NEAR EAST UNIVERSITY LIBRARY 1988 - LEFKOŞA

NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIRELESS LAN AND ITS SECURITY

Graduation Project
COM- 400

Student : Fady Al-Lada'a (971488)

Supervisor : Assoc.Prof.Dr. Rahib ABIYEV

Nicosia 2005

NEAR EAST UNIVERSITY
LIBRARY
1988 - LEFKOŞA

ACKNOWLEDGEMENT

First of all, and before saying anything, I wish to thank ALLAH – our Creator – who gave me the morale and opened my mind to get this project done.

Then, I would like to show my special appreciations to my supervisor Assoc.Prof.Dr. Rahib Abiyev, for his kindness, humility, patience, and support. He was actually very helpful, And special thanks to Mr. Tayseer Al-Shanablah who provided me with brotherhood, which I – a foreign student – miss in this far away country from my homeland.

After that, I love to send my special thanks to my family, to whom it was not possible to be what I am now without them. I won't ever forget their encouragement and support as long as I am alive. Thank you father, you have always been my ideal. Mother, I am so glad to thank you at this particular moment of my life, your prayers helped making this day come true. I also thank Mohammed, you are my brother, and I guess this word explains my feelings. Finally special thanks to my little sister: Bassma. I love you all so much.

And I hope to thank all my friends, for helping, supporting, and guiding me through my study. Finally, thanks to everybody, and may ALLAH bless you all.

ABSTRACT

Wireless LAN is a group of computers which is connected together by wireless interfacing devices, and this group of computers has a different standards and protocols than other computer networks, which we are going to see in this project.

Wireless LAN helps organizations raise profits, cut costs, and increase efficiency. Wireless devices can be installed as an extension of your Ethernet™ backbone or as a standalone network.

Wireless networks offer many organizations a variety of key competitive advantages. Today's demanding and competitive marketplace environment has become extremely data-intensive.

Wireless LAN technology was specifically developed to move large amounts of data quickly and cost effectively. Wireless LANs have proven to help organizations of all kinds boost productivity, cut costs, and dramatically increase profitability by quickly accessing data.

TABLE OF CONTENTS

INTRODUCTION

A Network is a group of computers and other devices that connected to each other. The most common types of Networks are LAN, WAN MAN. Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface. With the introduction of small portable devices such as PDAs (personal digital assistants), the WLAN technology is becoming very popular. WLANs provide high speed data communication in small areas such as a building or an office. It allows users to move around in a confined area while they are still connected to the network. Examples of wireless LAN that are available today are NCR's wave LAN and Motorola's ALTAIR.

For some time, companies and individuals have connected computer with local area networks (LANs). This allowed the ability to access and share data, application and other services not resident on any one computer. The LAN users have at disposal much more information, data and applications then they could otherwise store by themselves.

With the increasing number of portable computers and highly mobile users, the need of wireless Local Area Networks is increasing. Wireless LANs are especially needed in environments that make the use of cable difficult or impractical. The main advantages offered by wireless LANs are portability, low installation costs and quick set up time.

Wireless Data Networks can be easily considered as the ultimate limit to data communications, if flexibility, mobility and ease of relocation are considered as the most important parameters of a network. Wireless LANs (WLANs) are just the wireless counterparts of those traditional low-ranges, high bit rate and shared medium communication networks termed as Local Area Networks by the IEEE and HIPERLAN.

CHAPTER ONE
1. OVERVIEW OF LOCAL AREA NETWORKS (LANs)

1.1 Introduction

A network is a group of computers, printers, and other devices that are connected together with cables. Information travels over the cables, allowing network users to exchange documents & data with each other, print to the same printers, and generally share any hardware or software that is connected to the network. Each computer, printer, or other peripheral device that is connected to the network is called a node. Networks can have tens, thousands, or even millions of nodes. In the simplest terms, a network consists of two or more computers that are connected together to share information.

Principal components of a computer network:

- Computers (processing nodes or hosts)
- Data communication system (transmission media, communication processors, modems, routers, bridges, radio systems, satellites, switches, etc)

1.2 How and Why Network Exists?

The concept of linking a large numbers of users to a single computer via remote terminal is developed at MIT in the late 50s and early 60s. In 1962, Paul Baran develops the idea of distributed, packet-switching networks. The first commercially available WAN of the Advances Research Project Agency APRANET in 1969. Bob Kahn and Vint Cerf develop the basic ideas of the Internet in 1973.

In early 1980s, when desktop computers began to proliferate in the business world, then intent of their designers was to create machines that would operate independently of each other. Desktop computers slowly became powerful when applications like spreadsheets, databases and word processors included. The market for desktop computers exploded, and dozens of hardware and software vendors joined in the fierce competition to exploit the open opportunity for vast profits. The competition spurred intense technological development, which led to increased power on the desktop and lower prices. Businesses soon discovered that information is useful only when it is communicated between human beings. When large information being handled, it was impossible to pass along paper copies of information and ask each user to reenter it into their computer. Copying files onto floppy disks and passing them around was a little better, but still took too long, and was impractical when individuals were separated by great distances. And you could never know for sure that the copy you received on a floppy disk was the most current version of the information-the other person might have updated it on their computer after the floppy was made.

For all the speed and power of the desktop computing environment, it was sadly lacking in the most important element: communication among members of the business team. The obvious solution was to link the desktop computers together, and link the group to shared central repository of information. To solve this problem, Computer manufactures started to create additional components that users could attach to their desktop computers, which would allow them to share data among themselves and access centrally located sources of information. Unfortunately the early designs for these networks were slow and tended to breakdown at critical moments.

Still, the desktop computers continued to evolve. As it became more powerful, capable of accessing larger and larger amounts of information, communications between desktop computers became more and more reliable, and the idea of a Local Area Network (LAN) became practical reality for businesses. Today, computer networks, with all their promise and power, are more complicated and reliable than stand-alone machines. Figure 1.1 shows the network connectivity of the world.

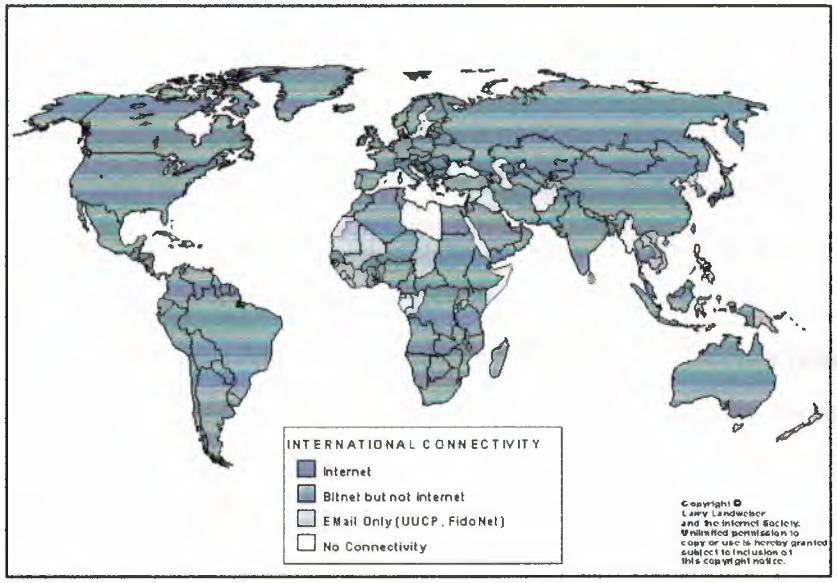

Figure 1.1 Computer Network Connectivity of the World

1.3 Goals of Computer Networks

1. Resource sharing and accessing them independently of their location.
2. Providing a universal environment for transmission of all kinds of information: data, speech, video, etc.
3. Supporting high reliability of accessing resources.
4. Distribution of loads according to the requirements very fast main frames, minis, PCs, etc.

