is the master) will send a train of 16 identical page messages on 16 different hop frequencies defined for the unit to be paged (the slave). The train covers half the sequence of frequencies in which the slave can wake up. It is repeated 128 or 256 times (1.28 or 2.56 seconds) depending on the needs of the paged unit. If no response is received after this time, the master transmits a train of 16 identical page messages on the remaining 16 hop frequencies in the wake-up sequence. The maximum delay before the master reaches the slave is 2 times 1.28 seconds or 2.56 seconds if a periodicity of 1.28 seconds was chosen for paging and 5.12 seconds with 2.56 seconds periodicity respectively. Clearly a trade off between access delay and power savings exists due to the available choices.

The hop frequencies in the first page train are based on the master's slave clock estimate. The train will include the estimated wake-up hop, and 8 hops before and 7 hops after this hop. As a result, the estimate can be 7 hops in error and still the master reaches the slave with the first page train. Because the estimate is updated at each connection establishment, the acquisition delay is shorter when a shorter time has elapsed since the units were last connected. With a Low Power Oscillator (LPO) inaccuracy better than 250 ppm, the first train is still valid after at least 5-hours lapse with no connection.

That is, for a time period of at least 5 hours since the last connection, the average acquisition times are 0.64 seconds and 1.28 seconds respectively. If the first train does not cover the slave's wakeup frequency, the second train does and the aver-age acquisition delays are 1.92 seconds and 3.84 seconds [20].

The INQUIRY message is typically used for finding public printers, faxes and similar equipment with an unknown address. The INQUIRY message is very similar to the page message but may require one additional train period to collect all the responses.

If no data needs to be transmitted, the units may be put on HOLD where only an internal timer is running. When units go out of HOLD mode data transfer can be restarted instantaneously. Units may thus remain connected, without data transfer, in a low power mode. The HOLD is typically used when connecting several piconets. It could also be used for units where data needs to be sent very infrequently and low power consumption is important. A typical application would be a room thermostat which may need to transfer data only once every minute.

Two more low power modes are available, the SNIFF mode and the PARK mode. If we list the modes in increasing order of power efficiency, then the SNIFF mode has the higher duty cycle, followed by the HOLD mode with a lower duty cycle, and finishing with the PARK mode with the lowest duty cycle.

5.7.4 Medium Access Control and Channel Allocation

As noted earlier, a large number of independent channels need to exist in the same space, each serving its own participants. On the modulation scheme used, the data rate available is 1Mbps. So, to conserve capacity, only the units, which need to transfer data among themselves, should be put on a particular channel. For this reason, the concept of piconets has been introduced. Each channel is identified with a unique hop sequence and the clock of one coordinating device on that channel, referred to as the master. This channel called a piconet and multiple piconets that overlap in terms of devices connected are referred to as a scatternet. To simplify implementation of duplex communication, TDD has been applied. Each device transmits in alternate slots and uses the intermediate slots to receive (figure 5.6)

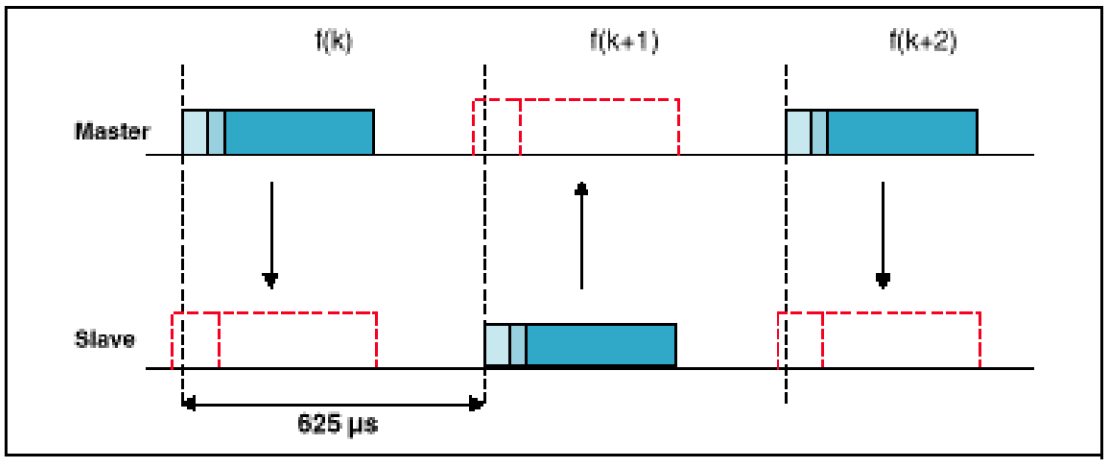

FIGURE 5.6 TDD scheme in Bluetooth [Haartsen]

The master of the piconet manages which device transmits when. Thus, the channel can be effectively shared. It can be noted that there are 79 frequencies in the hop sequence opening the possibility for 79 orthogonal frequency hop sequences. That can provide 80Mbps of data transfer capacity within a local space. However, as the Bluetooth devices do not coordinate, the hop sequences will not be orthogonal and the theoretical capacity of 80Mbps will not be reached.

5.7.5 Service Prioritization

Bluetooth devices intend to provide both voice communication as in mobile phones, headsets or voice browsers and also data communications to access networks in the traditional way. The voice channel must be synchronous and provide guarantees on delay and latency for acceptable voice quality. Thus a separate link to support voice is required which must be given priority over asynchronous data. Hence, Bluetooth uses two kinds of links:

- Asynchronous Connectionless-ACL.
- Synchronous Connection Oriented-SCO.

The SCO link is a point to point link in which resources are reserved-TDD slots at regular intervals are reserved to guarantee the continuity of the voice channel. The remaining slots can be used by ACL links. The SCO link is such that even during

paging, inquiry and scan procedures, which may be required for some parallel application, the synchronous packets can be transferred at their fixed slots.

Different link types may apply between different master-slave pairs of the same piconet and the link type may change arbitrarily during a session. The link type defines what type of packets can be used on a particular link. On each link type, 16 different packet types can be used. The packets differ in function and data bearing capabilities. For full duplex transmissions a Time Division Duplex scheme is used. Each packet is transmitted in a different hop channel than the previous packet.

The SCO link is full-duplex link between the master and a slave [20]. This link is established once by the master and kept alive until being released by the master. The SCO link is typically used for a voice connection. The master reserves the slots used for the SCO link on the channel.

The ACL link is packet oriented and supports both symmetric and asymmetric traffic. The ACL link makes a momentary connection between the master and any of the slaves for the duration of one frame (master-to-slave slot and slave-to-master slot). No slots are reserved. The master can freely decide which slave to address and in which order. The member subaddress in the packet header determines the slave. A polling scheme is used to control the traffic from the slaves to the master. The link is intended for asynchronous or isochronous data. However, if the master uses this link to address the same slave at regular intervals, it becomes a synchronous link. The ACL link supports both symmetric and asymmetric modes. In addition, modes have been defined with or without FEC, and with or without CRC and ARQ. The ACL link also supports broadcast messages from the master to all slaves in the piconet.

5.7.6 Interference

The ISM band being an unreserved band will have a variety of heterogeneous transmitters in its frequency range. Further, microwave ovens and lighting sources emit in this band-which was in fact the original reason for unlicensing this band. Another source that may be expected to be present in the same areas as the Bluetooth environment would be the 30dBm WLAN transmitters. Thus the Bluetooth devices must be immune to such interference. Two common approaches are suppression and avoidance. Suppression, which can be obtained by coding or DS spreading, makes

less sense for Bluetooth because the near far ratios may be too high to handle with practical attainable coding gains. Interference avoidance is more attractive because the desired signal is transmitted at points in frequency and/or time where interference is low or absent. Avoidance in frequency is more practical because most radio systems are band limited and most probably it should be possible to find some band where the interference is fairly low. Further, robustness to errors is required as interference in short bursts due to collisions or other reasons may corrupt data packets in a wireless environment. This calls for error correction at higher layers above the physical link. For this purpose Bluetooth has chosen to provide an acknowledgement based scheme with automatic repeat request (ARQ). The header information in packets that is very critical to the link operation is protected first by a cyclic redundancy check and further a 1/3 rate Forward Error Check (FEC) is applied, which repeat each bit three times. For protection of data various levels of redundancy are supported differing in their overheads. The required packet type may be used by an application as per its requirements. For the synchronous voice links it is difficult to retransmit a packet in case of errors, hence the CVSD voice coding is employed which is robust to high bit error rates.

5.7.7 Modulation Scheme Used

In the ISM band the bandwidth of signals is limited to 1MHz. For robustness, a Binary modulation scheme has been chosen. This is what places the data rate limit of 1Mbps. For FH systems and support for bursty data traffic, a non coherent detection scheme is most appropriate. A Gaussian prefiltered Frequency Shift Keying (FSK) is used with a nominal modulation index of 0.3. The Time Bandwidth product of the Gaussian prefilter is 0.5. Logical ones are sent as positive frequency deviations and zeros as negative frequency deviations. In this technique, demodulation can be simply accomplished by a limiting FM discriminator, thus enabling the implementation of low cost radio units (figure 5.7).

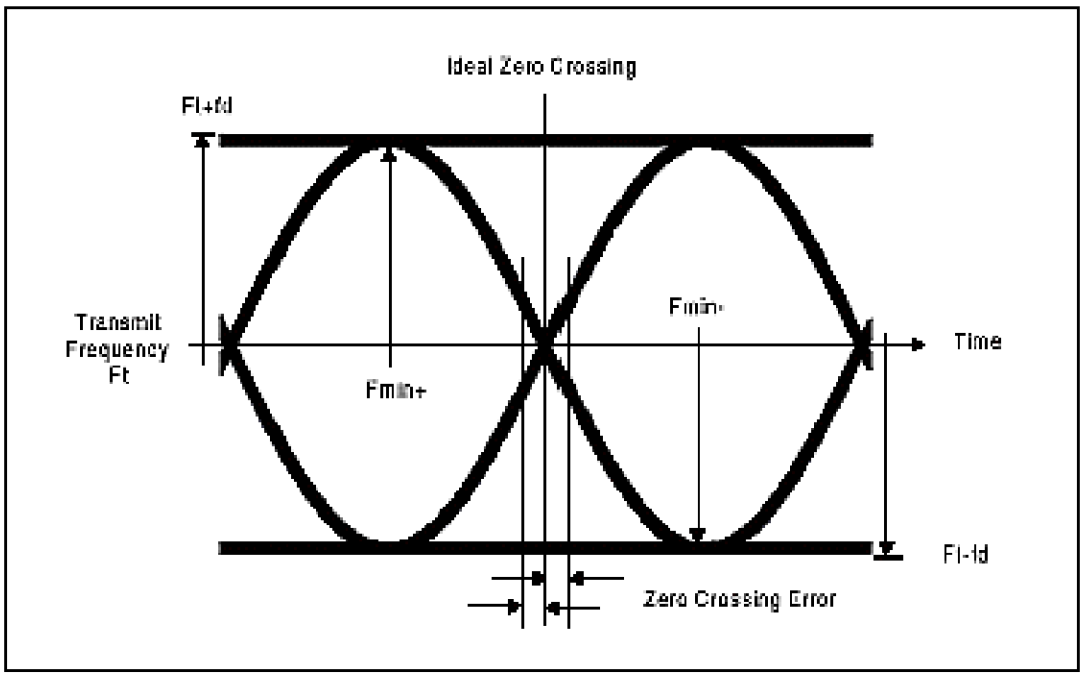

FIGURE 5.7 The Modulation scheme used in Bluetooth [Haartsen]

5.7.8 Protection of Data

Bluetooth devices will usually carry and transmit a person's very personal data as they will be the interface to most of her valuable information resources. Thus, it is essential that no compromise on security be made while shifting from the wired interfaces to wireless ones. For this reason it is necessary to provide data encryption facility. Further, services offered through Bluetooth access points may have to be limited to a certain set of authorized users. This means that the standard should provide some mechanism to allow restricted access and identification of registered devices. Keeping both these requirements in mind, Bluetooth provides both link level encryption and authentication. These are controlled by providing a PIN (Personal Identification Number) to users. This number must be known by the user if he has to access a secured device. Thus, access control can be implemented. To ensure safety of encryption long encryption keys are used. Further these keys are not transmitted over the wireless channel, rather other parameters are intimated using which in combination with the information specifically known to authenticated devices, the keys can be generated. Different types of keys have been provided to allow for varying computing power on non-uniform devices. Apart from encryption at link

level, which uses 128 bit keys, regarded as fairly safe currently, there is always the option to further encrypt at the application layer itself. Link level encryption however allows a universal standard.

5.7.9 Power Consumption

Wireless connectivity is rendered useless if a power cable has to be connected. Mobility can be achieved only if the device is battery operated. Thus power consumption becomes an important consideration. Attempts have been made to keep power consumption to the minimum, preferably not more than a small fraction of the power consumed by its host device. Various low power modes (Hold, Sniff, Park) have been provided to allow the unit to adjust its power consumption to the bare minimum required and use full power only when actively engaged in communication.

5.8 Design of The Higher Layers

Some issues to be considered in the design of the higher layers were that the Bluetooth module should be easily integrable into any existing device that may benefit from being connected. Further, for rapid acceptance into the market, it should be possible for existing applications developed over the conventional protocols to be easily portable to the Bluetooth platform. In addition, other wireless initiatives like IrDa OBEX, WAP and HomeRF should also be able to interoperate with this standard. Keeping this in view, interface points where existing protocols may be used over the Bluetooth platform have been provided.

The Bluetooth devices have some peculiar needs not covered by existing protocols, like the need to discover what all services are available on devices in proximity. Special protocols have been provided to meet these needs. For instance to discover services on nearby devices, Service Discovery Protocol (SDP) is provided. Similarly, for voice channel control, TCS (Telephony Control Specification) has been provided. To allow the applications using the serial port, an emulation of the same, the RFCOMM has been provided. Thus, an attempt has been made to provide for interoperability and universal acceptance. Existing protocols can be supported over Bluetooth for rapid development of applications.

The Host Controller Interface is a special layer added to the Bluetooth protocol stack due to the special requirements that can be met using this interface. This is especially relevant for integrating Bluetooth into computers and other general-purpose devices. As the lower three layers of the protocol stack-upto the LMP, may be implemented in hardware and the rest may be in software, especially the L2CAP, which is the main interface to applications, a means of communication is required between the two levels. In a PC or a laptop, the Bluetooth module would be preferred as an add-on card, either o the USB or the PCI. Then this Host Controller Interface provides the required functionalities for allowing the transfer of L2CAP data in the USB or PCI formats.

5.9 Bluetooth Security

The Bluetooth system is intended to be used as a uniform interface to all of a person's information sources and will thus be expected to transfer sensitive personal data. Security of the data is thus understandably an important issue. Further, Bluetooth devices are expected to be omnipresent and at some places the access to these devices by public users may have to be restricted. This calls for authentication procedures to be provided. As the channel used is wireless and the packets being transmitted are available to all members of a piconet, the security initialization communications should not send any information that can allow an unauthorized device to know the secret authentication keys. Further, the mechanisms should be appropriate for a peer-to-peer environment. The methods adopted by the Bluetooth standards take care of these issues. The scheme used is referred to as the challenge response scheme.

The application may itself encrypt its data for added security. That can add to the safety of the data, but the most of the authentication is based on the link level security procedures, as it is difficult to achieve uniformity in that step at the application level.

Security for Bluetooth devices provides link-level security plus encryption [33]. Security in a Bluetooth network is entirely device-based, not user-based, as in traditional systems. Bluetooth has three levels of security:

- Level 1: No security.
- Level 2: Service-level-enforced security. Security is established after channel negotiation.
- Level 3: Link-level-enforced security.

The Bluetooth SIG recommends that Level 2 be used in most instances. If Level 3 and full encryption are used, the ease of use and simplicity aspects of Bluetooth begin to fade. Level 3 would require user intervention for all services.

In Bluetooth, most security issues are expected to occur above the link layer, in the application or protocol layers. However, problems can occur at a purely physical level. It is also possible to cause denial of service (DoS) attacks against a wireless network by flooding the 2.4-GHz band with interference. Wireless networks are also vulnerable to passive eavesdropping attacks.

In one scenario, a potential hacker could simply listen for Bluetooth packets and extract data from them. The frequency-hopping characteristic of Bluetooth largely eliminates this problem. The hacker would have to know the exact sequence of hops and channels at 1,600 hops per second. Using an external encryption program to pre-encrypt the data before sending it across Bluetooth is recommended.

Other wireless solutions use more robust solutions like Wired Equivalent Privacy (WEP). However, implementing something like WEP on top of Bluetooth would once again restrict simplicity and ease of use.

Chapter 6

Global System for Mobile Communications (GSM)

6.1 History of GSM

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany [34]. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

- Good subjective speech quality
- Low terminal and service cost
- Support for international roaming
- Ability to support handheld terminals
- Support for range of new services and facilities
- Spectral efficiency
- ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990. Commercial service was started in mid-1991,

and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper interworking between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

6.2 Cellular Systems

6.2.1 The Cellular Structure

In a cellular system, the covering area of an operator is divided into cells [35]. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power.