1.4 Classification of Computer Networks

Network Classification Like snowflakes, no two networks are ever alike. So, it helps to classify them by some general characteristics for discussion. A given network can be characterized by its:

- Size: The geographic size of the network
- Security and Access: Who can access the network? How is access controlled?

- Protocol: The rules of communication in use on it (ex. TCP/IP, NetBEUI, AppleTalk, etc.)
- Hardware: The types of physical links and hardware that connect the network

Computer experts generally classify computer network into following categories:

- Local Area Network (LAN): A computer network, with in a limited area, is known as local area network (e.g in the same building)
- Wide Area Network (WAN): A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.
- Metropolitan Area Network (MAN): A data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media.
- Campus Area Network (CAN): The computer network within a limited geographic area is known as campus area network such as campus, military base etc.
- Home Area Network (HAN): A network contained within a user's home that connects a person's digital devices. It connects a person's digital devices, from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, home security systems, fax machines and other digital devices that are wired into the network.

In figure 1.2 the connecttivity of local area networks to metropolitan area networks and typical use of metropolitan area networks to provide shared access to a wide area network is shown.

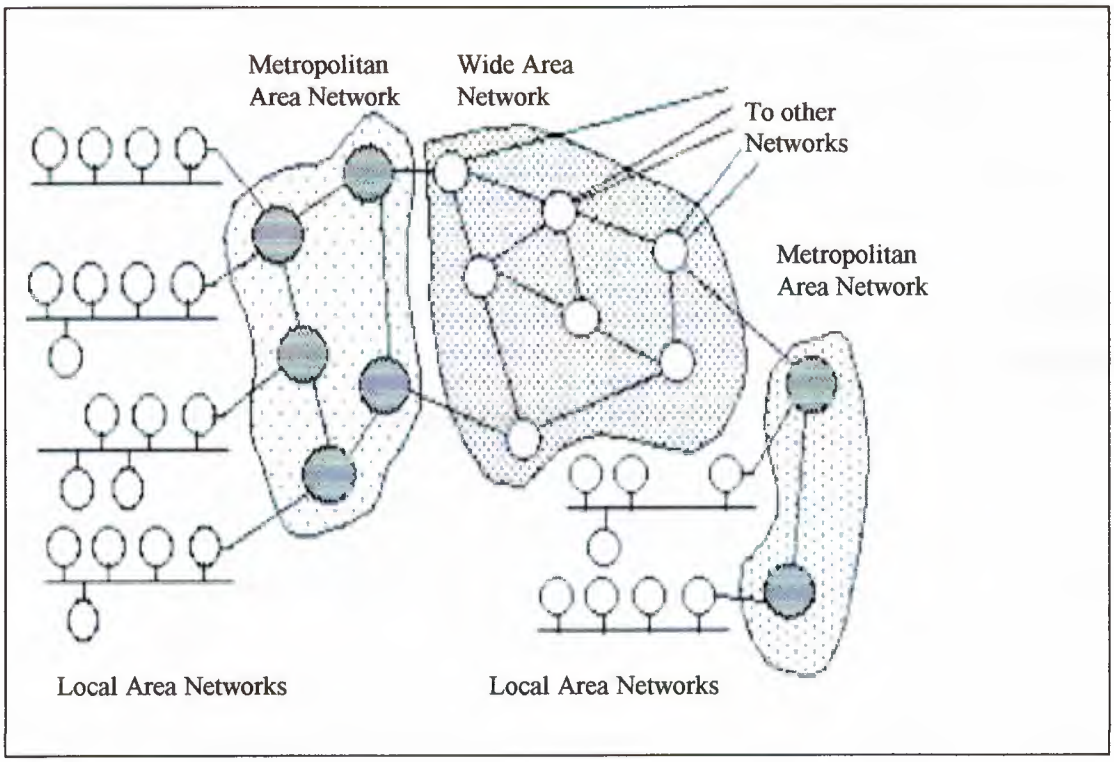

Figure 1.2 A typical use of MANs to provide shared access to a wide area network

Computer networks are used according to specified location and distance. In table 1.1 it is shown that which technology can be applied to the specific location and specific distance.

Table 1.1 Network Techonologies that Fit in Different Communication Spaces

NETWORK TYPE	DEFINITION	DISTANCE RANGE	COMMUNICATION SPACE
LAN	Local Area Network	0.1 to 1 Km	Building, floor, Room
WAN	Wide Area Network	100 to 10000+ Km	Region, Country
MAN	Metropolitan Area Network	10 to 100 Km	City
CAN	Campus Area Network	1 to 10 Km	Campus, Military base, Compnay site
HAN	Home Area Network	0.1 Km	Home

In Figure 1.3 a chart is shown which specifies the distances and speeds of different networks.

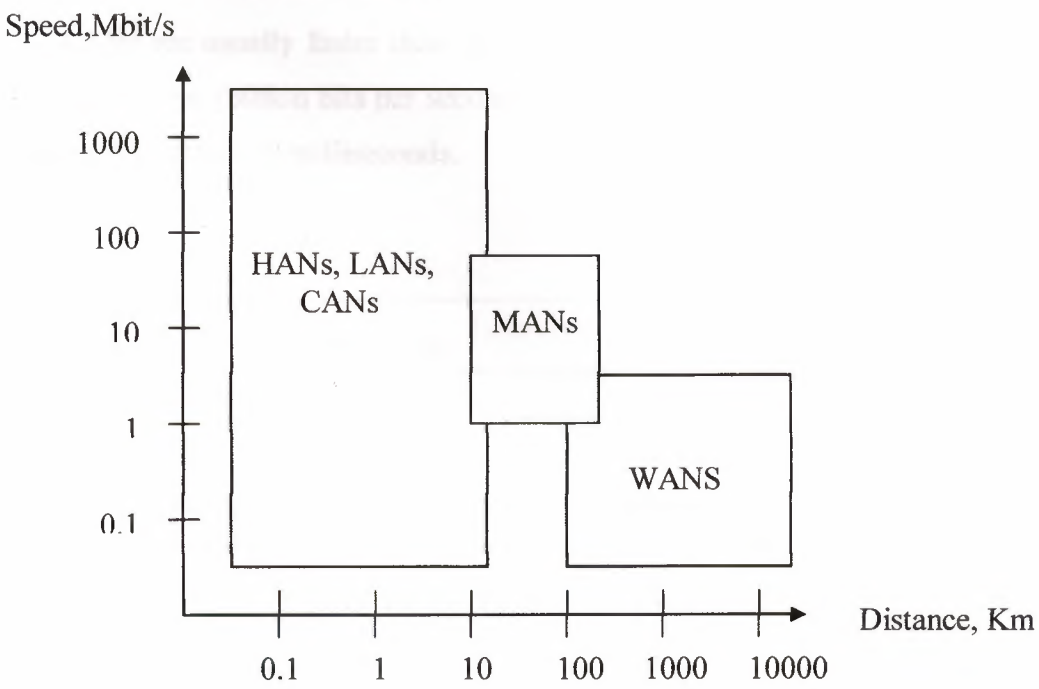

Figure 1.3 Distances and Speeds of the Different Networks

1.5 Local Area Networks

LANs are networks usually confined to a geographic area, such as a single building, office. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business organizations. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. Most LANs are built with relatively inexpensive hardware such as Ethernet cable and network interface cards (although wireless and other options exist). Specialized operating system software is also often used to configure a LAN. For example, some flavors of Microsoft Windows -- including Windows 98 SE, Windows 2000, and Windows ME -- come with a package called Internet Connection Sharing (ICS) that support controlled access to resources on the network.

1.6 LANs & WANs Comparison

LANs are usually faster than WANs, ranging in speed from 230 Kbps up to and beyond 1 Gbps (billion bits per second) as shown in Figure 1.4. They have very small delays of less than 10 milliseconds.

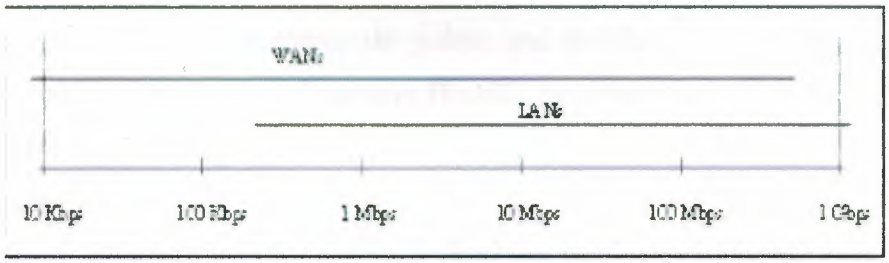

Figure 1.4 Data Speeds on LANs and WANs

How does one computer send information to another? It is actually rather simple. The figure 1.5 shows and explains a simple network.

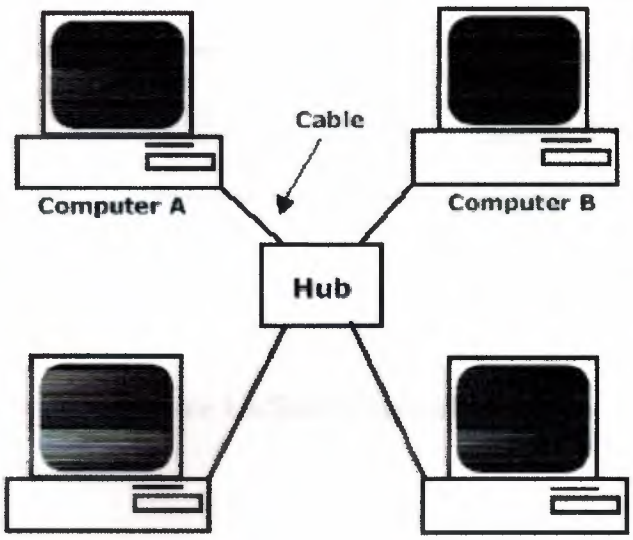

Figure 1.5 Simple Networks

If Computer A wants to send a file to Computer B, the following would take place:

1. Based on a protocol that both computers use, the NIC in Computer A translates the file (which consists of binary data -- 1's and 0's) into pulses of electricity.
2. The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
3. The hub takes in the electric pulses and shoots them out to all of the other cables.
4. Computer B's NIC interprets the pulses and decides if the message is for it or not. In this case it is, so, Computer B's NIC translates the pulses back into the 1's and 0's that make up the file.

Sounds easy. However, if anything untoward happens along the way, you have a problem, not a network. So, if Computer A sends the message to the network using NetBEUI, a Microsoft protocol, but Computer B only understands the TCP/IP protocol, it will not understand the message, no matter how many times Computer A sends it. Computer B also won't get the message if the cable is getting interference from the fluorescent lights etc. or if the network card has decided not to turn on today etc.

Figure 1.6 shows small Ethernet local area network.

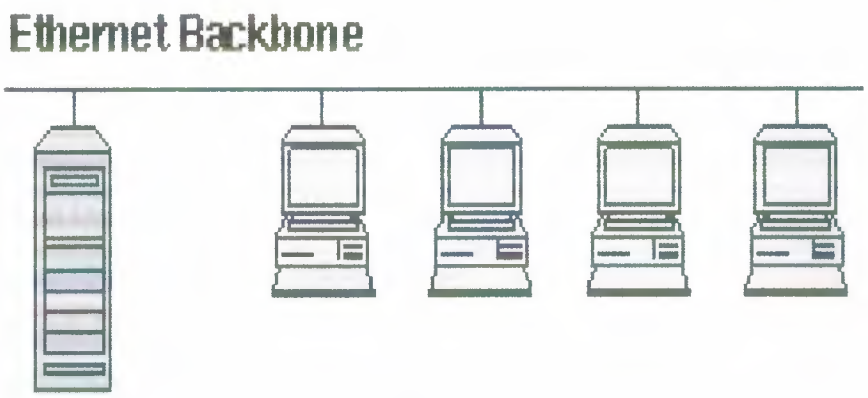

Figure 1.6 Small Ethernet LAN

The figure 1.7 shows briefly the interconnection of two LANs

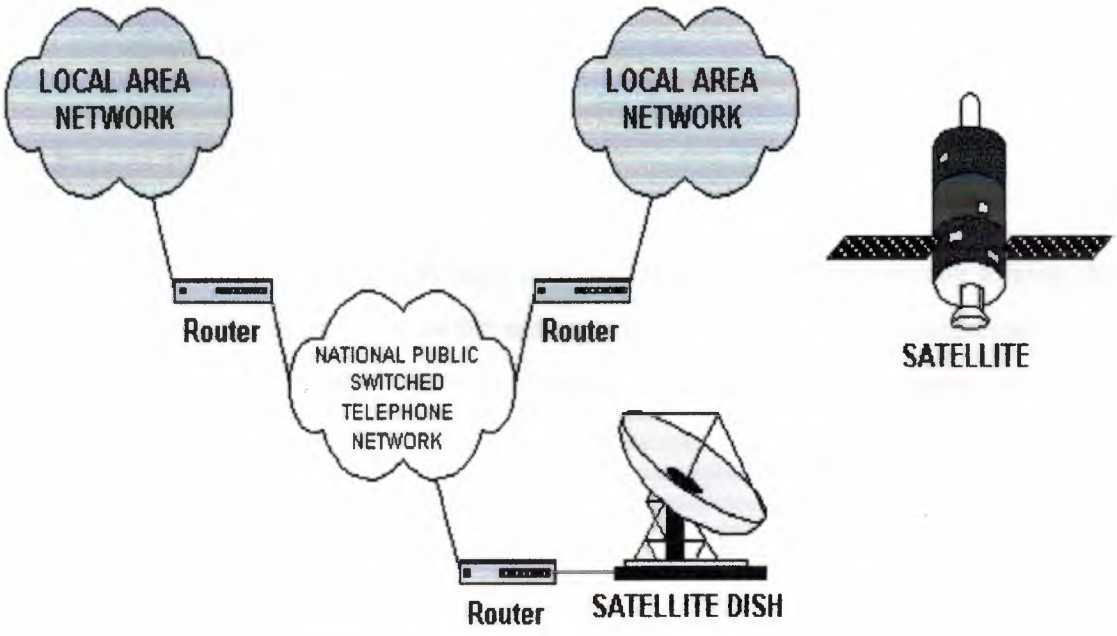

Figure 1.7 Interconnection of two LANs

1.7 Major Components of LANs

- Servers.
- Client / Workstation.
- Media.
- Shared Data.
- Shared Printers and other peripherals.
- Network Interface Card.
- Hubs / Concentrator.
- Repeaters, Bridges, Routers, Brouters, Gateways
- Physical connectors.
- Protocols.
- Network operating system (NOS).

1.8 Types of Local Area Networks

LANs are usually further divided into two major types:

1.8.1 Peer-to-Peer:

A peer-to-peer network doesn't have any dedicated servers or hierarchy among the computers. All of the computers on the network handle security and administration for themselves. The users must make the decisions about who gets access to what.

1.8.2 Client-Server:

A client-server network works the same way as a peer-to-peer network except that there is at least one computer that is dedicated as a server. The server stores files for sharing, controls access to the printer, and generally acts as the dictator of the network.

1.9 Local Area Networks Connectivity Devices

1.9.1 Repeaters

Boost signal in order to allow a signal to travel farther and prevent attenuation. Attenuation is the degradation of a signal as it travels farther from its origination. Repeaters do not filter packets and will forward broadcasts. Both segments must use the same access method, meaning that you can't connect a token ring segment to an Ethernet segment. Repeaters will connect different cable types.