The concept of cellular systems is the use of low power transmitters in order to enable the efficient reuse of the frequencies. In fact, if the transmitters used are very powerful, the frequencies cannot be reused for hundred of kilometers as they are limited to the covering area of the transmitter.

The frequency band allocated to a cellular mobile radio system is distributed over a group of cells and this distribution is repeated in all the covering area of an operator. The whole number of radio channels available can then be used in each

group of cells that form the covering area of an operator. Frequencies used in a cell will be reused several cells away. The distance between the cells using the same frequency must be sufficient to avoid interference. The frequency reuse will increase considerably the capacity in number of users.

In order to work properly, a cellular system must verify the following two main conditions:

- The power level of a transmitter within a single cell must be limited in order to reduce the interference with the transmitters of neighboring cells. The interference will not produce any damage to the system if a distance of about 2.5 to 3 times the diameter of a cell is reserved between transmitters. The receiver filters must also be very performant.
- Neighboring cells can not share the same channels. In order to reduce the interference, the frequencies must be reused only within a certain pattern.

In order to exchange the information needed to maintain the communication links within the cellular network, several radio channels are reserved for the signaling information.

6.2.2 Cluster

The cells are grouped into clusters. The number of cells in a cluster must be determined so that the cluster can be repeated continuously within the covering area of an operator. The typical clusters contain 4, 7, 12 or 21 cells. The number of cells in each cluster is very important. The smaller the number of cells per cluster is, the bigger the number of channels per cell will be. The capacity of each cell will be therefore increased. However a balance must be found in order to avoid the interference that could occur between neighboring clusters. This interference is produced by the small size of the clusters (the size of the cluster is defined by the number of cells per cluster). The total number of channels per cell depends on the number of available channels and the type of cluster used.

6.2.3 Types of cells

The density of population in a country is so varied that different types of cells are used:

6.2.3.1 Macrocells

The macrocells are large cells for remote and sparsely populated areas.

6.2.3.2 Microcells

These cells are used for densely populated areas. By splitting the existing areas into smaller cells, the number of channels available is increased as well as the capacity of the cells. The power level of the transmitters used in these cells is then decreased, reducing the possibility of interference between neighboring cells.

6.2.3.3 Selective Cells

It is not always useful to define a cell with a full coverage of 360 degrees. In some cases, cells with a particular shape and coverage are needed. These cells are called selective cells. A typical example of selective cells are the cells that may be located at the entrances of tunnels where a coverage of 360 degrees is not needed. In this case, a selective cell with a coverage of 120 degrees is used.

6.2.3.4 Umbrella Cells

A freeway crossing very small cells produces an important number of handovers among the different small neighboring cells. In order to solve this problem, the concept of umbrella cells is introduced. An umbrella cell covers several microcells. The power level inside an umbrella cell is increased comparing to the power levels used in the microcells that form the umbrella cell. When the speed of the mobile is too high, the mobile is handed off to the umbrella cell. The mobile will

then stay longer in the same cell (in this case the umbrella cell). This will reduce the number of handovers and the work of the network.

6.3 Services Provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signaling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved.

Using the ITU-T definitions, telecommunication services can be divided into bearer services, teleservices, and supplementary services. The most basic teleservice supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bidirectional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval.

Supplementary services are provided on top of teleservices or bearer services. In the current (Phase I) specifications, they include several forms of call forward

(such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

6.4 Architecture of the GSM Network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 6.1 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across the A interface.

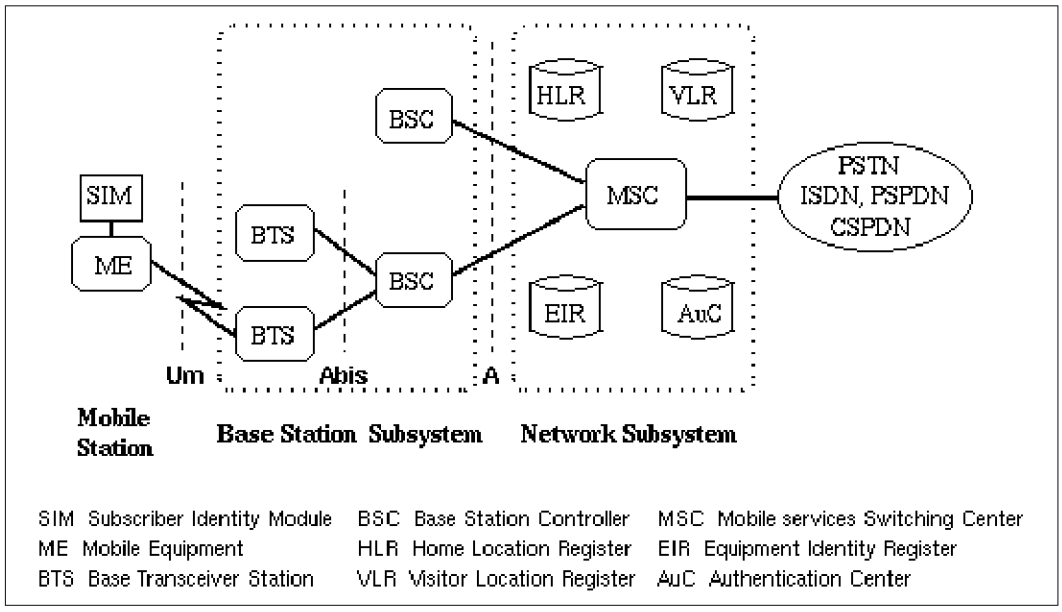

FIGURE 6.1 General architecture of a GSM network [Scourias 1997]

6.4.1 Mobile Station

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

6.4.2 Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio tranceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

6.4.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. The MSC contains no information about particular mobile stations (this information is stored in the location registers).

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is

a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

6.5 Radio Link Aspects

The International Telecommunication Union (ITU), which manages the international allocation of radio spectrum (among many other functions), allocated the bands 890-915 MHz for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station) for mobile networks in Europe. Since this range was already being used in the early 1980s by the analog systems of the day, the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed. Eventually, GSM will be allocated the entire 2x25 MHz bandwidth.

6.5.1 Multiple Access And Channel Structure

Since radio spectrum is a limited resource shared by all users, a method must be devised to divide up the bandwidth among as many users as possible. The method chosen by GSM is a combination of Time- and Frequency-Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a *burst period* and it lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a *TDMA frame* (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame.

Channels are defined by the number and position of their corresponding burst periods. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used by mobile stations in idle mode.

6.5.1.1 Traffic Channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused. TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics.

In addition to these *full-rate* TCHs, there are also *half-rate* TCHs defined, although they are not yet implemented. Half-rate TCHs will effectively double the capacity of a system once half-rate speech coders are specified (i.e., speech coding at around 7 kbps, instead of 13 kbps). Eighth-rate TCHs are also specified, and are used for signaling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

6.5.1.2 Control Channels

Common channels can be accessed both by idle mode and dedicated mode mobiles. The common channels are used by idle mode mobiles to exchange the signaling information required to change to dedicated mode. Mobiles already in dedicated mode monitor the surrounding base stations for handover and other information. The common channels are defined within a 51-frame multiframe, so that dedicated mobiles using the 26-frame multiframe TCH structure can still monitor control channels. The common channels include:

Broadcast Control Channel (BCCH)

Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency-hopping sequences.

Frequency Correction Channel (FCCH) and Synchronisation Channel (SCH)

Used to synchronise the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM

network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).

Random Access Channel (RACH): Slotted Aloha channel used by the mobile to request access to the network.

Paging Channel (PCH): Used to alert the mobile station of an incoming call.

Access Grant Channel (AGCH): Used to allocate an SDCCH to a mobile for signaling (in order to obtain a dedicated channel), following a request on the RACH.

6.5.1.3 Burst Structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signaling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.

The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts (thus allowing synchronization). The access burst is shorter than the normal burst, and is used only on the RACH.

6.5.2 Speech Coding

GSM is a digital system, so speech that is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited -- Linear Predictive Coder (RPE--LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not change

very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps. This is the so-called Full-Rate speech coding. Recently, an Enhanced Full-Rate (EFR) speech coding algorithm has been implemented by some North American GSM1900 operators. This is said to provide improved speech quality using the existing 13 kbps bit rate.

6.5.3 Channel Coding and Modulation

Because of natural and man-made electromagnetic interference, the encoded speech or data signal transmitted over the radio interface must be protected from errors. GSM uses convolutional encoding and block interleaving to achieve this protection. The exact algorithms used differ for speech and for different data rates. The method used for speech blocks will be described below.

Recall that the speech codec produces a 260 bit block for every 20 ms speech sample. From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others. The bits are thus divided into three classes:

- **Class Ia** 50 bits - most sensitive to bit errors
- **Class Ib** 132 bits - moderately sensitive to bit errors
- **Class II** 78 bits - least sensitive to bit errors

Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection. If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded. It is replaced by a slightly attenuated version of the previous correctly received frame. These 53 bits, together with the 132 Class Ib bits and a 4 bit tail sequence (a total of 189 bits), are input into a 1/2 rate convolutional encoder of constraint length 4. Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolutional encoder thus outputs 378

bits, to which are added the 78 remaining Class II bits, which are unprotected. Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps.

To further protect against the burst errors common to the radio interface, each sample is interleaved. The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts. Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

Recall that each time-slot burst is transmitted at a gross bit rate of 270.833 kbps. This digital signal is modulated onto the analog carrier frequency using Gaussian-filtered Minimum Shift Keying (GMSK). GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions. The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station. The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled so as to limit adjacent channel interference, and allow for the co-existence of GSM and the older analog systems (at least for the time being).

6.5.4 Multipath Equalization

At the 900 MHz range, radio waves bounce off everything - buildings, hills, cars, airplanes, etc. Thus many reflected signals, each with a different phase, can reach an antenna. Equalization is used to extract the desired signal from the unwanted reflections. It works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training sequence transmitted in the middle of every time-slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

6.5.5 Frequency Hopping

The mobile station already has to be frequency agile, meaning it can move between a transmit, receive, and monitor time slot within one TDMA frame, which normally are on different frequencies. GSM makes use of this inherent frequency

agility to implement slow frequency hopping, where the mobile and BTS transmit each TDMA frame on a different carrier frequency. The frequency hopping algorithm is broadcast on the Broadcast Control Channel. Since multipath fading is dependent on carrier frequency, slow frequency hopping helps alleviate the problem. In addition, co-channel interference is in effect randomized.

6.5.6 Discontinuous Transmission

Minimizing co-channel interference is a goal in any cellular system, since it allows better service for a given cell size, or the use of smaller cells, thus increasing the overall capacity of the system. Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time in normal conversation, by turning the transmitter off during silence periods. An added benefit of DTX is that power is conserved at the mobile unit.

The most important component of DTX is, of course, Voice Activity Detection. It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise. If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called clipping is heard at the receiving end. If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased. Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to the digital nature of GSM. To assure the receiver that the connection is not dead, *comfort noise* is created at the receiving end by trying to match the characteristics of the transmitting end's background noise.

6.5.7 Discontinuous Reception

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

6.5.8 Power Control

There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Stations operate at the lowest power level that will maintain an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dB from the peak power for the class down to a minimum of 13 dBm (20 milliwatts).

The mobile station measures the signal strength or signal quality (based on the Bit Error Ratio), and passes the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability. This arises from having mobiles in co-channel cells alternatingly increase their power in response to increased co-channel interference caused by the other mobile increasing its power. This in unlikely to occur in practice but it is (or was as of 1991) under study.

6.5.9 Interleaving

An interleaving rearranges a group of bits in a particular way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors. Being the errors less concentrated, it is then easier to correct them.

6.5.9.1 Interleaving for the GSM Control Channels

A burst in GSM transmits two blocks of 57 data bits each. Therefore the 456 bits corresponding to the output of the channel coder fit into four bursts (4*114 = 456). The 456 bits are divided into eight blocks of 57 bits. The first block of 57 bits contains the bit numbers (0, 8, 16, ...448), the second one the bit numbers (1, 9, 17, ...449), etc. The last block of 57 bits will then contain the bit numbers (7, 15, ...455). The first four blocks of 57 bits are placed in the even-numbered bits of four

bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the same four bursts. Therefore the interleaving depth of the GSM interleaving for control channels is four and a new data block starts every four bursts. The interleaver for control channels is called a block rectangular interleaver.

6.5.9.2 Interleaving for the GSM Speech Channels

The block of 456 bits, obtained after the channel coding, is then divided in eight blocks of 57 bits in the same way as it is explained in the previous paragraph. But these eight blocks of 57 bits are distributed differently. The first four blocks of 57 bits are placed in the even-numbered bits of four consecutive bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the next four bursts. The interleaving depth of the GSM interleaving for speech channels is then eight. A new data block also starts every four bursts. The interleaver for speech channels is called a block diagonal interleaver.

6.5.9.3 Interleaving for the GSM Data TCH Channels

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of 456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way :

- the first and the twenty-second bursts carry one block of 6 bits each
- the second and the twenty-first bursts carry one block of 12 bits each
- the third and the twentieth bursts carry one block of 18 bits each from
- the fourth to the nineteenth burst, a block of 24 bits is placed in each burst

A burst will then carry information from five or six consecutive data blocks. The data blocks are said to be interleaved diagonally. A new data block starts every four bursts.

6.5.10 Ciphering

Ciphering is used to protect signaling and user data. First of all, a ciphering key is computed using the algorithm A8 stored on the SIM card, the subscriber key and a random number delivered by the network (this random number is the same as the one used for the authentication procedure). Secondly, a 114 bit sequence is produced using the ciphering key, an algorithm called A5 and the burst numbers. This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst.

In order to decipher correctly, the receiver has to use the same algorithm A5 for the deciphering procedure.

6.5.11 Timing Advance

The timing of the bursts transmissions is very important. Mobiles are at different distances from the base stations. Their delay depends, consequently, on their distance. The aim of the timing advance is that the signals coming from the different mobile stations arrive to the base station at the right time. The base station measures the timing delay of the mobile stations. If the bursts corresponding to a mobile station arrive too late and overlap with other bursts, the base station tells, this mobile, to advance the transmission of its bursts.

6.6 Network Aspects

Ensuring the transmission of voice or data of a given quality over the radio link is only part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally, which requires that registration, authentication, call routing and location updating functions exist and are standardized in GSM networks. In addition, the fact that the geographical area covered by the network is divided into cells necessitates the implementation of a handover mechanism. These functions are performed by the Network Subsystem, mainly using the Mobile Application Part (MAP) built on top of the Signaling System No. 7 protocol.

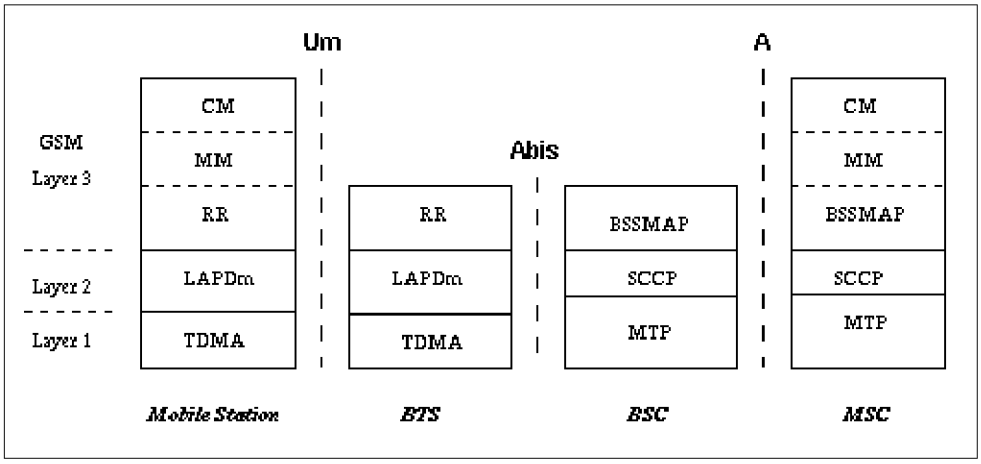

FIGURE 6.2 Signaling protocol structure in GSM [Scourias 1997]

The signaling protocol in GSM is structured into three general layers, depending on the interface, as shown in figure 6.2. Layer 1 is the physical layer, which uses the channel structures discussed above over the air interface. Layer 2 is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of Signaling System Number 7 is used. Layer 3 of the GSM signaling protocol is itself divided into 3 sublayers.

Radio Resources Management: Controls the setup, maintenance, and termination of radio and fixed channels, including handovers.

Mobility Management: Manages the location updating and registration procedures, as well as security and authentication.

Connection Management: Handles general call control, similar to CCITT Recommendation Q.931, and manages Supplementary Services and the Short Message Service.

Signalling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished through the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signalling System Number 7. The specification of the MAP is quite complex, and at over 500 pages, it is one of the longest documents in the GSM recommendations.

6.6.1 Radio Resources Management and Handover

The radio resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the mobile station, and the Base Station Subsystem, as well as the MSC. The RR layer is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels including the allocation of dedicated channels.