1.9.2 Bridges

Functions the same as a repeater, but can also divide a network in order to reduce traffic problems. A bridge can also connect unlike network segments (i.e. token ring and Ethernet). Bridges create routing tables based on the source address. If the bridge can't find the source address it will forward the packets to all segments.

1.9.3 Routers

A router will do everything that a bridge will do and more. Routers are used in complex networks because they do not pass broadcast traffic. A router will determine the most efficient path for a packet to take and send packets around failed segments. Unroutable protocols can't be forwarded.

1.9.4 Brouters

A brouter has the best features of both routers and bridges in that it can be configured to pass the unroutable protocols by imitating a bridge, while not passing broadcast storms by acting as a router for other protocols.

1.9.5 Gateways

Often used as a connection to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.

1.10 Local Area Networks (LAN) in the work place and its advantages

Network allows more efficient management of resources. For example, multiple users can share a single top quality printer, rather than putting lesser quality printers on individual desktops. Also network software licenses can be less costly than separate, stand alone licenses for the same number of users.

Network helps keep information reliable and up-to-date. A well managed, centralized data storage system allows multiple users to access data from different locations, and limit access to data while it is being processed.

Network helps speeds up data sharing. Transferring files across a network is almost always faster than other, non-network means of sharing files.

Networks help business service their clients more effectively. Remote access to centralized data allows employees to service clients in the field, and clients to communicate directly to suppliers.

Speed: Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files is very time-consuming.

Security: Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.

Centralized Software Management: One of the greatest benefits of installing a local area network is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

Electronic Mail: The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, people can communicate with others throughout the world. Network allows workgroups to communicate more effectively. Electronic mail and messaging is a staple of most network systems, in addition to scheduling systems, project monitoring, on-line conferencing and groupware, all of which help work teams be more productive.

Workgroup Computing: Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

1.11 Emerging Technology, Wireless Networks

Wireless networking refers to hardware and software combinations that enable two or more appliances to share data with each other without direct cable connections. Thus, in its widest sense, wireless networking includes cell and satellite phones, pagers, two-way radios, wireless LANs and modems, and Global Positioning Systems (GPS). Wireless LANs enable client computers and the server to communicate with one another without direct cable connections. Figure 1.8 and 1.9 shows the wireless network.

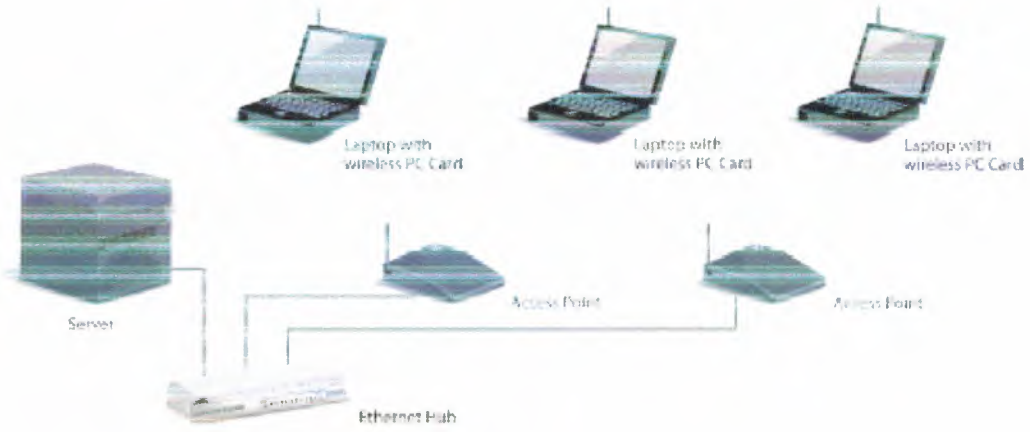

Figure 1.8 Wireless Networks

Figure 1.9 Wireless Peer-to-Peer Network

CHAPTER TWO

2. INTRODUCTION TO WIRELESS (LANs)

2.1 Overview

A wireless local area network (LAN) is a flexible data communications system implemented as an extension to or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

Wireless LANs have gained strong popularity in a number of vertical markets, including health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

There are two types of WLANs, infrastructure WLANs and independent WLANs. Infrastructure WLANs, where the wireless network is linked to a wired network, is more commonly deployed today. In an infrastructure WLAN, the wireless network is connected to a wired network such as Ethernet, via access points, which possesses both Ethernet links and antennas to send signals. These signals span microcells, or circular coverage areas (depending on walls and other physical obstructions), in which devices can communicate with the access points, and through these, with the wired network (*see picture below*). In a wireless LAN, devices can move within and between coverage areas without experiencing disruption in connectivity as long as they stay within range of an access point or extension point (similar to an access point) at all times

2.2 How Wireless LANs Work:

Wireless LANs use electromagnetic airwaves (radio or infrared) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. By superimposing the transmitted data onto the radio carrier, data can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies.

In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard cabling. At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet.

End users access the wireless LAN through wireless-LAN adapters, which are implemented as PC cards in notebook or palmtop computers, as cards in desktop computers, or integrated within hand-held computers. Wireless LAN adapters provide an interface between the client network operating system (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS.

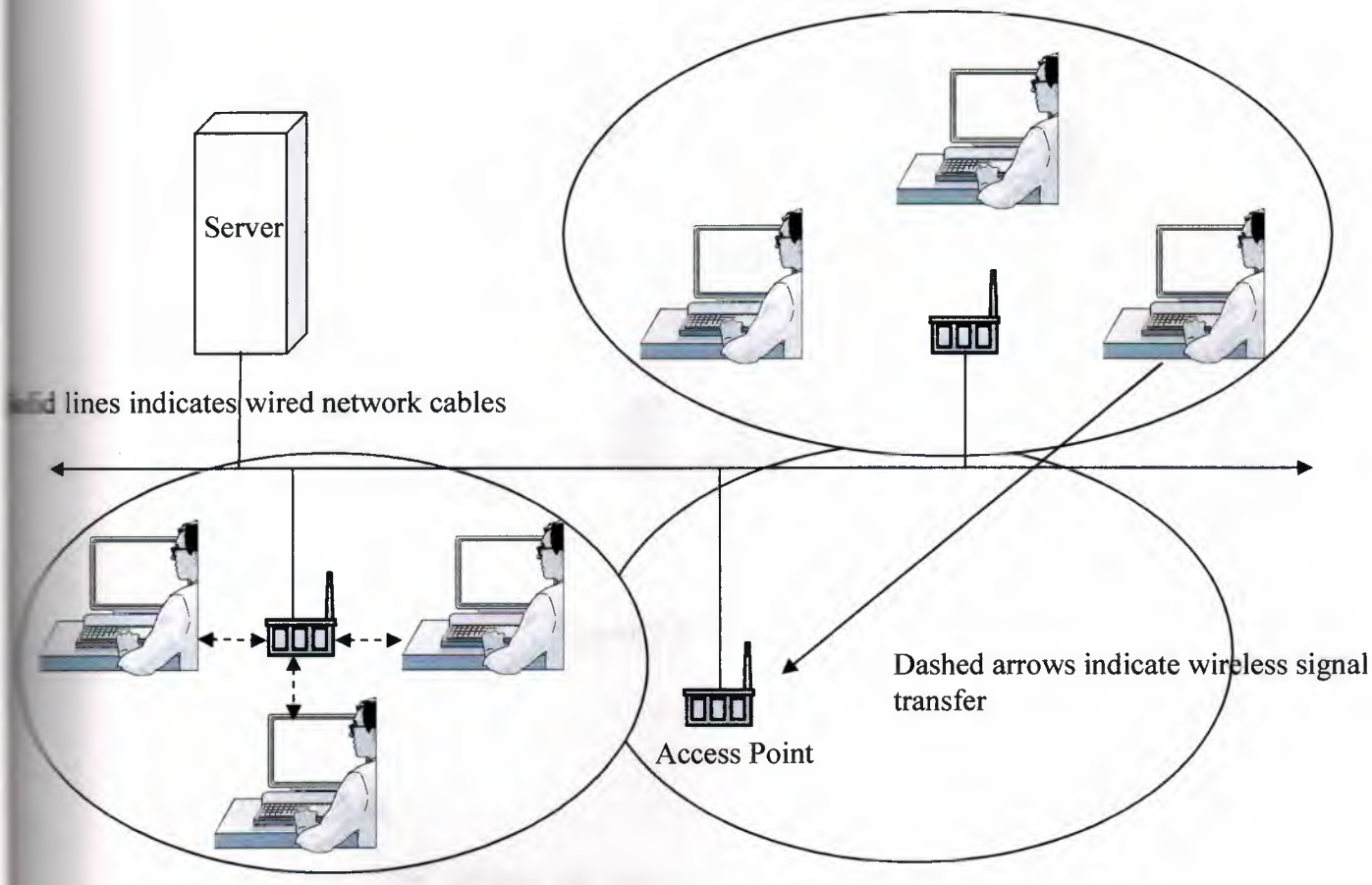

Figure 2.1 Wireless LAN Layouts

In an (infrastructure) wireless LAN, devices communicate wirelessly with access points, which are connected to the wired network. Devices can maintain network connectivity while roaming in the shaded region.

This model can be compared to those of wired LANs where devices connect via cables to hubs, or common wiring points, and from these to a central server. However, in wired networks, each hub has a finite number of jacks, and thus, can only connect a preset number of devices. Wire line networks are also confined by the existence of fixed cables, which limit connection to specified locations (seethe next picture).

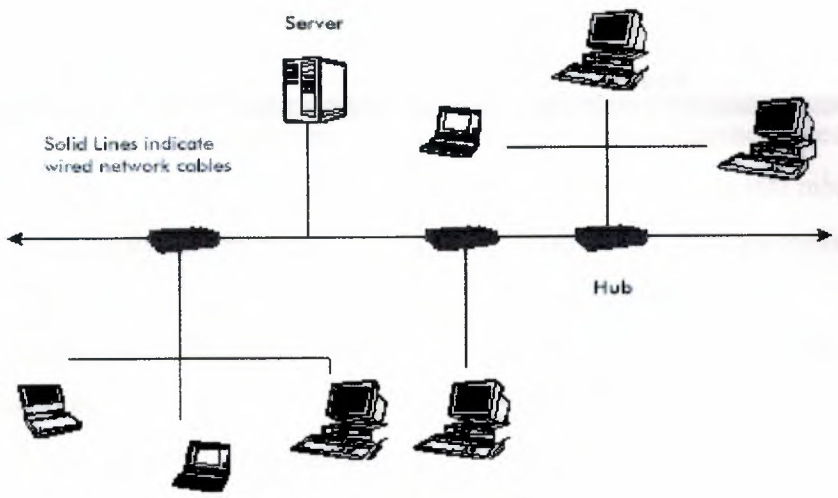

Figure 2.2 Wired LANs

2.2.1 Wired LANs

In a wired LAN, devices are connected to the network via cables. Devices are generally anchored to a set location depending on the placement of the network lines.

While WLANs provide some key benefits, including security, mobility, and scalability, they are currently much slower than wired LANs. For example, a wired LAN using 10BaseT Ethernet ranges from 10 - 100 Mbps. Other pros and cons of wireless LANs (in comparison with wired LANs) are listed in the table below:

Wireless LAN Pros and Cons

Pros	Cons
• Easier to deploy and configure • More secure • Ultimately more cost-effective (scalable) • Facilitates office relocation Easier to maintain • Makes available real-time data in broader range of coverage areas	• Slower — Ethernet speeds range from 10 mbps to 100 mbps; corporate networks require high bandwidths • Signal interference often causes disruptions in connection • Systems from different vendors may not be interoperable • Costly installation

2.3 Wireless LAN Glossary's

a. Access Point: a device that connects the wireless network to the wired network. As a transceiver, it sports an antenna to send and receive signals from the various devices, providing coverage areas in which devices can roam freely.

b. Extension Point: a device that acts like an access point and connects the wireless network. Unlike access points, extension points do not connect the wireless network to the wireline but rather extend coverage areas between and beyond access points.

c. Infrastructure Network: the more common form of a wireless LAN. Infrastructure networks are comprised of WLANs connected to wired LANs and contain access points to channel network traffic.

d. Independent Network: a peer-to-peer network containing devices (with network adapters) connected to one another, independent of a managing server or other form of administration.

e. LAN Adapter: generally a PC card in the portable device with an integrated antenna to receive signals from the access point/extension point. Can also be integrated into handhelds.

f. Microcell: a coverage area in which devices can roam freely with a wireless connection. Micro cells are generally circular (depending on the existence of interfering objects such as walls) and overlap to enable seamless connection as a user wanders through the wireless network. Spread spectrum-a radio frequency technology most commonly used in WLANs. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are two examples of the spread-spectrum technique. Transceiver-a device, such as a LAN adapter, used to receive signals sent by the transmitter. Transmitter-a device that sends signals to the transceiver (typically an access point or an extension point in WLANs).

2.4 Wireless LANs Advantages

The widespread reliance on networking in business and the rapid growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, convenience, and cost advantages over traditional wired networks:

- **Mobility**: Wireless LAN systems can provide LAN users with access to real-time information anywhere at work and in the home.
- **Installation Speed and Simplicity**: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- **Installation Flexibility**: Wireless technology allows the network to go where wire cannot go.
- **Reduced Cost-of-Ownership**: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- **Scalability**: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily

changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

2.5 How Wireless LANs Are Used in the Real World

Wireless LANs frequently augment rather than replace wired LAN networks—often providing the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.
- Students holding class on campus greens can access the Internet to consult the catalog of the Library of Congress or class notes.
- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- Training sites at corporations and students at universities use wireless connectivity to access information, information exchanges, and learning.
- Trade show and branch office workers minimize setup requirements by installing pre-configured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases, thereby increasing productivity.
- Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.

2.6 Wireless LAN Technology's

Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations.

2.6.1 Narrowband Technology

A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies.

A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, privacy and noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency.

From a customer standpoint, one drawback of narrowband technology is that the end-user must obtain an FCC license for each site where it is employed.

2.6.2 Spread Spectrum Technology

Most wireless LAN systems use spread-spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right

frequency, a spread-spectrum signal looks like background noise. There are two types of spread spectrum radio: frequency hopping and direct sequence.

2.6.3 Frequency-Hopping Spread Spectrum Technology

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

2.6.4 Direct-Sequence Spread Spectrum Technology

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, more bandwidth is required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected by most narrowband receivers.

2.6.5 Infrared Technology

A third technology, little used in commercial wireless LANs, is infrared. Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide limited range of approximately 3 feet and typically are used for personal area networks. Occasionally directed systems are used in specific wireless LAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks. Diffuse or reflective IR wireless LAN systems do not require line-of-sight, but cells are limited to individual rooms.

2.7 Wireless LAN Configuration

Wireless LANs can be simple or complex. At its most basic, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another. This is called a peer-to-peer network. On-demand networks, such as in this example, require no administration or preconfiguration. In this case each client would only have access to the resources of the other client and not to a central server.

Figure 2.3: A wireless peer-to-peer network

Installing an access point can extend the range of an ad hoc network, effectively doubling the range at which the devices can communicate. Since the access point is connected to the wired network, each client can have access to server resources as well as to other clients. Each access point can accommodate many clients; the specific number depends on the number and nature of the transmissions involved. Many real-world applications exist where a single access point services from 15-50 client devices.