An RR-session is always initiated by a mobile station through the access procedure, either for an outgoing call, or in response to a paging message. The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the mobile, and the paging sub-channel structure, are handled in the RR layer. In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

In a cellular network, the radio and fixed links required are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. The execution and measurements required for handover form one of basic functions of the RR layer.

There are four different types of handover in the GSM system, which involve transferring a call between:

- Channels (time slots) in the same cell
- Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
- Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and
- Cells under the control of different MSCs.

The first two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signalling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. An important aspect of GSM

is that the original MSC, the *anchor MSC*, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of the new MSC, called the *relay MSC*.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

The algorithm for when a handover decision should be taken is not specified in the GSM recommendations. There are two basic algorithms used, both closely tied in with power control. This is because the BSC usually does not know whether the poor signal quality is due to multipath fading or to the mobile having moved to another cell. This is especially true in small urban cells.

The 'minimum acceptable performance' algorithm gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased. If further power increases do not improve the signal, then a handover is considered. This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.

The 'power budget' method uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level. It thus gives precedence to handover over power control. It avoids the 'smeared' cell boundary problem and reduces co-channel interference, but it is quite complicated.

6.6.2 Mobility Management

The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

6.6.2.1 Location Updating

A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell. One extreme would be to page every cell in the network for each call, which is obviously a waste of radio bandwidth. The other extreme would be for the mobile to notify the system, via location updating messages, of its current location at the individual cell level. This would require paging messages to be sent to exactly one cell, but would be very wasteful due to the large number of location updating messages. A compromise solution used in GSM is to group cells into *location areas*. Updating messages are required when moving between location areas, and mobile stations are paged in the cells of their current location area.

The location updating procedures, and subsequent call routing, use the MSC and two location registers: the Home Location Register (HLR) and the Visitor Location Register (VLR). When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location. In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number. The reason a routing number is not normally assigned, even though it would reduce signalling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls. If the subscriber is entitled to service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.

For reliability reasons, GSM also has a periodic location updating procedure. If an HLR or MSC/VLR fails, to have each mobile register simultaneously to bring the database up to date would cause overloading. Therefore, the database is updated as location updating events occur. The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signalling traffic and speed of recovery. If a mobile does not register after the updating time period, it is deregistered.

A procedure related to location updating is the IMSI attach and detach. A detach lets the network know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages. An attach is similar to a location update, and informs the system that the mobile is reachable again. The activation of IMSI attach/detach is up to the operator on an individual cell basis.

6.6.2.2 Authentication and Security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be, is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjunction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated.

The same initial random number and subscriber key are also used to compute the ciphering key using an algorithm called A8. This ciphering key, together with the TDMA frame number, use the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst (the two 57 bit blocks). Enciphering is an option for the fairly paranoid, since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.

Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber. As mentioned earlier, each GSM terminal is identified by a unique International Mobile Equipment Identity (IMEI) number. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

White-listed: The terminal is allowed to connect to the network.

Grey-listed: The terminal is under observation from the network for possible problems.

Black-listed: The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

6.6.3 Communication Management and Call Routing

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management. Each of these may be considered as a separate sublayer within the CM layer. Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code which identifies the subscriber's operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. It should be noted that the GMSC function is distinct from the MSC function, but is usually implemented in an MSC.

The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan. MSRNs are related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have the MSRN (see the location updating section). The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area (figure 6.3).

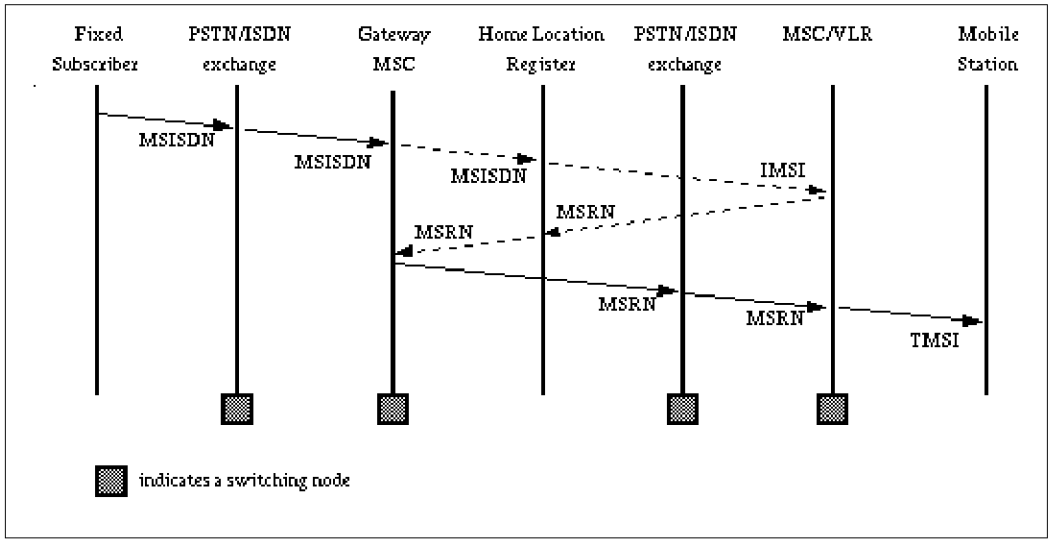

FIGURE 6.3 Call routing for a mobile terminating call [Scourias 1997]

6.7 Wireless Application Protocol (WAP) and Applications

The Wireless Application Protocol (WAP) is a global standard that bridges the gap between the mobile world and Internet Protocol-based resources such as the public Internet and private corporate intranets and extranets [2]. WAP is based on a layered architecture common in the communications world. Each layer can develop independently. As a result, it is possible to introduce new bearer services or to use new transport protocols without major changes in the other layers. The WAP specifications include a markup language and a set of protocols in application, session, transaction, security, and transport layers. In addition, WAP defines an environment that includes a micro-browser, scripting facilities, telephony integration, and Web-to-mobile-handset messaging. The browser offers not only access to

information, but also services such as banking applications, ticket booking, and synchronization of Web-based personal databases. WAP is enabled through gateway infrastructure software deployed in a mobile operator's network; the user interface is the familiar browser, albeit one tuned to the peculiarities of the mobile handset.

WAP is built on a basis of wireless mark-up languages (WML), which are built on a platform of eXtensible Mark-up Language (XML) and operate on top of user Datagram Protocol (UDP) and Internet Protocol (IP). Many of the protocols are based on Internet standards such as hypertext transfer protocol (HTTP) but have been adapted for the low-bandwidth, high-latency, and low-connection reliability of wireless systems.

WAP exists to bring Internet resources to the wireless world where terminals are designed to be lightweight, battery powered, and small-sized. Internet standards such as HyperText Transfer Protocol (HTTP), HyperText Markup Language (HTML), Transport Layer Security (TLS), and Transfer Control Protocol (TCP) are inefficient over mobile networks because they require large amounts of mainly text-based data to be sent. Furthermore, most HTML content cannot be displayed very well on the small screens typical of mobile phones, pagers, and wireless personal digital assistants. WAP uses binary transmission for greater data compression and is adaptable for longer latencies and lower bandwidth. WAP sessions can cope with intermittent coverage and can operate over a wide variety of wireless transports. In fact, the lightweight WAP protocol stack is designed to minimize the required bandwidth and maximize the number of wireless network types that can deliver WAP content.

The protocol architecture is similar to that of the Web, such as the use of Wireless Markup Language (WML, a cousin of HTML) optimized for mobile devices [39].

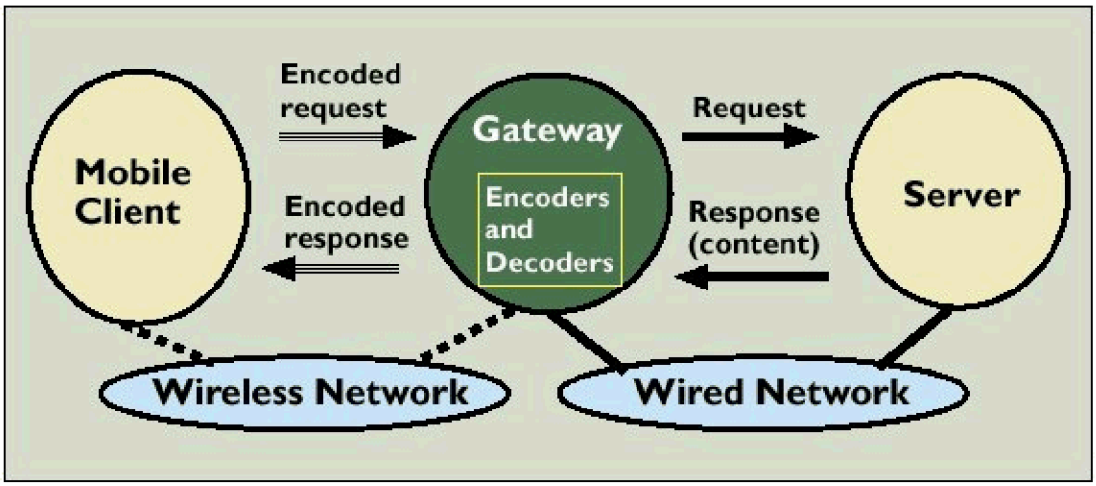

FIGURE 6.4 WAP basic architecture [Varshney 2000]

The architecture of WAP is shown in figure 6.4, where a gateway acts as a proxy server to a mobile client and translates requests from WAP protocol stacks to protocol stacks employed by the information server on the other side. Encoders translate the content coming from the server into compact formats to reduce the size of data over the wireless network. This infrastructure ensures mobile users can access a wide variety of contents and applications and also allows application developers to build content services and applications that can run on a large base of mobile terminals. To support this configuration, the WAP forum defines several layers of protocols as presented in Table 6.1.

TABLE 6.1 WAP layers, protocols, and functions.[Varshney 2000]

WAP Layer	Protocol	Functions
Application Layer	Wireless Application Environment (WAE)	Provides micro browser environment and wireless markup language (WML) and script
Session Layer	Wireless Session Protocol (WSP)	HTTP functions and semantics Facility for reliable and unreliable data push Protocol feature negotiation
Transaction Layer	Wireless Transaction Protocol (WTP)	Provides several types of transaction services Uses delayed ACKs and concatenated PDUs
Security Layer	Wireless Transport Layer Security (WTLS)	Provides authentication and privacy
Transport Layer	Wireless Datagram Protocol (WDP)	Provides a common interface to upper layer protocols by adapting to specific features of the underlying technologies
Wireless Layer	Wireless and Mobile Networks	Provides a specific way to transmit information over a wireless link

WAP is being used to develop enhanced forms of existing applications and new versions of today's applications [4].

Existing mobile data software and hardware supplies are adding WAP support to their offering, either by developing their own WAP interface or more usually partnering with one of the WAP Gateway suppliers profiled above. WAP is also given a significant impetus for new players to add mobile as a new distribution channel for their existing products and services- for example, CNN and Nokia teamed up to offer CNN Mobile, and Reuters and Ericsson teamed up to provide Reuters Wireless Services.

The Wireless Application Protocol will allow customers to easily reply to incoming information on the phone by allowing new menus to access mobile services. This is part of the business case for network operators- by making the value-added services more easily to reply to and request (using menus instead of keywords, for example), WAP can help generate additional traffic on the network and therefore revenue.

Previously, application developers wrote proprietary software applications and had to port that application to different network types and bearers within the same platform.

By separating the bearer from the application, WAP facilitates easy migration of applications between networks and bearers. As such, WAP is similar to Java in that it simplifies application development. This reduces the cost of wireless application development and therefore encourages entry to the mobile industry by software developers.

Corporate applications that are being enhanced and enabled with a WAP interface include:

- Job Dispatch
- Remote Point Of Sale
- Customer Service
- Remote Monitoring Such As Meter Reading
- Vehicle Positioning
- Corporate Email
- Remote LAN Access
- File Transfer

- Web Browsing
- Document Sharing/ Collaborative Working
- Audio
- Still Images
- Moving Images
- Home Automation

Consumer Applications that are being enhanced and enabled with a WAP interface include:

- Simple Person to Person Messaging
- Voice and Fax Mail Notifications
- Unified Messaging
- Internet Email
- Prepayment
- Ringtones
- Mobile Commerce
- Affinity Programs
- Mobile Banking
- Chat
- Information Services

6.8 General Packet Radio Services (GPRS)

General Packet Radio Services (GPRS) is a packet overlay for existing Global System for Mobile Communications (GSM) networks [2]. GPRS will enable the deployment of mobile data applications anticipated to be superior to today's voice-driven GSM applications.

Without GPRS, data moves over a GSM network by way of a 9.6 kilobits per second (Kbits/s) modem using a single timeslot in the GSM allocation. GSM includes provisions for extending this performance to 14.4 Kbits/s. The connections are slow, far below what Internet users demand, and the cost of the call is significant. With GPRS, packet technology is used instead, and different classes of GPRS service can use varying transmit and receive time slots. The system requires a packet handling overlay network and a base station update, normally via a software

download, making GPRS relatively expensive to install but still likely to be much less costly than building a dedicated data network. However, the data rate is much higher than 9.6 Kbits/s, and the incremental service costs are very low.

Packet switching is spectrum-efficient because GPRS radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time (as is the case with voice), the available radio resource can be concurrently shared between several users. This means large numbers of GPRS users can share the same bandwidth and be served from a single cell. GPRS therefore lets network operators maximize the use of their network resources in a dynamic and flexible way.

To use GPRS, a user will need:

- a mobile phone or terminal that supports GPRS
- a valid subscription to a mobile telephone network that supports GPRS
- applications that use the data connection, for example WAP, email, or a PC connected to a telephone
- a destination to send or receive information through GPRS. Whereas with a messaging service, the destination was often another mobile handset, with GPRS the destination is likely to be an Internet site.

From the service provider's point of view, GPRS can improve the peak time capacity of a GSM network because it allocates scarce radio resources more efficiently by supporting virtual connectivity and also migrates traffic that was previously sent using circuit-switched-data to GPRS.

6.8.1 Network Features of GPRS

6.8.1.1 Packet Switching

GPRS involves overlaying a packet based air interface on the existing circuit switched GSM network [5]. This gives the user an option to use a packet-based data service. To supplement a circuit switched network architecture with packet switching is quite a major upgrade. However, as we shall see later, the GPRS standard is delivered in a very elegant manner- with network operators needing only to add a

couple of new infrastructure nodes and making a software upgrade to some existing network elements.

With GPRS, the information is split into separate but related "packets" before being transmitted and reassembled at the receiving end. Packet switching is similar to a jigsaw puzzle- the image that the puzzle represents is divided into pieces at the manufacturing factory and put into a plastic bag. During transportation of the now boxed jigsaw from the factory to the end user, the pieces get jumbled up. When the recipient empties the bag with all the pieces, they are reassembled to form the original image. All the pieces are all related and fit together, but the way they are transported and assembled varies. The Internet itself is another example of a packet data network, the most famous of many such network types.

6.8.1.2 Spectrum Efficiency

Packet switching means that GPRS radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time, the available radio resource can be concurrently shared between several users. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell. The actual number of users supported depends on the application being used and how much data is being transferred. Because of the spectrum efficiency of GPRS, there is less need to build in idle capacity that is only used in peak hours. GPRS therefore lets network operators maximize the use of their network resources in a dynamic and flexible way, along with user access to resources and revenues.

6.8.1.3 Internet Aware

For the first time, GPRS fully enables Mobile Internet functionality by allowing interworking between the existing Internet and the new GPRS network. Any service that is used over the fixed Internet today- File Transfer Protocol (FTP), web browsing, chat, email, telnet- will be as available over the mobile network because of

GPRS. In fact, many network operators are considering the opportunity to use GPRS to help become wireless Internet Service Providers in their own right.

The World Wide Web is becoming the primary communications interface- people access the Internet for entertainment and information collection, the intranet for accessing company information and connecting with colleagues and the extranet for accessing customers and suppliers. These are all derivatives of the World Wide Web aimed at connecting different communities of interest. There is a trend away from storing information locally in specific software packages on PCs to remotely on the Internet. When it is desired to check the schedule or contacts, user may go onto the Internet site such as a portal. Hence, web browsing is a very important application for GPRS.

Because it uses the same protocols, the GPRS network can be viewed as a sub-network of the Internet with GPRS capable mobile phones being viewed as mobile hosts. This means that each GPRS terminal can potentially have its own IP address and will be addressable as such.

6.8.1.4 Supports TDMA and GSM

It should be noted right that the General Packet Radio Service is not only a service designed to be deployed on mobile networks that are based on the GSM digital mobile phone standard. The IS-136 Time Division Multiple Access (TDMA) standard, popular in North and South America, will also support GPRS. This follows an agreement to follow the same evolution path towards third generation mobile phone networks concluded in early 1999 by the industry associations that support these two network types.

6.8.2 Limitations of GPRS

It should already be clear that GPRS is an important new enabling mobile data service which offers a major improvement in spectrum efficiency, capability and functionality compared with today's nonvoice mobile services. However, it is important to note that there are some limitations with GPRS, which can be summarized as:

6.8.2.1 Limited Cell Capacity for All Users

GPRS does impact a network's existing cell capacity. There are only limited radio resources that can be deployed for different uses- use for one purpose precludes simultaneous use for another. For example, voice and GPRS calls both use the same network resources. The extent of the impact depends upon the number of timeslots, if any, that are reserved for exclusive use of GPRS. However, GPRS does dynamically manage channel allocation and allow a reduction in peak time signalling channel loading by sending short messages over GPRS channels instead.

6.8.2.2 Speeds Much Lower in Reality

Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight timeslots without any error protection. Clearly, it is unlikely that a network operator will allow all timeslots to be used by a single GPRS user. Additionally, the initial GPRS terminals are expected be severely limited- supporting only one, two or three timeslots. The bandwidth available to a GPRS user will therefore be severely limited. As such, the theoretical maximum GPRS speeds should be checked against the reality of constraints in the networks and terminals. The reality is that mobile networks are always likely to have lower data transmission speeds than fixed networks.

6.8.2.3 Support of GPRS Mobile Terminate (MT) by Terminals

Availability or not of GPRS MT is a central question with critical impact on the GPRS business case such as application migration from other nonvoice bearers.

By originating the GPRS session, users confirm their agreement to pay for the delivery of content from that service. This origination may well be performed using a Wireless Application Protocol (WAP) session using the WAP microbrowser that will be built into GPRS terminals. However, mobile terminated IP traffic might allow unsolicited information to reach the terminal. Internet sources originating such unsolicited content may not be chargeable. A possible worse case scenario would be that mobile users would have to pay for receiving unsolicited junk content. This is a

potential reason for a mobile vendor NOT to support GPRS Mobile Terminate in their GPRS terminals.

However, there is always the possibility of unsolicited or unwanted information being communicated through any media, but that does not mean that we would wish to preclude the possibility of any kind of communication through that means altogether. A network side solution such as GGSN or charging platform policing would be preferable rather than a non-flexible limitation built into all the GPRS handsets.

6.8.2.4 Suboptimal Modulation

GPRS is based on a modulation technique known as Gaussian minimum-shift keying (GMSK). EDGE is based on a new modulation scheme that allows a much higher bit rate across the air interface- this is called eight-phase-shift keying (8 PSK) modulation. Since 8 PSK will also be used for UMTS, network operators will need to incorporate it at some stage to make the transition to third generation mobile phone systems.

6.8.2.5 Transit Delays

GPRS packets are sent in all different directions to reach the same destination. This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link. The GPRS standards recognize this inherent feature of wireless packet technologies and incorporate data integrity and retransmission strategies. However, the result is that potential transit delays can occur.

Because of this, applications requiring broadcast quality video may well be implemented using High Speed Circuit Switched Data (HSCSD). HSCSD is simply a Circuit Switched Data call in which a single user can take over up to four separate channels at the same time. Because of its characteristic of end to end connection between sender and recipient, transmission delays are less likely.

6.8.2.6 No Store and Forward

Whereas the Store and Forward Engine in the Short Message Service is the heart of the SMS Center and key feature of the SMS service, there is no storage mechanism incorporated into the GPRS standard, apart from the incorporation of interconnection links between SMS and GPRS.

Chapter 7

MOBILITY SUPPORT OF IPv6

IP version 6 (IPv6) is being designed within the Internet Engineering Task Force (IETF) as a replacement for the current version of the IP protocol used in the Internet (IPv4) [29].

Without specific support for mobility in IPv6, packets routed to a mobile node would not be able to reach it while the mobile node is away from its home IP subnet, since as in IPv4, routing is based on the network prefix in a packet's destination IP address. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new IP subnet, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is really important, because mobile computers are likely to be the most populated part of the Internet during the lifetime of IPv6.

IPv6 is derived from IPv4 and is in many ways similar to it. As such, the IETF Mobile IP Working Group's current protocol design [30] for mobility of IPv4 nodes could be adapted for use in IPv6, with only the straightforward changes needed to accommodate differences between IPv4 and IPv6 such as the size of addresses.

Each mobile node has a permanent IP address like all other nodes, and this IP address is known as the mobile node's *home address.* A mobile node's home address remains same wherever it is attached to the Internet. Therefore the IP subnet of that home address is the mobile node's *home subnet,* and standard IP routing mechanisms will deliver packets sent to a mobile node's home address only to the mobile node's home subnet. A mobile node is simply any node that may change its connection point from one IP subnet to another and it is still be addressed by its home address. Any node that a mobile node is communicating is referred as a *correspondent nod.* This node may be either stationary or mobile.

A mobile node's current location while away from home is known as its *care-of address*. This is a globally-routable address handled by the mobile node by using the

IPv6 address autoconfiguration function in *the foreign subnet.* The association of a mobile node's home address with a care-of address, along with the remaining lifetime of that association, is known as a *binding.*

The router on the mobile node's home subnet known as mobile node's *home agent.* While away from home subnet, home agent keeps a record of the current binding of the mobile node. The home agent then intercepts any packets of mobile node that addressed to home address of mobile node and *tunnels* them to the mobile node at its current care-of address. This tunneling uses IPv6 encapsulation, and the path followed by a packet while it is encapsulated is known as a *tunnel.* Once a correspondent node has learned the mobile node's care-of address, it may cache it and route its own packets for the mobile node directly there using an IPv6 Routing header, bypassing the home agent completely.

The most important function needed to support mobility is the reliable and timely notification of a mobile node's current care-of address to those other nodes that need it. This provides for avoiding the routing anomaly known as *triangle routing,* as illustrated in figure 7.1. In triangle routing, all packets sent *to* a mobile node must be routed first to the mobile node's home subnet and then forwarded to the mobile node at its current location by its home agent. However, packets sent from a mobile node are not forwarded in this way, leading to this "triangular" combination of the two routes used for all communication between these two nodes.

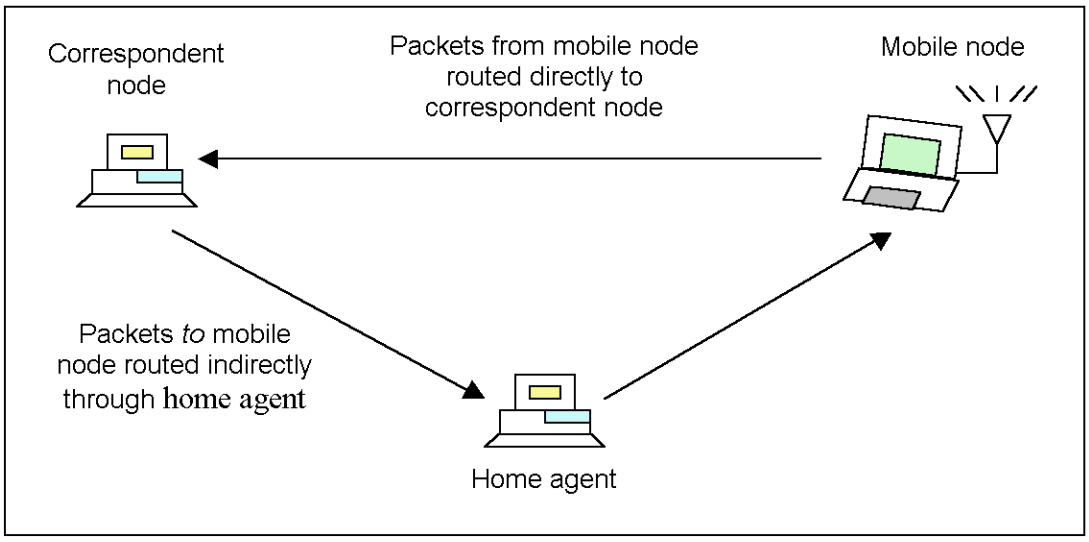

FIGURE 7.1 Triangle routing [Perkins 1996]

Triangle routing, because of its poor route selection, has some problems, such as:

- Increased impact of possible network partitions,
- Increased load on the network, and
- Increased delay in delivering packets.

7.1 Overview of IPv6

The most visible difference between IPv6 and IPv4 is that IPv6 addresses are all 128 bits long, whereas IPv4's are 32 bits long. Within this huge IPv6 address space, a tiny part is reserved for all current IPv4 addresses, and another tiny part is reserved for the *Link-Local* addresses, which are not routable but are guaranteed to be unique on a link (i.e., on a local network). Nodes on the same local network can communicate with each other by just using their Link-Local addresses without help of a router.

Nodes discover each other's presence, as well as each other's link-layer (i.e., MAC) addresses, by means of Neighbor Discovery protocol. IPv6 nodes also discover local routers and network prefixes again by using Neighbor Discovery. The IPv6 Neighbor Discovery protocol can be stated as a much improved version of two IPv4 protocols, the Address Resolution Protocol (ARP) and the ICMP Router Discovery Protocol.

IPv6 defines several kinds of *extension headers,* which may be used to include additional information in the headers of an IPv6 packet. The defined IPv6 extension headers include:

- Destination Options header,
- Hop-by-Hop Options header,
- Routing header,
- Authentication header.

The Destination Options header may be included in a packet to carry a sequence of one or more options and these options are processed only when the packet reaches to the final destination node. Similarly, the Hop-by-Hop Options header may be included to carry a sequence of one or more options, but these options are processed by every intermediate router that receives and forwards the packet as

well as by the final destination node. In IPv4, every IP option is treated essentially as a Hop-by-Hop option and thus causes performance degradation because of processing needed at every intermediate router, whether it belongs to that router or only to the final destination node.

The Routing header is particularly useful for the mobility protocol, and is similar to the Source Route options defined for IPv4. The IPv6 Routing header can serve both as a strict source route and a loose source route. Mobile IPv6 uses it only as a loose source route. However, unlike the IPv4 Source Route options in IPv6, the Routing header is not examined or processed until it reaches the next node identified in the route. In addition, the destination node receiving a packet with a Routing header is under no obligation for routing packets back to the sender.

The Authentication header provides a means by which a packet can include optional authentication data, for example based on a one-way cryptographic hash of the packet's contents. The inclusion of this authentication data allows the receiver to verify the authenticity of the packet sender, and also protects against modification of the packet while in transit, since a modified packet will be viewed by the receiver the same as a attacked packet. The Authentication header is also useful by providing a replay protection of packets, such that saved copies of an authenticated packet cannot be resent by an attacker later. The computation of the authentication data and use of replay protection are controlled by a "security association" that the sender of the packet must have established with the receiver. Security associations may be manually configured or automatically established.

7.2 Overview of Mobile IPv6

7.2.1 Requirements, Goals, and Applicability

Mobile IPv6 has a main job of enabling IPv6 nodes to move from one IP subnet to another. Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it accommodates node movement from an Ethernet segment to a wireless LAN cell.

The protocol supplies a mobile node to communicate with other nodes (stationary or mobile) after changing its link-layer point of attachment from one IP

subnet to another without changing the mobile node's IPv6 address yet. A mobile node is always addressable by its home address, and packets may be routed to it using this address regardless of the mobile node's current point of attachment to the Internet. The movement of a mobile node away from its home subnet is therefore transparent to transport and higher-layer protocols and applications.

All packets used to inform another node about the location of a mobile node must be authenticated. Otherwise, a malicious host would be able to hijack traffic intended for a mobile node by the simple matter of causing the mobile node to seem to be elsewhere than its true location. Such hijacking attacks are called "remote redirection" attacks.

The link by which a mobile node is directly attached to the Internet may often be a wireless link. This link may thus have a substantially lower bandwidth and higher error rate than traditional wired networks. Moreover, mobile nodes are likely to be battery powered, and minimizing power consumption is important. Therefore, the number of administrative packets sent over the link, where a mobile node is directly attached to the Internet, should be minimized. Additionally the size of these packets should be kept as small as reasonably possible.

It is assumed that mobile nodes will generally not change their point of attachment to the Internet more frequently than once per second, although the protocol is likely to work even when the point of attachment changes more frequently. In addition, as is usual in the Internet today, it is assumed that IPv6 unicast packets are routed based on the destination address in the packet's IP header so that routing mechanism is not influenced by the packet's IP source address.

7.2.2 Basic Operations of the Protocol

Mobile nodes will have assigned to their network interface(s) at least three IPv6 addresses whenever they are going away from their home subnet. One is its *home address,* which is permanently assigned. The second address is the mobile node's current *Link-Local address.* Mobile IPv6 adds a third address, known as the mobile node's *care-of address,* which is associated with the mobile node only while visiting a particular foreign subnet. The network prefix of a mobile node's care-of address is equal to the network prefix of the foreign subnet being visited by the mobile node.

Therefore packets addressed to this care-of address will be routed by normal Internet routing mechanisms.

Each time the mobile node moves its point of attachment from one IP subnet to another, the mobile node will configure its care-of address by stateless address autoconfiguration, or alternatively by some means of stateful address autoconfiguration such as DHCPv6 or PPPv6. The decision about using which manner of automatic address configuration is made according to the methods of IPv6 Neighbor Discovery. A mobile node may have more than one care-of address at a time. For example, if it is link-level attached to more than one (wireless) network at a time or if more than one IP network prefix is present on a network to which it is attached. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a *binding*. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a *Binding Cache*.

While away from home, a mobile node registers one of its bindings with a router in its home subnet, requesting this router to function as the *home agent* for the mobile node. The care-of address in this binding registered with its home agent is known as the mobile node's *primary care-of address,* and the mobile node's home agent retains this entry in its Binding Cache, marked as a "home registration," until its lifetime expires. While it has a home registration entry in its Binding Cache, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet. Then home agent tunnels each intercepted packet to the mobile node's primary care-of address indicated in this Binding Cache entry. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation.

In addition, Mobile IPv6 provides a mechanism for IPv6 correspondent nodes communicating with a mobile node, to dynamically learn the mobile node's binding. The correspondent node adds this binding to its Binding Cache, although when space must be reclaimed in the Binding Cache. Such a cache entry may be replaced at any time by any reasonable local cache replacement policy such as LRU. When sending a packet to any IPv6 destination, a node checks its Binding Cache for an entry for the packet's destination address, and if a cached binding for this address is found, the node routes the packet directly to the mobile node at the care-of address indicated in

this binding. This routing mechanism uses an IPv6 Routing header instead of IPv6 encapsulation, because this adds fewer overheads to the size of the packet. The home agent cannot use a Routing header, since adding one to the packet at the home agent would invalidate the authentication in any IPv6 Authentication header included in the packet by the correspondent node. If no Binding Cache entry is found, the node instead sends the packet normally (with no routing header), and the packet is then intercepted and tunneled by the mobile node's home agent as described before. This use of cached bindings for routing packets directly to a mobile node at its current care-of address is similar to the existing work on "route optimization" for IPv4 mobility.

Mobile IPv6 introduces two new IPv6 Destination options to allow a mobile node's home agent and correspondent nodes learn and cache the mobile node's binding. After configuring a new care-of address, a mobile node must send a *Binding Update* option containing that care-of address to its home agent It must also informs any correspondent nodes that may have an out-of-date care-of address for the mobile node in their Binding Cache. Receipt of a Binding Update must be acknowledged using a *Binding Acknowledgement* option, if an acknowledgement was requested in the Binding Update.

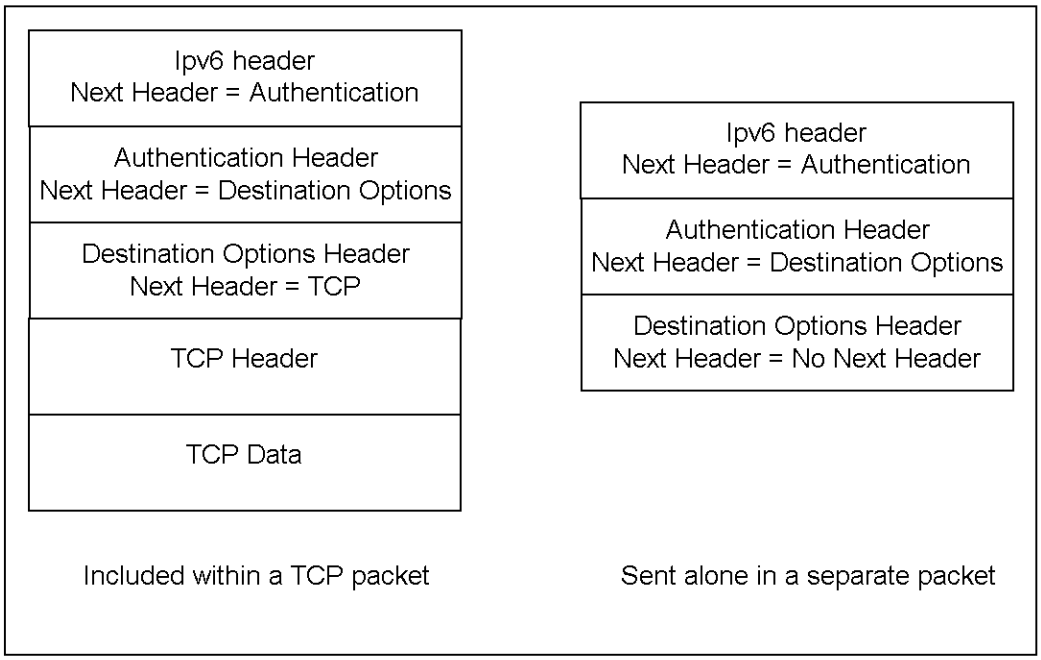

FIGURE 7.2 Sending Binding Updates and Acknowledgements as IPv6 Destination options [Perkins 1996]

Since an IPv6 Destination Options header containing one or more Destination options can appear in any IPv6 packet, any Mobile IPv6 option can be sent in either of two ways, as illustrated in figure 7.2:

• A Binding Update or Binding Acknowledgement can be included within any IPv6 packet carrying any payload such as TCP or UDP.