Figure 2.4: Client and Access Point

Access points have a finite range, on the order of 500 feet indoor and 1000 feet outdoors. In a very large facility such as a warehouse, or on a college campus, it may be necessary to install more than one access point. Access point positioning is accomplished by means of a site survey. The goal is to blanket the coverage area with overlapping coverage cells so that clients can range throughout the area without ever losing network contact. The ability of clients to move seamlessly among a cluster of access points is called *roaming*. Access points hand the client off from one access point to another in a way that is invisible to the client, ensuring unbroken connectivity.

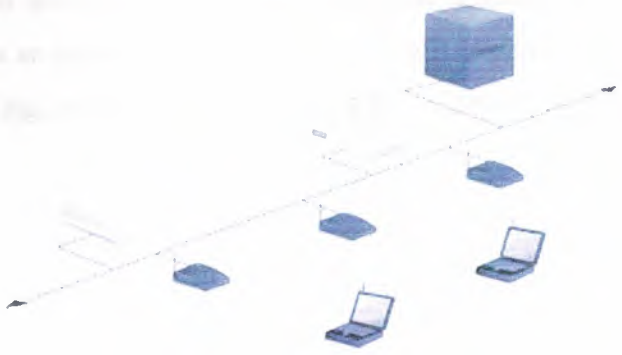

Figure 2.5: Multiple access points and roaming

To solve particular problems of topology, the network designer might choose to use Extension Points to augment the network of access points. Extension Points look and function like access points, but they are not tethered to the wired network as are APs. EPs function just as their name implies: they extend the range of the network by relaying signals from a client to an AP or another EP. EPs can be strung together in order to pass along messaging from an AP to far-flung clients (just as humans in a bucket brigade pass pails of water hand-to-hand from a water source to a fire).

Figure 2.6: Use of an Extension Point

One last item of wireless LAN equipment to consider is the directional antenna. Let's suppose you had a wireless LAN in your building A and wanted to extend it to a leased building, B, one mile away. One solution might be to install a directional antenna on each building with each antenna targeting the other. The antenna on A is connected to your wired network via an access point. The antenna on B is similarly connected to an access point in that building, which enables wireless LAN connectivity in that facility.

Figure 2.7: The use of Directional Antennas

2.8 Customer Consideration

While wireless LANs provide installation and configuration flexibility and the freedom inherent in network mobility, customers should be aware of the following factors when considering wireless LAN systems.

2.9 Range and coverage

The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Solid objects block infrared signals, which impose additional limitations. Most wireless LAN systems use RF because radio waves can penetrate most indoor walls and obstacles. The range (or radius of coverage) for typical wireless LAN systems varies from under 100 feet to more than 300 feet. Coverage can be extended and true freedom of mobility via roaming, provided through micro cells.

2.10 Throughput

As with wired LAN systems, actual throughput in wireless LANs is product- and set-up-dependent. Factors that affect throughput include the number of users, propagation factors such as range and multipath, the type of wireless LAN system used, as well as the latency and bottlenecks on the wired portions of the LAN. Data rates for the most widespread commercial wireless LANs are in the 1.6 Mbps range. Users of traditional Ethernet or Token Ring LANs generally experience little difference in performance when using a wireless LAN. Wireless LANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, Internet access, file transfer, and access to multi-user databases and applications.

As a point of comparison, state-of-the-art V.90 modems transmit and receive at data rates of less than the advertised 56.6 Kbps. In terms of throughput, a wireless LAN operating at 1.6 Mbps is (almost thirty times faster than the state-of-the-art V.90 modem)

2.11 Integrity and Reliability

Wireless data technologies have been proven reliable through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the home or workplace. Robust designs of proven wireless LAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

2.12 Compatibility with the Existing Network

Most wireless LANs provide for industry-standard interconnection with wired networks such as Ethernet or Token Ring. Wireless LAN nodes are supported by network operating systems in the same fashion as any other LAN node through the use of the appropriate drivers. Once installed, the network treats wireless nodes like any other network component.

2.13 Interoperability of Wireless Device

Wireless LAN systems from different vendors may not be interoperable. For three reasons. First, different technologies will not interoperate. A system based on spread spectrum frequency hopping (FHSS) technology will not communicate with another based on spread spectrum direct sequence (DSSS) technology. Second, systems using different frequency bands will not interoperate even if they both employ the same technology. Third, systems from different vendors may not interoperate even if they both employ the same technology and the same frequency band, due to differences in implementation by each vendor.

2.14 Interference and Coexistent

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a wireless LAN system. Microwave ovens are a potential concern, but most wireless LAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple wireless LANs. While wireless LANs from some manufacturers interfere with wireless LANs, others coexist without interference.

2.15 Licensing Issues

In the United States, the Federal Communications Commission (FCC) governs radio transmissions, including those employed in wireless LANs. Other nations have corresponding regulatory agencies. Wireless LANs are typically designed to operate in portions of the radio spectrum where the FCC does not require the end-user to purchase a license to use the airwaves. In the U.S. most wireless LANs broadcast over one of the ISM (Instrumentation, Scientific, and Medical) bands. These include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz. For wireless LANs to be sold in a particular country, the manufacturer of the wireless LAN must ensure its certification by the appropriate agency in that country.

2.16 Simplicity/Ease of Use

Users need little new information to take advantage of wireless LANs. Because the wireless nature of a wireless LAN is transparent to a user's network operating system, applications work the same as they do on wired LANs. Wireless LAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools.

Wireless LANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of wireless LANs require cabling, network managers are freed from pulling cables for wireless LAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on wireless LANs. Finally, the portable nature of wireless LANs lets network managers preconfigure and troubleshoot entire networks before installing them at remote locations. Once configured, wireless LANs can be moved from place to place with little or no modification.

2.17 Security

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

2.18 Cost

A wireless LAN implementation includes both infrastructure costs, for the wireless access points, and user costs, for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed. The number of access points typically depends on the required coverage region and/or the number and type of users to be serviced. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms.

The cost of installing and maintaining a wireless LAN generally is lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, a wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because wireless LANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead.

2.19 Scalability

The design of wireless networks can be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

2.20 Battery Life for Mobile Platforms

Since end-user wireless products are designed to run off the AC or battery power from their host notebook or hand-held computer, wireless products have no direct wire connectivity of their own.

2.21 Safety

The output power of wireless LAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to wireless LANs.

2.22 Summary

Flexibility and mobility make wireless LANs both effective extensions and attractive alternatives to wired networks. Wireless LANs provide all the functionality of wired LANs, without the physical constraints of the wire itself. Wireless LAN configurations range from simple peer-to-peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment, wireless LANs enable portable networks, allowing LANs to move with the workers that use them.

CHAPTER THREE

3. TYPES OF WIRELESS LANs

3.1 Overview

It might seem obvious that the key differentiating factor between wireless LANs and wireless WANs is that they operate in a local area, but local operation has many significant and not necessarily obvious consequences. First and foremost, wireless LANs operate at much higher speeds, ranging from 1 Mbps to 20 Mbps compared to wireless WANs, which today range from 4 Kbps to 30 Kbps. Higher speeds are possible because that band of the spectrum is shared by a much smaller number of users. Whereas a cellular base station can serve a radius of over 10 kilometers (six miles), a wireless LAN access point typically serves a maximum radius of about a hundred meters. Due to the shorter distances involved in wireless WANs, radio signals experience less interference and distortion from the environment, thus reducing the amount of error control required. Users are also stationary or moving at walking speeds, while wide area networks support users moving at highway speeds where signals are subject to a form of interference known as Rayleigh fading. Another factor is that smaller distances result in much better signal-to-noise ratios. All these factors in combination allow much higher throughputs.