• A Binding Update or Binding Acknowledgement can be sent as a separate IPv6 packet containing no transport-level payload. In this case, the Next Header field in the Destination Options header is set to indicate "No Next Header".

The capability of correspondent nodes learning the care-of address of a mobile node and caching this information for use in sending future packets to the mobile node's care-of address are very essential for scalability and minimizing network load. By caching the care-of address of a mobile node, optimal routing of packets can be achieved between the correspondent node and the mobile node. Routing packets directly to the mobile node's care-of address also eliminates congestion at the home agent and thus contributes significantly to the overall health of the Internet.

Moreover, most packets sent by a correspondent node to a mobile node can be delivered with no assistance from the home agent. Thus, the impact of failure at the home agent can be significantly reduced. This situation is important because many administrative domains will have a single home agent to serve a particular home subnet, and so as a single point of failure for communications to nodes using that home agent. Furthermore, communications between the home agent and a mobile node may depend on a number of intervening networks. Therefore there are many more ways that packets can fail to reach a mobile node when the home agent is required as an intermediate node. This would be particularly relevant on links between home agent and mobile node. Caching the binding of a mobile node at the correspondent node enables communication with the mobile nodes even if the home agent fails or is difficult to reach over the Internet.

7.2.3 The Binding Update Option

A mobile node sends a Binding Update to another node to inform it of its current binding. Since the Binding Update is sent as an IPv6 Destination option, the mobile node may include it in any existing packet (such as a TCP packet). The

Binding Update is used by a mobile node to register its primary care-of address with its home agent, and to notify correspondent nodes of its binding so that they may create or update entries in their Binding Cache for use in future communication with the mobile node.

A Binding Update should be considered a form of routing update. If it is handled incorrectly, a Binding Update could be a source of security problems due to the possibility of remote redirection attacks. Therefore, packets, which carry a Binding Update, must also include an IPv6 Authentication header, which provides authentication and replay protection for the Binding Update.

7.2.4 The Binding Acknowledgement Option

The *Binding Acknowledgement* option is sent by a node to acknowledge receipt of a Binding Update. When a node receives a Binding Update addressed to itself it must return a Binding Acknowledgement. Other Binding Updates may also be acknowledged but need not be. The destination address in the IPv6 header of the packet carrying the Binding Acknowledgement must be the care-of address from the Binding Update. This causes the Binding Acknowledgement to be returned directly to the mobile node sending the Binding Update.

7.2.5 Mobile Node Operation

Every IPv6 mobile node must be able to perform IPv6 decapsulation. Every mobile node must be able to send Binding Updates and to receive Binding Acknowledgements. Based on the Lifetime field in Binding Updates that it sends, every IPv6 mobile node must keep track of which other IPv6 nodes may need to receive a new Binding Update as a result of recent movement by the mobile node. Every IPv6 mobile node must also be able to send Binding Updates when it receives a packet from a correspondent node encapsulated to it by its home agent, rather than sent directly to it by the correspondent node using a Routing header.

7.2.6 Correspondent Node Operation

Every IPv6 node may be a correspondent node communicating with one or more mobile nodes. Thus, every IPv6 node must be able to process received Binding Updates, to send Binding Acknowledgements, and to maintain a Binding Cache.

An existing requirement in IPv6 is that every IPv6 node must be able to maintain security associations for use in IPv6 Authentication headers. Nodes receiving a Binding Update or Binding Acknowledgement must verify the authentication data contained in the Authentication header in the packet carrying the Update or Acknowledgement.

7.2.7 Home Agent Operation

Every IPv6 router must perform the mobility-related functions for correspondent nodes, but not necessarily the additional functions for mobile nodes.

In addition, every IPv6 router must be able to send Binding Acknowledgements in response to Binding Updates received from a mobile node. Every IPv6 router must also be able to encapsulate packets in order to tunnel them to a care-of address known for a mobile node for which it is serving as a home agent.

7.2.8 Security Issues

The IPv6 and IP Security specifications require authentication to be implemented by all IPv6 nodes. Thus, whenever a mobile node is able to establish a security association with a correspondent node, the mobile node will be able to send authenticated Binding Updates to that correspondent node.

7.2.8.1 Session Keys with Local Routers

In the IPv4 "route optimization" proposal, a mechanism is outlined whereby a session key can be established between a mobile node and its foreign agent, without requiring any pre-established security relationship between them. A similar mechanism will work in IPv6, to avoid the need for a possibly time-consuming

negotiation between routers and mobile nodes for the purpose of obtaining the session key, which under many circumstances would only be used once. This mechanism, if needed, can be specified completely outside the Mobile IPv6 protocol and would amount to a way of creating a dynamic security association between two nodes which do not share a trust relationship, but which need to agree on a key for some limited purpose. Methods for key distribution for use by Internet hosts, being standardized now, should allow this function to be performed appropriately for mobile nodes.

7.2.8.2 Source Address Filtering by Firewalls

The current design of Mobile IPv6 does nothing to permit mobile nodes to send their packets through firewalls that filter out packets with the "wrong" source address in their IPv6 header. The mobile node's home address may be unlikely to fall within the ranges required to satisfy the firewall's criteria for allowing the packet through the firewall.

Firewalls are unlikely to disappear. However, any solution to the firewall problem based on hiding the non-local source address outside the source address field of the IPv6 header is likely to fail. Any vendor or facilities administrator wanting to filter based on the address in the IPv6 source address field would also quickly begin also filtering on such hidden source addresses.

Chapter 8

ORGANIZATIONS AND INDUSTRY GROUPS

American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a privately funded federation of leaders representing both the private and public sectors. Its main job is coordinating the U.S. voluntary consensus standards system. ANSI was organized in 1918 and is made up of manufacturing and service businesses, professional societies and trade associations, standards developers, academic institutions, government agencies, and consumer and labor interests, all working together to develop voluntary national consensus standards.

ANSI provides U.S. participation in the international standards community as the sole U.S. representative to the two major nontreaty international standards organizations: The International Organization for Standardization (ISO) and, through the U.S. National Committee, the International Electrotechnical Commission (IEC).

http://www.ansi.org

Automatic Identification Manufacturers (AIM)

AIM is an industry association representing interests that drive the automatic identification and data capture (AIDC) industry. The primary mission of AIM is to educate end users on integrated technology solutions using bar codes, radio frequency identification (RFID), radio frequency data communications (RFDC), and so on. AIM is recognized as the industry catalyst for market growth and the center for standards development.

http://www.aimglobal.org/europe/

European Telecommunications Standards Institute (ETSI)

ETSI is a non-profit organization whose mission is to produce the telecommunications standards that are used throughout Europe. Based in Sophia Antipolis, a high-tech research park in southern France, ETSI unites 789 members from 52 countries inside and outside Europe, and represents administrations, network operators, manufacturers, service providers, research bodies and users.

http://www.etsi.org/

Federal Communications Commission (FCC)

The FCC was established by the Communications Act of 1934 as an independent United States government agency directly responsible to Congress. The Act, which has been amended over the years, charges the Commission with establishing policies to govern interstate and international communications by television, radio, wire, satellite and cable. In other words, the FCC regulates all forms of electronic communications both within and going out of the United States. The FCC works with the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI) and other organizations to establish international regulation.

http://www.fcc.gov/

Infrared Data Association (IrDA)

The Infrared Data Association (IrDA) was established in 1993 to set and support hardware and software standards for creating infrared communications links. The association's charter is to create an interoperable, low-cost, low-power, half-duplex, serial data interconnection standard that supports a walk-up, point-to-point user model that is adaptable to a wide range of applications and devices. IrDA standards support a broad range of computing, communications, and consumer devices.

http://www.irda.org

Institute for Electrical and Electronic Engineers (IEEE)

The IEEE is a non-profit professional organization founded by a handful of engineers in 1884 for the purpose of consolidating ideas dealing with electro-technology. In the past 100 plus years, IEEE has maintained a steady growth. Today, the IEEE, which is based in the United States, has more than 320,000 members located in 150 countries. The IEEE consists of 35 individual societies, including the Communications Society, Computer Society, and Antennas and Propagation Society, to name just a few. The Computer Society is the official sponsor of the IEEE 802.11 Working Group.

The IEEE plays a significant role in publishing technical works, sponsoring conferences and seminars, accreditation, and standards development. IEEE has published nearly 700 active standards publications, half of which relate to power engineering; most others deal with computers. The IEEE standards development process consists of 30,000 volunteers (who are mostly IEEE members) and a Standards Board of 32 people.

Regarding LANs, IEEE has produced some popular and widely used standards. The majority of LANs in the world utilize network interface cards based on the IEEE 802.3 (ethernet), IEEE 802.5 (token ring), and the IEEE 802.11 (wireless LAN) standards, for example.

http://www.ieee.org/index.html

International Organization for Standardization

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies. ISO is a nongovernmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements, which are published as international standards.

http://www.iso.ch

International Telecommunication Union (ITU)

The International Telecommunications Union (ITU) is an intergovernmental organization founded in Paris in 1865 as the International Telegraph Union. The International Telecommunication Union took its present name in 1934 and became a specialized agency of the United Nations in 1947.

The ITU adopts international regulations and treaties governing all terrestrial and space uses of the frequency spectrum. It also develops standards to facilitate the interconnection of telecommunication systems on a worldwide scale regardless of the type of technology used.

http://www.itu.int/home/index.html

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) provides a forum for working groups to coordinate technical developments of new protocols. Its most important function is the development and selection of standards within the Internet protocol suite. The IETF began in January 1986 as a forum for technical coordination by contractors for the then U.S. Defense Advanced Projects Agency (DARPA), working on the ARPAnet, U.S. Defense Data Network (DDN), and the Internet core gateway system. Since that time, the IETF has grown into a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.).

http://www.ietf.cnri.reston.va.us/home.html

Multimedia Mobile Access Communications Systems Promotion Council

The Multimedia Mobile Access Communication Systems Promotion Council (MMAC-PC) was formed in Japan in 1996 in cooperation with users, carriers, manufacturers as well as academia. The objective of the Council is to propose a high

performance wireless system to allow any person to communicate "at anytime and any place". The Promotion Council's goal is to realize MMAC as soon as possible through investigations of system specifications, demonstrative experiments, information exchanges and popularization activities which contribute to the efficient use of the radio frequency spectrum. MMAC involves indoor and outdoor broadband high data rate communications tied together via both wireless and fiber optic systems.

http://www.arib.or.jp/mmac/e/index.htm

Mobile and Portable Radio Research Group

The mission of the Mobile and Portable Radio Research Group (MPRG) is to establish a national resource for research and education in the field of wireless communications. MPRG's mission is to provide design and analysis tools and techniques for U.S. manufacturers, government and consumer service providers, and regulatory agencies, while at the same time providing a high-caliber educational experience for graduate and undergraduate engineering.

http://www.mprg.org

Mobile Management Task Force (MMTF)

The Mobile Management Task Force (MMTF) is an industry group that promotes new management standards that specifically address the concerns of network administrators who must manage mobile computer users. The MMTF was first formed and spearheaded by Epilogue Technology Corporation and Xircom, Inc. Current MMTF member companies include IBM Networking Division, Lannair, Motorola, National Semiconductor Corp., and Zenith Data Systems.

The joint aim of the group is to define and address the needs of mobile computer users, which are inherently different from those of desktop computer users. The group's aim is to identify the administrative needs of laptop workstation users, mobile computer users, palmtop users, and others who need reliable access to computer networks on a sporadic basis. The concerns of the MMTF also include managing on-demand access to local area networks, dial-up network access, wireless

LAN communications, and related administration issues unique to the needs of mobile computer users.

http://www.epilogue.com/mmtf/mmtf.html

Portable Computer and Communications Association (PCCA)

The Portable Computer and Communications Association (PCCA) was established in 1992 to advance the portable computing industry.

http://www.pcca.org/

Wireless Ethernet Compatibility Alliance (WECA)

The Wireless Ethernet Compatibility Alliance (WECA) is a nonprofit organization formed in 1999 to certify interoperability of Wi-Fi (IEEE 802.11b) products and to promote Wi-Fi as the global, wireless LAN standard across all market segments. WECA has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi-certified products. When a product successfully passes the test, the company is granted the Wi-Fi seal of interoperability and may display the Wi-Fi logo on that product and its corresponding collateral material. This testing assures that products bearing the Wi-Fi logo will work with each other. Membership in WECA is open to all companies who support the Wi-Fi standard, including any member manufacturer that would like to submit its Wi-Fi-based product for interoperability testing. WECA now comprises 82 members.

http://www.weca.net/

Wireless LAN Group

At the University of Massachusetts, Amherst, the Wireless LAN Group researches, develops, and introduces efficient wireless LAN architectures that can support the Quality of Service requirements of multimedia applications. Such architectures include point-to-point, single-cell, multiple-cell, and combinations with

various wired backbones and connections to other different wireless communication networks.

http://dvd1.ecs.umass.edu/wireless/

Wireless LAN Interoperability Forum (WLIF)

The Wireless LAN Interoperability Forum was formed to promote the use of wireless LANs through the delivery of interoperable products and services at all levels of the value chain. Members of the WLI Forum believe that open competition between compatible products will benefit customers by assuring them that their wireless LAN will support the best products on the market today and will furthermore offer unparalleled flexibility and adaptability for the future.

http://www.wlif.org/

Wireless Local Area Networking Association (WLANA)

The Wireless LAN Association is a non-profit educational trade association, comprised of the thought leaders and technology innovators in the local area wireless technology industry. Through the vast knowledge and experience of sponsor and affiliate members, WLANA provides a clearinghouse of information about wireless local area applications, issues and trends and serves as a resource to customers and prospects of wireless local area products and wireless personal area products and to industry press and analysts.

http://www.wlana.com/index.htm

Wireless Opportunities Coalition (WOC)

The Wireless Opportunities Coalition (WOC) is a diverse group of organizations and companies dedicated to preserving and expanding the opportunities for growth in the wireless industry. The coalition's primary focus is to support the development, manufacturing, and use of wireless communications and related devices that are not licensed by the Federal Communications Commission but are regulated under Part 15 of the FCC's rules.

The Wireless Opportunities Coalition is working to communicate -to the FCC, Congress, and the public- the importance of preserving access to the use of these low-cost, unlicensed devices on the public airwaves.

http://wireless.policy.net/wireless/wireless.html

Wireless Research Group

At Cornell University, the Wireless Research Group develops systems for future wireless networks. Its activities cover primarily the design, fabrication, and testing of digital millimeter and microwave transmitters and receivers.

Chapter 9

PRESENT MARKETS and APPLICATIONS

Wireless networking is applicable to all industries with a need for mobile computer usage or when the installation of physical media is not feasible [15]. Such networking is especially useful when employees must process information on the spot, directly in front of customers, via electronic-based forms and interactive menus. Wireless networking makes it possible to place portable computers in the hands of mobile frontline workers such as doctors, nurses, warehouse clerks, inspectors, claims adjusters, real estate agents, and insurance salespeople.

The coupling of portable devices with wireless connectivity to a common database and specific applications meets mobility needs, eliminates paperwork, decreases errors, reduces process costs, and improves efficiency. The alternative to this is utilizing paperwork to update records, process inventories, and file claims. This manual method processes information slowly, produces redundant data, and is subject to errors caused by illegible handwriting. The wireless computer approach using a centralized database is clearly superior.

9.1 Retail

Retail organizations need to order, price, sell, and keep inventories of merchandise. A wireless network in a retail environment enables clerks and storeroom personnel to perform their functions directly from the sales floor. Salespeople are equipped with a pen-based computer or a small computing device with bar code reading and printing capability, with the wireless link to the store's database. They are then able to complete transactions – such as pricing, bin labeling, placing special orders, and taking inventory – from anywhere within the store.

In some cases, the batch-based scanner/printer has enough memory to store all the price information needed to effectively perform the pricing function throughout a shift or entire day. This situation makes sense if the price information is updated in

the database once a day, typically during the evening. The clerks load the data on to the device at the beginning of their shifts and then walk throughout the store continuously pricing items within the store. If the memory in the device is not large enough to store all the data, however, a wireless network connection, the data can be stored in the much larger memory capabilities of a centralized PC server or mainframe and accessed each time the item's bar code is scanned. In addition, a wireless network-based solution has merits if it is too time consuming to download in to a batch device.

9.2 Warehouses

Warehouse staff must manage the receiving, putting away, inventory, and picking and shipping of goods. These responsibilities require the staff to be mobile. Warehouse operations have traditionally been a paper-intensive and time-consuming environment. An organization can eliminate paper, reduce errors, and decrease the time necessary to move items in and out, however, by giving each warehouse employee a handheld computing device with a bar code scanner interfaced via wireless network to a warehouse inventory system.

The inventory system keeps track of all transactions, making it easy to produce accurate inventory reports. As shipping orders enter the warehouse, the inventory system produces a list of the items and their locations. A clerk can view this list from the database via a handheld device and locate the items needed to assemble a shipment. As the clerk removes the items from the storage bins, the database can be updated via the handheld device. All the functions depend heavily on wireless networks to maintain real-time access to data stored in a central database.

9.3 Healthcare

Healthcare centers such as hospitals and doctors' offices, must maintain accurate records to ensure effective patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record rest results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms healthcare stuff, taking 50-70 percent of their time.

Doctors and nurses are also extremely mobile, going from room to room caring for patients. The use of electronic patient records, with the ability to input, view and update patient data from anywhere in the hospital, increases the accuracy and speed of healthcare. This improvement is possible by providing each nurse and doctor with a wireless pen-based computer, coupled with a wireless network to databases that store critical medical information about the patients.

A doctor caring for someone in the hospital, for example, can place an order for a blood test by keying the request into a handheld computer. The laboratory will receive the order electronically and dispatch a lab technician to draw blood from the patient. The laboratory will run the tests requested by the doctor and enter the results into the patient's electronic medical record. The doctor can then check the results via the handheld appliance from anywhere in the hospital.

Another application for wireless networks in the hospitals is the tracking of pharmaceuticals. The use of mobile handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug transactions, such as receiving, picking, dispensing, inventory taking, and the tracking of drug expiration dates. Most importantly, however, it ensures that hospital staff can administer the right drug to the right person in a timely fashion. This would not be possible without the use of wireless networks to support a centralized database and mobile data collection devices.

9.4 Real Estate

Real estate salespeople perform a great deal of their work away from the office, usually talking with customers at the property being sold or rented. Before leaving the office, salespeople normally identify a few sites to show a customer, print the Multiple List Service (MLS) information that describes the property, and then drive to each location with the potential buyer.

Wireless networking makes the sale of real estate much more efficient. The real estate agent can use a computer away from the office to access a wireless MLS record. An agent can also use a portable computer and printer to produce contracts and loan applications for signing at the point of sale.

9.5 Hospitality

Hospitality establishments check customers in and out and keep track of needs, such as room-service orders and laundry requests. Restaurants need to keep track of the names and numbers of people waiting for entry, table status, and drink and food orders. Restaurant staff must perform these activities quickly and accurately. Wireless networking satisfies these needs very well.

9.6 Home and Small Office

Among the homeowners and small office people, a wireless LAN system is arising as an effective solution as compared to wired one for sharing the devices such as printers, scanners etc [16]. It's generally less expensive to set up a wireless LAN nowadays and provides not to lay down cabling throughout a home or small office. In addition to cost saving, mobility benefits are making more people to possess such kind of structure in their homes or offices, especially as wireless LAN prices continue to drop. Moreover when renting a house or office, a wireless structure may be the only solution according to the landlord's rules.

A wireless LAN system for the home and small office is very simple, generally composed of a single access point that connects directly to the underlying connection (such as ISDN, DSL, or cable modem) via a router.

9.7 General Enterprise Systems

In the past, the implementation of a wireless LAN cost was relatively much higher than the high performance wired one. This drawback caused the wireless applications to be more efficient than wired to satisfy the cost-affectivity. However by lowering the wireless prices and increasing the performance, many enterprise information system managers are beginning to consider seriously the use of wireless LANs instead of traditional Ethernet. The benefits are providing mobile and portable access to general network functions such as e-mail, Internet browsing, access to databases, and so on and eliminating the time and expense of installing and

supporting physical cable. So, wireless LANs are today effectively satisfying applications in horizontal markets.

9.8 Wireless Services

Most wireless LAN applications reside inside buildings and are privately owned. Many companies, however, are in the process of constructing wireless networks in metropolitan areas to offer non-point-to-point wireless connectivity to subscribers in fixed locations. As a result, these companies are offering wireless services to provide options to traditional wire-based technologies such as ISDN, DSL, and cable modem. Because of lack of wires subscribers can initiate services much faster.

9.9 Utilities

Utility companies operate and maintain a highly distributed system that delivers power and natural gas to industries and residences [15]. Utility companies must continually monitor the operation of the electrical distribution system and gas lines, and must check usage meters at least monthly to calculate bills. Traditionally, this means a person must travel from location to location, enter residences and company facilities, record information, and then enter the data at a service or computing center. Today, utility companies employ wireless networks to support the automation of meter reading and system monitoring, saving time and reducing overhead costs.

9.10 Field Service

Field service personnel spend most of their time on the road installing and maintaining systems or inspecting facilities under construction. To complete their jobs, these individuals need access to product documentation and procedures. Traditionally, field service employees have had to carry several binders of documentation with them to sites that often lack a phone and even electricity.

In some cases, the field person might not be able to take the entire document with him to a job site, causing him to delay the work while obtaining the proper

information. On long trips, this information may also become outdated. Updates require delivery that may take days to reach the person in the field. Wireless access to documentation can definitely enhance field service. A field service employee, for example, can carry a portable computer connected via wireless network to the office LAN containing accurate documentation of all applicable information.

9.11 Field Sales

Sales professionals are always on the move meeting with customers. While on site with a customer, a salesperson needs access to vast information that describes products and services. Salespeople must also place orders, provide status - such as meeting schedules - to the home office, and maintain inventories.

With wireless access to the home office network, a salesperson can view centralized contact information, retrieve product information, produce proposals, create contracts, and stay in touch with home office staff and other salespeople. This contact permits salespeople to complete the entire sale directly from the customer site, which increases the potential for a successful sale and shortens the sales cycle.

9.12 Vending

Beverage and snack companies place vending machines in hotels, airports, and office buildings to enhance the sales of their products. Vending machines eliminate the need for a human salesclerk. These companies, however, must send employees around to stock the machines periodically. In some cases, machines might become empty before the restocking occurs because the company has no way of knowing when the machines runs out of a particular product.

A wireless network can support the monitoring of stock levels by transporting applicable data from each of the vending machines to a central database that can be easily viewed by company personnel from a single location. Such monitoring allows companies to be proactive in stocking their machines, because they will always know the stock levels at each machine.

Remote monitoring of vending machines reduces the number of delivery visits, determines the optimal amount of inventory to be carried on the delivery trucks and reduces the cost of servicing the vending machines [21].

9.13 Credit Card Devices

Credit card devices are commonly referred to as wireless point of sale credit card verification. These devices operate away from power and land-line connections but have the capability to receive credit card information (swipe card) and transmit it for validation and processing.

9.14 Parking Meters

Wireless parking meter monitors alleviate many of the high costs associated with meter monitoring. Parking meters that have wireless transmitters can call an attendant when it detects it has run out of time and a car is in front of it (by a sonic sensor).

9.15 Environmental Monitoring

Wireless service is the most practical method of transferring small amounts of telemetry and monitoring information in rural areas. Environmental monitoring applications include water levels, earthquake sensors, fire watch (temperature), contamination level monitoring, bridge corrosion detection and other types of sensors that are located in rural regions.

9.16 Energy Management

Energy management can be enabled by wireless networks. Smart "thermostat-like" panels allow businesses and homes to use electricity more efficiently by programming heating, ventilation and air conditioning system and hot water heater. Devices within the building would communicate with one another over existing electrical wiring using power line carrier (PLC) technology. Two-way wireless data

networks could provide a connection between the building and a utility to deliver pricing signals, home management services, and public information, and to send customer messages and device status signals back to the utility.

9.17 Dispatch

Dispatch is the monitoring and scheduling of information to workers. It consists of issuing work tickets, providing routing information or directions, tracking and data collection, inventory levels and order entry for parts and other mobile work related functions. Wireless data provides many companies, such as taxi and limousine companies, with dispatch messaging services.

9.18 Wireless E-mail

Wireless email is the sending and receiving of short messages of text to a portable computing device. Because most wireless data systems have limited data transfer rates and have a high cost of service for large amounts of data, a wireless data system must allow the user to select if the delivery of large attachments is desired.

9.19 Wireless Internet

Wireless Internet involves communicating with the Internet, particularly the web, without wires. Because communicating with the Internet can require the transfer of large amounts of data (for pictures and audio clips) and interconnection has been normally costly, wireless Internet has had limited success until recently.

There are several advantages associated with wireless Internet. The first is the Internet service provider can commonly bypass the local telephone company. Users of their service may directly connect to their computers without the need for a telephone line. Next, wireless Internet service provides more efficient use of the Internet site communications interface. This is because a single interface can be processing multiple users as opposed to the Internet service provider having modems for each user that is connected to a phone line.

To allow more efficient communication between wireless devices and the web, handheld device markup language (HDML) was created. HDML provides similar features as hypertext markup language (HTML) without the intense use of graphics, through the limited use of input keys. This allows devices such as cellular telephones to take advantage of information on the web without transferring large quantities of data.

9.20 Mobile Computing

Mobile computing provides the ability for mobile workers to connect to information sources while on the road. Mobile computing can involve a combination of wired and wireless connection. Typical applications for mobile computing include sales force automation, inventory tracking and scheduling appointments and tasks.

9.21 Advertising

Advertising is starting to find its way into wireless devices. Already, some cellular phone systems automatically call a roaming customer that has entered into their system to inform them that they are authorized to use the service in their system.

Wireless data can be used to send advertising messages to billboards, displays on vending machines or to set top boxes that display text or graphics on televisions or monitors.

9.22 Vehicle Monitoring Services

In some vehicles, wireless devices such as cellular telephones and vehicle tracking systems are being integrated as part of the vehicle's electronics system. Vehicular applications include traffic alert bulletins and re-routing directions. Some automobile manufacturers have begun the standardization effort to create plug-and-play equipment for the consumer electronics in automobiles. In one application, if the car develops a fault (breaks down), a wireless data transmitter automatically calls for help to the nearest location and begins transmitting stored computer data to aid in diagnosis of the problem which is likely occurring.

Chapter 10

DISCUSSIONS

10.1 Comparisons

A wireless network is primarily intended as a complement to an existing wired network and possibly, over time, may replace the wired network in settings where mobility and constant connectivity are important. Wireless is perfect for users who want the convenience to roam without being cabled and the flexibility to take the network as moving.

While wireless networks are getting faster and improving over the wireless networking products that were available just a few years ago, none of the wireless products on the market compare in performance to a typical hard-wired 100Mb (megabit) Ethernet network in terms of price and performance, as well as speed and reliability [54]. Networking components for 100Mb networks still cost only a fraction of the price of new wireless networking equipment. While the price has been coming down, wireless networking adapters still cost up to four times the amount of standard 100Mb Ethernet adapters.

Pros and cons of wireless and wired media can be generally outlined as seen in table 10.1 [56].

TABLE 10.1 General comparisons of wireless and wired systems

	Wireless	Wired
Pros	• Eliminates wiring cost. • Accommodates mobile work-stations. • Transmission medium almost free.	• Equipment required simple and less expensive compared wireless. • Allows expansion of bandwidth. • High-speed physical connections. • Physical connection means more reliability.
Cons	• Less secure • Regulatory restrictions • Slower in comparison to wired.	• Wiring very expensive to install and maintain. • Does not accommodate mobile workstations.

10.1.1 Bandwidth

In wired medium the bandwidth is only limited due to the wires between two stations. Bandwidth can be increased by connecting more wires or by changing the quality of wires etc. So wired medium has virtually unlimited bandwidth (limited by physical limits), while wireless medium can use only a limited [allowed by the authorities] bandwidth in order not to interfere with other transmissions (like TV/radio broadcasting) [46]. For wireless medium the bandwidth is limited in terms of airwave congestion and propagation factors.

10.1.2 Reliability

In terms of reliability, wired medium is much more reliable than wireless. As the connection is physical there is little or no chance of data getting disarrayed. In case of wireless the data packets are sent over the airwaves. The sending station has to make sure that the frequency of the data is high enough for being received at the other end. The receiving end has to be sensitive enough to take all the data in. But reliability aspect differs according to the way of consideration. That is, reliability of wire is generally limited since it can be broken/loose its quality over the time. At the same time reliability of wireless medium (air/vacuum) is ~100% under normal operating conditions. However, under extreme operating conditions (such as nuclear explosion in the vicinity, for example, or even transmissions by unauthorized source) wireless medium cannot perform its functions. Moreover, wireless networks offer more reliability than cable networks because there is less length of physical connection to go wrong or to get damaged [47]. As most antennas are mounted up high i.e. roofs and masts there is less risk of people accidentally damaging the antennas. Because the transceivers are usually in doors this also reduces the chances of physical damage and as a result of this, the overall reliability of the network is increased.

10.1.3 Cable Faults

A problem inherent to wired networks is down time due to cable faults. In fact cable faults can be a primary cause of system downtime. Unprotected cable and even protected cables are prone to damage caused by erosion, storm damage and accidental damage and this can happen regularly. These problems are not easy to overcome if the cable runs under roads or water and could prove to be very expensive to rectify. Wireless links by comparison have fewer chances of faults occurring. Wireless equipment is generally accessible so maintenance can be carried out easily. The equipment it also modular so parts can be easily changed and replaced.

10.1.4 Natural Effects

Wind will not interfere with antennas because they are small and because they are built to withstand strong winds and gales. The outdoor equipment is fully waterproof and if necessary the transponders can also be mounted outside in a waterproof box to save space inside. Water, if persistent, can erode cable and it often cannot be detected until the network itself fails. By comparison, wireless equipment can be more easily checked at regular intervals as part of the annual maintenance, as it is more accessible.

10.1.5 Power

The wireless LANs use unguided media through air, which means that the transmission needs to be stronger than wired media, which are able to physically guide the transmitted signals [57]. Wireless networks need more power (from hundreds of milliWatts to several Watts) whereas in case of wired LANs signal power required is around tens of milliWatts.

10.1.6 Overhead

The Wireless LANs protocols have usually a higher overhead than their wired counterpart (such as Ethernet) [36]. This is due to different factors:

The first is the *radio technology*: radio receivers require large synchronization fields (receiver training, antenna selection...); the radio itself is slow to react (switch from receive to transmit), so needs large slots in the contention window and between packets.

The second is the addition of the *features* necessary for the radio protocol that makes the packet MAC headers larger (fields for network id, encryption parameters...) or introduces new management packets (synchronization, authentication, access point registration).

The third is that some *trade-offs* are made to improve the reliability. Acks and RTS/CTS add also some overhead. Having a slotted contention decreases the collisions but makes the average contention delay larger as well.

10.1.7 Mobility versus Portability

In a network environment, the terms mobility and portability imply the ability to move or carry a network device from one place to another. For example, in a wired network, a laptop computer can be disconnected from the network, carried to another location having a network connection, and reconnected to the network. In such an example, the laptop can remain "on" while it is motion, but network communications are interrupted while the laptop is carried from one location to another. The laptop only uses network communications while it is stationary at a fixed location having a network connection.

In a wireless network environment, "mobility" also implies that a network device can continue network communications without interruption while the device is in motion [52]. For example, handheld network devices are used outdoors by a number of rental car agencies to expedite the procedures for rental car returns. The customer's car is checked in, the method of payment is processed (including the approval process of a credit card transaction), and a receipt is printed for the customer. This device demonstrates the "mobility" feature of a wireless LAN where

the device maintains network communications while in motion, namely while the employee is roaming from customer to customer.

To sum up mobility versus portability in network environments:

Wired LAN = Portability

The ability to move a network device from one location to another. However, NO network communications exist while the device is in motion.

Wireless LAN = Portability + Mobility

The ability to move a network device from one location to another AND maintain network communications while the device is in motion

The notion of "mobility" in a wireless LAN environment is attributed to the fact that a wireless LAN is free of network cables. A mobile user is free to "roam" and maintain network communications while using a wireless network device. In a wired LAN environment, the freedom to roam doesn't exist.

In addition to mobility, expanding a wireless network can be done quickly, easily and with minimal labor cost. For example, to add a new computer to an existing wireless LAN is as simple as installing a new wireless LAN card into the new computer and turning on the card. In a wired network environment, expanding the network by adding one new computer can require large amounts of labor for cabling and possibly the additional expense of new network equipment. For example, adding a new computer may require the purchase of a new hub if no connections are available on the existing hub(s). In a wireless LAN environment, no such requirements exist.

10.1.8 Drawbacks

The most commonly cited drawback is lower data rates. The data transmission rate of an IEEE 802.11 wireless LAN card is 1 or 2 Mb/s. This rate may appear significantly lower than an Ethernet card running at an optimal 10 Mb/s. However, when Ethernet collision behavior, server latency and other network bottlenecks are factored in, the perceived data rate for wired and wireless LAN cards is virtually identical. Therefore, lower data rates of wireless LAN cards is no longer a drawback.