The higher throughput of wireless LANs has the virtue of allowing you to use existing network operating systems and applications (e.g., file and printer sharing, database access) compared to the modem-like applications for wireless WANs. And unlike wireless WANs, which are mostly operated by public carriers with usage fees, you get to buy and operate your own network. This gives you control of the whole network, but leaves you responsible for its proper installation and functioning. Fortunately, wireless LAN technology is well past its infancy and is ready to meld into your

organization as a reliable subsystem. And the radio bands used by nearly all wireless LANs let you deploy networks without obtaining a license.

In this section, we delve into the different topologies available: spread spectrum, which is the most common RF technology used today (the two types of spread spectrum include direct sequence and frequency hopping); a low-power, narrowband approach that enables higher speeds; HiperLAN, which is a European standard; and infrared approaches.

3.2 Topologies

The term wireless is actually somewhat misleading, since most wireless LANs interconnect with wired networks. The bulk of the distance between a wireless node and another node may well be over wires or fiber. Nevertheless, it is possible to build a network that is completely wireless. In such an instance, the physical size of the network is determined by the maximum reliable propagation range of the radio signals. Networks such as these are referred to as ad hoc networks, and are well suited for temporary situations such as meetings, conferences and sporting events.

It is more likely that you will install what is called an infrastructure network, where your WLAN connects to an existing wired LAN. In this instance you will need an access point that effectively bridges wireless LAN traffic onto your LAN. This function may be handled by software in a workstation that houses both a wireless card and a wired (e.g., Ethernet) card. But most wireless LAN vendors recommend dedicated hardware called an access point for this function. The access point can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.

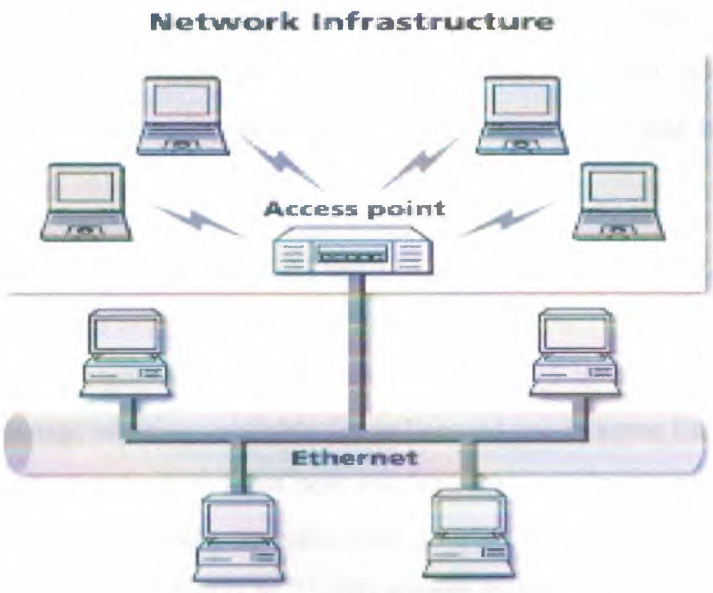

Figure 3.1: Network Infrastructure

3.3 Spread Spectrum

Most wireless LANs today use spread spectrum technology, not because spread spectrum is the best radio technology for wireless LANs but more as a result of FCC rules (Federal Code of Regulations 15.247) that allow for unlicensed operation in a number of radio bands, including 902 to 928 MHz, 2.400 to 2.483 GHz and 5.725 to 5.85 GHz. These are the industrial, scientific and medical (ISM) bands where unlicensed users are "secondary users" of the band and must not interfere with licensed primary users. Fortunately such interference has not been an issue because wireless nodes are restricted to 1 watt of power for transmissions and because the nature of spread spectrum is that it appears as noise to all but intended receivers.

Nevertheless, as a user of wireless LAN technology you need to be aware that primary users of the spectrum are not restricted to 1 W of transmission and could potentially interfere with your network. Moreover, companies are finding more an d more use for the ISM bands, including wireless speakers and cordless telephones. The

Metricom Ricochet network for instance, uses the 900-MHz ISM band. Will you experience interference problems using spread spectrum? Probably not, but you may want to think twice before using wireless LANs for mission-critical or life-and-death applications.

In today's market, the 900-MHz ISM band best serves consumer products, while the 2.4-GHz band best serves midrange performing wireless LANs (1 to 3 Mbps) and the 5.7-GHz band best serves higher-performance wireless LANs (5 to 10 Mbps). The 2.4-GHz band has the advantage of being available for unlicensed use in some European countries and Japan, and is the band where most new wireless LAN products operate today. As to coverage, spread spectrum usually operates over a typical range of about 100 meters and coverage areas ranging from 5,000 to 25,000 square meters (50,000 to 250,000 square feet).

Spread spectrum was developed by the U.S. military as a robust radio technology that is both difficult to jam and to eavesdrop on. It works by spreading a signal that would normally occupy a certain amount of spectrum over a much broader amount of spectrum. There are two forms of spread spectrum: frequency hopping and direct sequence. Both are allowed by FCC rules.

In frequency hopping, the signal dwells momentarily on one frequency, then hops to another, then another in a pseudorandom sequence that eventually repeats itself. A receiver must hop at exactly the same time to exactly the right frequency to be able to receive the signal. FCC rules require that the band be divided into a certain number of frequencies and that the hopper must use a certain number of these frequencies.

Direct sequence is very different. Each "one" in the binary data is converted to a sequence of predetermined ones and zeroes and each "zero" is converted to the inverted sequence. The binary data in the sequences are referred to as chips, and the ratio of chips to original bits is referred to as the spreading ratio, or gain, of the system. FCC rules require a minimum spreading ratio or gain.

Some wireless LANs are based on frequency hopping, some on direct sequence. Direct sequence allows higher throughputs, although such designs may cost more and use more power. There is almost a holy war about which type of spread spectrum is better, though mobile designs today tend to use frequency hopping. You should choose your network based on features and price, and not on which spread spectrum technology it uses.

3.4 Low-Power Narrowband

An alternative approach to spread spectrum that some wireless LAN vendors are using is to transmit narrowband signals at low-power levels, a method allowed by FCC CFR 15.249 rules. By transmitting at low-power levels, vendors do not have to use spread spectrum, which gives them the ability operate at higher data rates. RadioLAN's product uses this approach and operates at 10 Mbps in the 5.8-GHz band with 50 mill watts (mW) of peak transmission power. The price of this higher performance is a reduced transmission range of about 30 meters (100 feet) in an office environment.

3.5 HiperLAN

HiperLAN, an abbreviation for Higher Performance Radio LAN, is a wireless technology standard developed by the European Telecommunications Standards Institute. It boasts very impressive capabilities, including a data rate of about 24 Mbps using a channel width of 23.5 MHz. In Europe, spectrum is available in the 5.15 to 5.3 GHz range, allowing for five separate channels. This type of throughput readily supports multimedia applications. Unfortunately, no commercial products are yet available. But the technology is under consideration for new spectrum in the United States in the 5-GHz band as part of the U.S. Unlicensed National Information Infrastructure band.

3.6 Infrared LANs

An alternative approach to radio-based wireless L ANs is infrared communications. Infrared networking uses electromagnetic radiation with wavelengths of 820 to 890 nanometers, corresponding to a frequency of about 350,000 GHz. The advantages of IR include no need for licenses, no safety issues, huge potential capacity and good control of interference. IR does not penetrate walls, so infrared LANs must be contained in a room. Note that IR LANs generally do not operate in outdoor areas where there is sunlight. IR transmitters and receivers can be designed either for directional use or for diffuse use, where signals bounce off walls and other objects to reach the receiver. In fact, IR is specified as one of the physical layer options in the new IEEE 802.11 standard.