The second most cited drawback for wireless LAN is equipment cost. Nowadays, a wireless LAN card costs 2-4 times more than the average Ethernet card.

However, cost comparison between these two cards is not the whole picture. A potential user must also evaluate the cost savings of a wireless LAN due to the elimination of cable, jacks, cable management systems, network concentrators, and the labor required to install and maintain this equipment. Additionally, a potential user must also evaluate the increased value of a wireless LAN over a wired LAN due to the presence of mobile computing capabilities.

The third most cited drawback of wireless LAN technology is limited range. As with the other drawbacks, this drawback is only apparent because of inappropriate comparisons. According to one wireless LAN vendor, wireless LAN cards have a range of approximately 70-100 meters indoors and approximately 1000 meters outdoors (true line of sight). When comparing these ranges to the range of a cellular phone, wireless LAN doesn't seem very good. But because a wireless LAN card isn't a cellular phone this is not a good approach to compare. A wireless LAN card is a Local Area Network adapter so comparing with a 10BaseT wired Ethernet adapter seems more logical. The IEEE standard for 10BaseT Ethernet states that the maximum distance between a central hub and any station connected to it can be no more than 100 meters. Therefore, wireless LAN compares favorably when compared (appropriately) with other LAN technologies.

10.1.9 Mobile and Wireless

Mobile users do not necessarily need to use wireless interfaces and wireless interfaces do not necessarily support mobility [39]. A mobile user can simply connect to fixed networks using wired interfaces as he or she moves. Likewise, a fixed-location user might use a wireless interface (via a LAN) while sitting in an office. Therefore, mobile and wireless systems are not the same even though there is considerable overlap. Mobile networks provide support for routing (how to maintain communication with mobility) and location management (keeping track of the location) functions. Wireless networks provide wireless interfaces to users (both mobile and stationary) by supporting bandwidth allocation and error-control functions. When combined, there are several interesting issues that arise, including optimal use of low bandwidth channels due to limited frequency allocation, management of large bit-error rates due to high noise levels, application-level quality

of service support, increased security concerns, and failure or malfunctioning of equipment (Table 10.2).

TABLE 10.2 Mobile and wireless networking issues [Varshney 2000]

Issues	Possible Choices		Comments
Network Configuration	Infrastructure-based configuration		More scalable but less flexible
	Ad-hoc configuration		Less scalable but more flexible
Limitations of Devices	New protocols to handle device limitations		Interworking with existing protocols
	Content adaptation to device capabilities		Additional complexity at network/server
Bandwidth and Frequency of Operation	Use of existing frequencies (regulated/unregulated)		Lower bandwidth, higher interference, lower signal loss, lower cost
	Use of higher frequencies		Higher bandwidth possible, lower interference, higher signal loss, higher cost
Handoffs	Type of handoffs	Hard handoff	Device can communicate with one access point
		Soft handoff	Device can communicate with several access points
	Handoff Implementation	Network initiated	Network to compare signal access strength at several points
		Mobile assisted	Mobile to compare signals with several base stations and report to the current one
	Priority	User-based	Keep track of different classes of users
		Application-based	Keep track of different classes of applications
	Channel Assignment	Fixed-size	Easy but not suitable to all applications
		Variable	Difficult but suitable to applications
MAC Protocols	Frequency Division Multiple Access (FDMA)		Analog and amount of interference
	Time Division Multiple Access (TDMA)		Synchronization and slot speed match requirements
	Code Division Multiple Access (CDMA)		Difficult to satisfy varying bandwidth requirements

Table 10.2 (Continued) Mobile and wireless networking issues

Error Control	Error detection and retransmission		Impact on delay (not used for real-time applications)
	Error correction		Amount of excess bandwidth required
	Error correction and retransmission		Adaptive to the channel conditions
QOS Management	Admission control techniques		Amount of processing (micro-cellular environment)
	Priority to existing user's resource request		Knowledge of the traffic in nearby cells/clusters
	Dynamic advance reservation		Difficult to match user's future needs with network resources
	Adaptive error control techniques		Complexity and resource requirements
	QOS-oriented MAC protocols		Amount of protocol processing
	Channel borrowing from underloaded regions		Difficult to implement
Mobility Management	Addressing and Routing	Same address in different locations for a mobile user	Difficult to implement Exact location information is required for communications
		Different addresses	Complex routing
	Modification of existing protocols to deal with loss over wireless links		Differentiation between packet loss due to congestion and due to wireless links/user movement
Location Tracking	Broadcasting (paging) to locate a user		Delay, Amount of paging overhead
	Location updating by a user after every move		Amount of updating overhead
	Combination of paging and updating		
Applications and Middleware	Applications to adapt to varying QOS		Requires development of new applications
	Wireless middleware to deal with mobility allowing no changes in existing applications		Cost of building middleware to deal with heterogeneous wireless networks
Security	Encryption		Processing requirements at mobile devices
	Frequency hopping		Complex
	Use of infrared (indoors only)		Limited use
Failure	Deployment of back-up systems		High initial cost

The choice of media access control (MAC) can affect both performance and use of wireless networks. The MAC protocols used in cellular and PCS systems in the U.S. and Europe differ considerably. For example, the U.S. standards use FDMA (in AMPS), TDMA (in PCS), and CDMA (IS-95), while GSM uses TDMA/FDMA over different frequencies. This directly affects the interoperability and global roaming of mobile users. These differences are also affecting the standardization of the next (third) generation -3G- of wireless/mobile systems where North American companies are pushing for CDMA (or Wideband CDMA) to allow for backward compatibility with CDMA-based IS-95 while Europe is supporting TDMA for GSM compatibility. Some agreements on 3G systems have been reached, allowing all of the previously mentioned networks to inter-operate with or evolve into 3G wireless networks [51].

Mobile and wireless networks are also experiencing significant progress in the form of wireless local area networks (WLANs), satellite-based networks, Wireless Local Loops (WLL), mobile Internet Protocol (IP), and wireless Asynchronous Transfer Mode (ATM) networks. A comparison is shown in table 10.3.

TABLE 10.3 A comparison of several mobile and wireless networks [Varshney 2000]

Issues	Wireless LANs	Wireless Loops	Cellular/PCS	Mobile IP	Wireless ATM	Satellites
Coverage	Local Area	Local* or Metropolitan	Metropolitan	Wide Area	Wide Area	Wide Area
User Bandwidth	1-20Mbps	1-20Mbps	19.2Kbps	Network Dependent**	1-20Mbps	19-2Kbps to few Mbps***
Application	Data/voice	Voice/data	Voice/data	Data/voice	All	Voice/data
Major issue	Limited area	Interference	Bandwidth	Limited applications	Cost	Initial cost
Status	In use	Emerging	In use	Emerging	Emerging	Emerging

* Depending on the underlying technology such as 3-10 miles of LMDS.

** Bandwidth depends on the underlying wireless network.

*** Higher limit for satellites such as Teledesic.

10.1.10 Various Wireless Methods

The table 10.4 [45], [7] below compares the major features of the various wireless methods that are being used to provide Internet access.

TABLE 10.4 Various wireless methods

	IEEE 802.11b	**HomeRF**	**Bluetooth**
Speed	11, 5.5, 2, 1 Mbps	Mbps 1, 2, 10	30-400 Kbps
Use	Home, office or campus LAN	Home office, house and yard	Personal area network
Types of terminals	Add-on to notebook, desktop PC, Internet appliances, palm device, internet gateway	Add-on to notebook, desktop PC, modem, phone, Internet appliance, mobile device, Internet gateway	Built into notebook, cell phone, palm device, pager, appliance, car
Typical configuration	Multiple clients per access point	Point-to-point or multiple devices per access point	Point-to-point or multiple devices per access point
Range	50 to 300 feet	150 feet	30 feet
Frequency sharing	Direct sequence spread spectrum	Wideband frequency hopping	Narrowband frequency hopping
Power	More Power Required	Low Power Mode	Low Power Mode
Topology	Distributed Ctrl. Points	Peer-Peer	Multi point-to-point
Phone support	Requires IP Telephony	4+ Lines (DECT)	3 lines
Physical Interface	2.4 GHz DSSS	2.4 GHz 802.11 FHSS 50 hops/sec	2.4 GHz FHSS radio 1600 hops/sec
MAC Layer	IEEE 802.11	OpenAir & DECT	Non-IP base
Certification	WECA	Purdue's PlugLab	Various
Backers	Cisco, Lucent, 3Com, WECA consortium	Apple, Compaq, Dell, HomeRF Working Group, Intel, Motorola, Proxim	Bluetooth Special Interest Group, Ericsson, Motorola, Nokia
Status	Shipping	Shipping	In development
URL	http://www.wirelessethernet.com/	http://www.homerf.org	http://www.bluetooth.com

10.1.11 802.11 versus HiperLAN2

Table 10.5 summarizes the characteristics of 802.11, 802.11b, 802.11a, and HiperLAN2.

TABLE 10.5 Comparison 802.11 V/S HiperLAN2 [Jhonsson 1999]

Characteristic	802.11	802.11b	802.11a	HiperLAN2
Spectrum	2.4 GHz	2.4 GHz	5 GHz	5 GHz
~Max physical rate	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
~Max data rate, layer 3	1.2 Mb/s	5 Mb/s	32 Mb/s	32 Mb/s
Medium access control/Media sharing	Carrier sense	CSMA/CA		Central resource control/ TDMA/TDD
Connectivity	Conn.-less	Conn.-less	Conn.-less	Conn.-orientated
Multicast	Yes	Yes	Yes	Yes *1
QoS support	(PCF) *2	(PCF) *2	(PCF) *2	ATM/802. 1p/RSVP/DiffServ (full control)
Frequency selection	Frequency-hopping or DSSS	DSSS	Single Carrier	Single carrier with Dynamic Frequency Selection
Authentication	No	No	No	NAI/IEEE address/X.509
Encryption	40-bit RC4	40-bit RC4	40-bit RC4	DES, 3DES
Handover support	(NO) *3	(NO) *3	(NO) *3	(No) *4
Fixed network support	Ethernet	Ethernet	Ethernet	Ethernet, IP, ATM, UMTS,FireWire, PPP *5
Management	802.11 MIB	802.11 MIB	802.11 MIB	HiperLAN2 MIB
Radio link quality control	No	No	No	Link adaption

***1.** Two different modes supported, multicast via a dedicated MAC-ID (same as for 802.11) and N*unicast for improved quality.

***2.** Point Control Function, a concept defined in 802.11 to allow certain time slots being allocated for realtime-critical traffic.

***3.** Requires signaling over the fixed network, which is still proprietary.

***4.** Requires signaling over the fixed network, to be specified by H2GF.

***5**. Ethernet supported in first release.

10.2 General about PAN, LAN, WAN

Table 10.6 illustrates wireless technologies for PANs, table 10.7 gives an overview of WLAN technologies, Table 10.8 gives an overview of WWAN technologies[32].

TABLE 10.6 Wireless Personal Area Networking Technologies [Richardson 2001]

Key Technologies	Dataspeeds (Max/Average)	Date of Introduction	Likelihood of Success	The Good	The Bad	The Bottom Line
Bluetooth	Variable to max. 723.2 Kbps	2001	High	Low-cost replacement for cables	Interferes with other technologies in the 2.45GHz frequency band, such as 802.11b; limited security	By 2004, Bluetooth will replace cables and infrared as the primary connectivity solution for applications such as synchronization between devices (0.7 probability)
Infrared	Typically 9.6 Kbps to 115 Kbps through serial ports; extensions offer 1-Mbps and 4-Mbps max. data rates	Already in use	High	Very low cost, reliable and secure in-room	Poor early interoperability hindered uptake; requires line of sight	Will be usurped by Bluetooth as the primary means of wireless interdevice communication
802.15.1	Variable to max. 723.2 Kbps	2002	High	See Bluetooth	See Bluetooth	Formalized development of the Bluetooth standard within an accredited standards organization
802.15.3 High Rate	Designed for applications requiring greater than 20 Mbps	2003	Medium	High data rates	Potentially expensive; no proven backward compatibility with existing Bluetooth devices	Necessary development, but case not yet proven; widespread deployment only after 2005
Time Modulated Ultra Wideband	>20 Mbps	2006	High	High data rates, myriad applications, requires no dedicated frequency	Not approved, current silicon solutions expensive	Underhyped potentially revolutionary technology

TABLE 10.7 Wireless Local Area Networking Systems [Richardson 2001]

Application	Key Technologies	Dataspeeds (Max/Average)	Date of Introduction	Likelihood of Success	The Good	The Bad	The Bottom Line
Enterprise Networking	802.11	2 Mbps/ 1.2 Mbps	Already in use	Medium	Wireless local area networking	Slow, expensive, poor security	Good start but now superceded
	802.11b	11 Mbps/5.5 Mbps	Already in use	Medium	Faster, cheaper, stronger than 802.11	Security still not cast iron, more expensive than wireline	Viable for widespread enterprise adoption now
	802.11g	22 Mbps	2002	High	Faster than 802.11b	Specification not fixed, competing technologies could divide vendor focus	Should supersede 802.11b within 18 months
Enterprise and Metropolitan Area Networking	802.11a	54 Mbps/24 Mbps, future iterations being planned to support up to 100 Mbps	2002	Medium	Faster than 802.11b and 802.11g	New modulation scheme and different frequency band, unlikely to be backward compatible with 802.11b. No support for voice in initial specification. Costs not proven, likely to be relatively expensive	Available 2002, but wait 12 months for cost reduction
	HiperLAN/2	54 Mbps/24 Mbps	2002	Medium	Backed by "big names," supports connection-oriented services such as voice	Likely to be expensive. Direct competitor with 802.11a; likely to be the loser in a head-to-head competition	Will struggle against competition from 802.11a
Home Networking	HomeRF	2 Mbps/1 Mbps; planned future iterations will support up to 10 Mbps	Already in use	Medium	Fast, cost-effective home networking standard	Unlikely to be established outside home environment	Some penetration, but fails to become mainstream

TABLE 10.8 Wireless Wide Area Networking Systems [Richardson 2001]

Application	Key Technologies	Dataspeeds (Max/Average)	Date of Introduction	Likelihood of Success	The Good	The Bad	The Bottom Line
Second-Generation (2G) W-WANs	GSM	9.6 Kbps circuit-switched	Already in use	High	Dominant 2G mobile telephony standard	Spectrum becoming scarce	The "VHS" of the mobile phone world
	CDMA (IS95A)	9.6 Kbps circuit-switched	Already in use	High	Improved spectrum efficiency compared with GSM and TDMA	Smaller international footprint than GSM	Elegant 2G to 3G migration path, no future guarantee
	TDMA (IS136)	9.6 Kbps circuit-switched	Already in use	High	Reasonable Americas footprint	Something of a "dead end" when it comes to future migration	Soon to reach the end of the road
	CDPD	19.2 Kbps packet-switched	Already in use	Low	Packet data for TDMA	Limited deployment and only 19 Kbps	No future migration path
	PDC	9.6 Kbps circuit-switched	Already in use	High	Protected Japan-only technology	Protected Japan-only technology	Protected Japan-only technology
Interim Generation (2.5G) W-WANs	HSCSD	115 Kbps/ 28.8 Kbps	Already in use	Low	Dedicated data channels that can be combined to provide high data rates	Little terminal equipment, few network deployments and expensive	Low cost of deployment, but few care
	GPRS	171.2 Kbps/ 28 Kbps	2001	High	Packet data for GSM world	Data rates may disappoint bandwidth hungry	GPRS will be the single most successful packet data technology through 2005 (0.8 probability)
	EDGE Classic	384 Kbps/ 64 Kbps	2003	Low	Higher data rates for both circuit and packet networks	Expensive to deploy, little terminal support and will coincide with W-CDMA	Technology that has garnered interest, but unlikely to succeed
	EDGE Compact	250 Kbps/ 56 Kbps	2002	Low	Higher data rates for both circuit and packet TDMA networks	Main proponent, AT&T Wireless, has changed direction. Will now adopt GSM-GPRS and W-CDMA as route to 3G services	Technology that has garnered interest, but unlikely to be successful
	CDMA IS95B	115 Kbps/ 64 Kbps	Already in use	Medium	Interim packet data technology for CDMA networks. Terminals backward compatible with IS95A	Only adopted in South Korea and Japan	Most carriers will prefer to deploy cdma2000 1xMC
	cdma2000 1xMC	307 Kbps/ 144 Kbps	2002	High	High data rates, smooth migration path	Limited global footprint	The "Betamax" of the mobile phone world

TABLE 10.8 (Continued) Wireless Wide Area Networking Systems

Application	Key Technologies	Dataspeeds (Max/Average)	Date of Introduction	Likelihood of Success	The Good	The Bad	The Bottom Line
	PDC-P	9.6 Kbps packet data	Already in use	High	The bearer technology underlying NTT DoCoMo's i-mode service; currently the world's most successful wireless packet data technology	Protected Japan-only technology; only 9.6 Kbps	Currently most successful wireless packet data technology
Third-Generation (3G) W-WANs	W-CDMA	2 Mbps/ 144 Kbps	2001-2003	High	High data rates, massive industry support	High licence fees in many markets may hinder cost reduction	WCDMA becomes de facto global 3G standard by 2003 (0.7 probability)
	cdma2000 3xMC	2 Mbps/ 144 Kbps	2004	Low	Backward compatible with 1xMC and IS95A	Rapidly cooling support from previous proponents of cdma2000.	Despite undoubted technology benefits — success unlikely
	CDMA 1x EV DV	2.4 Mbps	2003	Medium	High data rates, straightforward migration path	Limited global footprint	Will be deployed but will not be mainstream
	CMDA 1 XTREME	5.2 Mbps	2004	Low	Even higher data rates from the evolved CDMA 1x specification	Proprietary developments by Motorola and Nokia.	No indications of intent from carriers
Fourth-Generation (4G) W-WANs	Undefined	>100 Mbps	2010-2015	High	Based on applications not technology; data rates are assumed to be enough	No concerted effort from single interest group likely to lead to fragmented efforts	The basis for the Supranet

Chapter 11

FUTURE WORKS and CONCLUSIONS

11.1 Future Studies

The next decade years will be technologically volatile in the wireless networking concept, far more so than the previous decade. But the promise of the usable wireless data networking is now within the grasp of the regular mobile worker.

At the end of next five years, users expect to be able to synchronize their e-mail applications with their PDA using a variety of over-the-air media. The cheapest, and the most pervasive, will likely to be Bluetooth. However, wide-area packet data networks should be widely available in urban and suburban areas of first-world countries. These will potentially allow for remote access links to corporate intranets and e-mail servers. However, high overall data speeds will not be expected. Access to personalized data services can be expected, driven by extensive self-created profiles. For high-speed real-time access, public WLAN access points will provide the most economic solution. For example, by 2005, lounges in major airports, public areas in hotels, libraries and convention centers will be expected to provide WLAN access at shared access speeds greater then 20 Mbps.

Almost ten years after, the networking technologies will come so close each other that the distinction between personal, local, and wide-area domains will decrease. Wide-area access speeds (averaging less than 1 Mbps) will still be slow in comparison with personal area and local area links (averaging more than 50 Mbps), but applications will be designed to cope with the differentials.

The Gartner Group has some strategic business assumptions for the rest of this decade [32]:

By 2005 enterprise users will use Bluetooth as the standard method for linking untethered devices, replacing cables and infrared (0.7 probability).

By 2010, Bluetooth functionality will have merged with wireless LAN developments and will provide personal area network data speeds in excess of 20 Mbps (0.6 probability).

By 2005, 50 percent of Fortune 1000 companies will have extensively deployed WLAN technology based on evolved 802.11 standards (0.7 probability).

By 2010, the majority of Fortune 2000 companies will have deployed WLANs to support standard wireline LANs (0.6 probability).

The personal area network that described in section 2.5 is really interesting and will be applicable in future. A lot of interesting applications have been proposed which signify the potential of the technology [19]. These include:

If there is a need to exchange business cards, just shaking hands will do the job. The electronic card will be transferred automatically from the person's card device via his body, transmitted to the other person via his hand in contact with former's to his card device and vice versa.

When entering local supermarket the person's preferences of brands will be automatically transferred to the supermarket database from a PAN device in his foot to a PAN receiver in the supermarket floor (of course with permission).

It will be possible transfer information between all sorts of electronic devices: cellular phones, pagers, personal digital assistants (PDAs) and smart cards. For instance, when someone sends a telephone number on a pager, it could be transferred automatically to a cellular phone.

The problem of synching the address books of PDAs, mobile phone etc can be done seamlessly over a PAN.

When making a long distance call using a pre-paid card there will no need to key in the PIN first. The phone can sense PIN as soon as touching the keypad. The PIN will be transferred securely from the pre-paid card in the pocket to the phone by a simple touch.

Homework assignments, grades, shopping lists, errands, and reminders could be automatically exchanged among family members at the dinner table.

In case of medical emergencies the doctors will be able to immediately access all the patient's medical information at the touch of a finger.

IBM researcher David Thompson envisions a prosthetic memory system that could be hidden in one's clothing - a miniature camera to record those new faces, a

microphone hooked to a speech recognition system that would record and transcribe conversations, a visual display built into a wrist watch or displayed heads-up fashion on a pair of eyeglasses, and a very high-density hard disk.

When reaching house in the evening the door could open immediately as touching the door knob. An identification code could flow from the body to the door knob and on authentication it could open.

11.2 Conclusions

Wireless is viewed as an accepted technology, not an emerging technology. Therefore, potential users are looking for characteristics such as easily found service and lower costs for service and equipment. The acceptance of wireless technology among mobile users has forced network managers to explore new ways for providing people at all organizational levels to stroll freely by satisfying links to required resources. While wireless networking satisfies a considerable solution to the cabling and maintaining problems of traditional networks, it has actually a real potential to provide necessary infrastructure for the portable computing which shows tremendous growth nowadays. But of course, for this potential being come into life, wireless LAN technologies must develop and perform the same level of standardization, reliability, and security as wired networks.

Applications developers are building their products providing the capability to support wireless transmission, enabling users today's required mobile workforce. Many existing applications are being optimized for use over wireless networks. Already there may be found such software products that provide the user with connectivity between conventional wired systems and their wireless devices.

Nowadays, lots of companies in various type and size are using wireless technology to improve business operations, increase customer satisfactions, and enhance their income. Despite of requiring some developments, the technology has proofs demonstrated its usefulness in many kind of applications

Wireless LANs has got a real potential for extending existing LANs, especially in situations where adding wires is expensive, impractical, or having some problems about safety. In these circumstances, choosing the right one, infrared or radio

systems, is depend on the underlying area. Because wireless LANs bring productivity, mobility, and flexibility, they easily provide frequent move, improvements and changes, and solve the problems of hard-to-wire environments. They also offer seamless integration with wired LANs. Although wireless LANs provide remote sites with operational autonomy, they may still be managed from a central location via SNMP.

There is a fact that more and more people now know they're well on their way to the future [18]. But they want to travel light and not get bogged down in a morass of wires and unwieldy equipment. They need to access and share information on the move; and they need it fast. Even on an enterprise scale, many businesses expect to take charge of their servers, routers, or even entire networks from back-of-beyond locations.

These are the sentiments propelling the demand for wireless data transfer services. Adding fuel to this has been the dramatic increase in Internet usage and mobile telephony.

But, to make this new technology realize its purported potential, there must be an architecture that's flexible, open and standards-based. More importantly, wireless networks of the near future should be able to offer the convenience and economy of today's peer-to-peer IP networks, and deliver better value to service operators and end users alike.

Broadly speaking, wireless networks must have four key deliverables:

- The technology must be customizable, easy to use, and allow fast access to all services from a single device.
- A smooth migration path from existing wireless network protocols to the new wireless IP network is a must, and the new network must deliver superior performance.
- The new service must be made available immediately, while keeping the existing services going.
- The technology must be able to translate the wireless architecture into business, particularly for worldwide operators and service providers.

Wireless LANs are still 10 times slower than modern switched Ethernet LANs and are more than twice the price, and they cannot deliver the total site capacity of their wired Ethernet cousins.

In the right situations, however, it may make sense for certain enterprises to invest in wireless LANs. Enterprises should consider wireless LANs in these circumstances:

- To extend the functions of wired LANs where more workers carrying laptops and personal digital assistants demand convenient access to corporate network resources.
- To accommodate frequent physical plant additions, moves and changes that drive up the cost (and downtime) of maintaining a LAN connection.
- To accommodate intracompany site visitors and reduce the logistics and cost of getting those visitors access to their corporate network resources without having to find a spare Ethernet drop.
- To ease the frustration of getting connected to high-bandwidth networks for workers who carry their laptops between company offices, homes and, increasingly, public places such as airports, hotels and convention centers.

Mobile and wireless networks represent the next wave of networking because of their usefulness in assisting an emerging mobile workforce in a growing information-oriented society. However, mobile and wireless networks also present many challenges to application, hardware, software and network designers and implementers. In the near future, universal devices that can access the closest/best quality/cheapest wireless network out of several choices will be developed. Wireless networks will be able to implement a uniform addressing system, for example, in which a person has a consistent identifying number or network address that is portable across all wireless networks. Within this decade, these networks will almost compete with "wired" networks for applications with low to medium bandwidth requirements. However, with increased frequency allocations, advanced in semiconductor technology, and more efficient coding of information over wireless channels, mobile and wireless networks will become the networks of choice for most users and applications, making wired networks relics of the past.

The hardware needed for wireless networking includes an access point, various types of adapters, and possibly a wireless bridge. Wireless client devices are available as PCI (Peripheral Component Interconnect) cards, ISA (Industry Standard Architecture) cards, and PCMCIA (Personal Computer Memory Card International Association) cards for laptops. As prices continue to fall for wireless networking, products and demand for them keep growing. When choosing wireless networking equipment, it is a good idea to stick with one of the larger wireless vendors such as 3Com, Lucent, Cisco, and Nokia. There are lots of products in the market and as the prices decrease and as the standards grow the variety of products increases continuously. So that the scope of this study does not include the products of wireless systems.

For the final speaking, wireless systems have found places in almost every aspect of the information technologies; and the future and borders of wireless technology is just limited with the imagination of human being.

REFERENCES

[01] F. Anderson, "802.11a Speeds Wireless LANs", Internet document, http://www.itworld.com/Net/1749/NWW0129tech/pfindex.html, Network World, 29 January 2001

[02] J. Becker, "GPRS & WAP: A Giant Leap for Wireless Internet", Internet document, http://www.wirelessdesignonline.com/content/news/article.asp?DocID={864A1057-1ED9-11D5-A770-00D0B7694F32}, March 22, 2001

[03] D. Blankenbeckler, "An Introduction to Bluetooth", Internet document, http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html, 2000

[04] S. Buckingham,"An Introduction to the Wireless Application Protocol", Mobile Lifestreams Limited, Internet document, http://www.gsmworld.com/technology/yes2wap.html, January 2000

[05] S. Buckingham,"An Introduction to the General Packet Radio Service", Mobile Lifestreams Limited, Internet document, http://www.gsmworld.com/technology/yes2gprs.html, January 2000

[06] W. Caswell, "Designed for Homes and Ideal for Teleworkers", Network World, Southborough, 2001

[07] W. Caswell, "Wireless Home Networks Disconnected Connectivity ", Internet document, Home Toys Article, http://www.hometoys.com/mentors/caswell/apr00/wireless.htm, April 2000

[08] J. Cereceda, P. Houldsworth, "Wireless ATM: Technology and Applications", April 1997

[09] X. Cong, "Wireless ATM – An Overview"

[10] J. Conover, "802.11a: Making Space for Speed", Internet document, http://www.networkcomputing.com/1201/1201ws1.html, 8 January 2001

[11] G. Fleishman, "New Wireless Standards Challenge 802.11b", The O'Reilly Network, Internet Document, http://oreilly.wirelessdevnet.com/pub/a/wireless/2001/05/08/standards.html, 06 August 2001

[12] J. Geiger, " Wireless LANs", 1st ed., p. 1-41, USA, 1999

[13] J. Geiger, "Wireless LANs", 1st ed., p. 43-87, USA, 1999

[14] J. Geiger, “Wireless LANs”, 1st ed., p. 90-122, USA, 1999

[15] J. Geiger, “Wireless LANs”, 1st ed., p. 14-20, USA, 1999

[16] J. Geiger, “Wireless LANs”, 2nd ed., p. 17-21, USA, 2001

[17] J. Geiger, “Wireless LANs”, 2nd ed., p. 60-61, USA, 2001

[18] D. Gupta, “Wireless Networking Technologies of the Future”, ZDNet, Internet document, http://www.zdnetindia.com/techzone/networking/stories/12070.html, January 21, 2001

[19] P. Gupta, “Personal Area Networks: Say It And You Are Connected!”, Wireless Developer Network, Internet document, http://www.wirelessdevnet.com/channels/bluetooth/features/pans.html, 2000

[20] J. Haartsen, et. al, “Bluetooth: Vision, Goals and Architecture”, Mobile Computing and Communications Review, Volume 1 , Number 2.

[21] L. Harte, R. Dreher, S. Kellogg, T. Schaffnit, “The Comprehensive Guide to Wireless Technologies”, p. 129-134, USA, 2000

[22] M. Jhonsson, “HiperLAN2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band”, HiperLAN2 Global Forum, 1999

[23] R. Kawatra, “The IEEE 802.11b Standard”, Internet document, http://krypton.mnsu.edu/~kawatra/ieee80211.htm

[24] B. Kiacz, “HIPERLAN/1 Technical Overview”, Internet document, http://www.etsi.org/Technicalactiv/h1tech.htm

[25] B. Kiacz, “HIPERLAN/2, Technical Overview”, Internet document, http://www.etsi.org/Technicalactiv/h2tech.htm, September 2000

[26] M. E. Kounavis, “Multipath”, Internet document, http://www.ctr.columbia.edu/~mk/multipath.html

[27] D. L. Lough, T. K. Blankenship, K. J. Krizman, "A Short Tutorial on Wireless LANs and IEEE 802.11”, 1997

[28] V. Myslik, “Inroduction to IrDA”, Internet document, http://www.hw.cz/english/docs/irda/irda.html, 1998

[29] C. E. Perkins, D. B. Jhonson, “Mobility Support in IPv6”, Proceedings of the Second Annual International Conference on Mobile Computing and Networking (MobiCom’96), New York, USA, November 10-12 1996

[30] C. Perkins, “IP Mobility Support”, Internet-Draft, May 1996

[31] A. Proust, "Personal Area Network: A Bluetooth Premier", Internet document, http://oreilly.wirelessdevnet.com/pub/a/wireless/2000/11/03/bluetooth.html

[32] P. Richardson, "Personal to Global: Wireless Technologies, 2005-2010", Gartner Group Inc., February 23, 2001

[33] S. J. Schuchart Jr., "The Bluetooth Invasion Begins", Internet document, http://www.nwc.com/1206/1206ws3.html, March 19, 2001

[34] J. Scourias, "Overview of the Global system for Mobile Communications", October 1997.

[35] J. G. Sempere, "An Overview of the GSM System", IEEE Vehicular Technology Society, Scotland

[36] J. Tourrilhes, "The MAC level (link layer)", Internet document, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/ Linux.Wireless.Overview.htm, Hewlett Packard Laboratories, Palo Alto, 3 August 2000

[37] J. Tourrilhes, "Some Wireless LAN Standards", Internet document, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/ Linux.Wireless.Overview.htm, Hewlett Packard Laboratories, Palo Alto, 3 August 2000

[38] A. Trivedi, "Wireless Local Area Network IEE 802.11", Internet document, http://alpha.fdu.edu/~anandt/

[39] U. Varshney, Ron Vetter, "Emerging Mobile and Wireless Networks", Communications of the ACM, Vol. 43, No. 6, p. 73-81, June 2000

[40] U. Varshney, R. J. Vetter, R. Kalakota, "Mobile Commerce : A New Frontier", Computer, October 2000

[41] D. W. Suvak, "IrDA and Bluetooth: A Complementary Comparison", Extended Systems Inc., 2000

[42] D. W.Suvak, P. J.Megowan, "IrDA Infrared Communications:An Overview", Extended Systems Inc.

[43] J. Walrand, P. Varaiya, "High-Performance Communication Networks", p.306-309, 2nd ed., USA, 2000

[44] T. A. Wilkinson, "HIPERLAN An Air Interface Designed for Multimedia", HP Laboratory Bristol, UK, May 1995

[45] Internet document, http://content.Honeywell.com/yourhome/webpad/router_faq.htm

[46] Internet document, http://oh114.wpi.edu/~imaleev/ee536/ee536_h2.html

[47] Internet document, http://www.cybercityco.com/faq1.html

[48] Internet document, http://www.gsmdata.com

[49] Internet document, http://www.handytel.com/technology/bluetooth01.htm, 2001

[50] Internet document, http://www.intersil.com/design/prism/standards_organizations.asp, 2001

[51] Internet document, http://www.itu.org

[52] Internet document, http://www.linux-wlan.com/writings/linuxdev-funprofit/funprofit-whitepaper.html

[53] Internet document, http://www.palowireless.com/bluearticles/intro.html

[54] Internet document, http://www.smartcomputing.com

[55] Internet document, http://www.wow-com.com

[56] Internet document, http://www.wpi.edu/~shahzad/cs576/a2.htm

[57] Internet document, http://www.wpi.edu/~shahzad/cs576/a3.htm

[58] "HiperLAN", Internet document, http://www.hiperlan.uk.com/about/about_hiperlan2.htm

[59] "The Evolution of LANs from Wired to Wireless", Internet document, http://www.aironet.com/wireless

[60] "Wireless & Related Network Standards & Organizations", Intersil, Internet document, http://www.intersil.com/design/prism/standards_organizations.asp

[61] "Home Networking Technologies", Property of HomeRF Working Group, May 2001

[62] "Wireless Networking Choices for the Broadband Internet Home", Property of HomeRF Working Group, 2001