Though it is a promising technology, there are relatively few IR LAN products available today. But one type of infrared technology that has been broadly deployed is the use of IR for short point-to-point connections following standards specified by the Infrared Data Association.

3.7 Infrared Data Association (IRDA)

The Infrared Data Association is a consortium of vendors that has defined low-cost IR communications characterized by:

- Directional point-to-point communications of up to one meter
- 115-Kbps and 4-Mbps connectivity
- Walk-up ad hoc connectivity for LAN access, printer access, and portable computer to portable computer communications

Many laptops today include IRDA ports, though devices such as LAN access points and printers with IR capability are not yet very common. The IRDA estimates some 60 million IRDA ports in the market.

3.8 Unlicensed PCS

When allocating spectrums for Personal Communications Service, the FCC included some bands for what is called unlicensed PCS: 1910 to 1920 MHz and 2390 to 2400 MHz were reserved for data and 1920 to 1930 MHz for voice. Unfortunately, restrictions on the use of this spectrum have limited its usefulness for wireless data to the extent that no product offerings are yet available.

CHAPTER FOUR

4. WLANs TECHNOLOGY & IMPLEMENTATIONS

4.1 Overview

Local Area Networks have evolved over the past 20 or so years to become a crucial ingredient in the success of businesses, large and small. From the smallest office to the largest multinational corporation shared access to information resources is an indispensable part of modern business processes. Local Area Networks (LAN) have been traditionally connected with wired infrastructure and a multi-billion dollar industry has grown up to supply customer's needs for wired networking products. Companies like Cisco, 3Com; Bay Networks and Cabletron have developed a vast range of products to implement and manage Local Area Networks of all sizes and to interconnect them throughout the enterprise.

Over the past ten or so years an alternative to wired LAN structures has evolved in the form of the Wireless LAN (WLAN). In a manner analogous to the growth of the wired LAN, initial application and market success of the WLAN was in specialized, vertical markets. Thus applications that highly valued the mobile, untethered connectivity were the early targets of the WLAN industry. These first generation products, which operated in the unlicensed 902-928 MHz ISM (Industrial Scientific and Medical) band had limited range and throughput, but proved useful in many factory floor and warehouse applications. These systems took advantage of emerging semiconductor processes developed for cellular telephone applications to enable inexpensive WLAN products. Unfortunately these same inexpensive components also enabled a wide variety of other 900 MHz products like cordless telephones. Consequently, the band quickly became crowded with a variety of unlicensed products. Building upon technology originally developed for military applications, spread spectrum techniques were employed to

minimize sensitivity to interference. This approach allowed the design and manufacture of 900 MHz WLAN products having nominal data rates of 500 kilobits per second. Ultimately, the growing popularity of the band for a large range of unlicensed products, aggravated by the limited bandwidth caused users of WLAN to look to a different frequency band for growth in performance.

The second generation of WLAN products evolved in the 2.40-2.483 GHz ISM band. Again enabled by semiconductor advances, this time from the PCS market, products were developed by a number of manufacturers for this band, again generally for specialized vertical markets. Because a major user of the 2.4 GHz ISM band is microwave ovens, a transmission scheme less sensitive to this type of noise source needs to be used. Extending the experience from the crowded 900 MHz band, spread spectrum techniques combined with more available bandwidth and more complex modulation schemes allowed second generation 2.4 GHz band products to operate at data rates of up to 2.0 megabits per second. Third generation WLAN products are evolving to more complex modulation formats in the 2.4 GHz band to allow nominal 11 megabit per second raw data rate and about 7 megabit per second throughput even as the decreasing cost of 2.4 GHz semiconductor technology allows for ever more use of this band. In the third and fourth quarters of 1998, the first 2.4 GHz cordless telephones became available as did several new consumers electronic PC interconnection products. The history of the 900 MHz band WLAN seems poised to repeat itself as the 2.4 GHz band becomes a victim of its own success.

The fourth generation of WLAN technology, offering users data rates of 10 megabits per second and up, is beginning. Again evolving from advances in semiconductor technology, fourth generation devices are operating at a new, higher frequency the 5 GHz band. The first of these fourth generation products has been available from Radio LAN Inc since late 1996. The initial products operate in the 5.775-5.850 GHz ISM band, and additional bandwidth around 5.2 GHz has also been made available. Unlike the lower frequency bands used in prior generations of WLAN products, the 5 GHz bands do not have a large indigenous population of potential interferors like microwave ovens or

industrial heating systems as was true at 900 Mhz and 2.4 GHz. In addition there is a much more bandwidth available at 5 GHzó 350 Mhz compared with 83 Mhz at 2.4 GHz and 26 Mhz at 900 MHz. This combination of greater available bandwidth and reduced sources of interference make the 5 GHz bands an ideal region in which WLAN products having performance comparable to that achieved by wired networks are being created.

A Wireless LAN can enhance the value of installed wired networks in large corporations by offering untethered mobility and reduce the total costs of network ownership in small companies by easy reconfiguration with growth and change. In the sections below, a brief review of data networks will be presented. This will be followed by a section on the various technology issues surrounding WLAN and finally by a discussion of the different standards relating to WLAN.

4.2 Network Structures

To provide a basis for the further discussions of the technology and standards issues related to WLAN, a brief review of network structures is in order. The first concept to keep in mind is that networks represent an interactive collection of often powerful computers. The complexities of the interactions among these members of the network are many. To provide a common framework for describing and understanding, the International Standards Organization approved a standard called ISO-7498 that defines a seven-layered model to describe the interconnection processes between various members of a network.

This model, which is officially known at the Open System Interconnect model, is the basis for most discussions of network function. The seven layers are shown in Figure 4.1. WLAN products, in common with other networking products, typically work at the two bottoms most layers of the 7-layered model. The Physical Layer (usually referred to as simply PHY) is the actual physical method by which data is passed from one member of the network to another. For a WLAN its description includes such things as frequency of

operation, data rate, modulation method, etc. In addition to the PHY, the lower half of the Data Link layer, usually known as the Media Access Control (or MAC) layer is defined by the WLAN product. The MAC layer is conventionally defined as the protocol by which data is transferred between network members. In Figure 4.1, the shaded areas represent the PHY and MAC layers. These layers and their important features will be discussed in the Technology section that follows.

Wireless networks are implemented with two basic types of components: a Network Adapter which is the electronic interface between the client

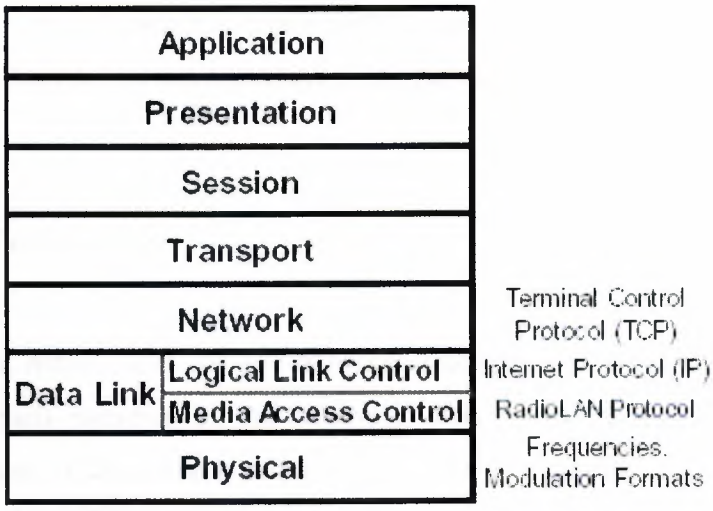

Figure 4.1: Open System Interconnect Model

Computer (these days often a notebook PC) and the wireless network and an Access Point which provides the bridge between the wireless network and a wired network. A wireless network can consist solely of Network Adapters connecting members of a completely wireless network, or a combined network in which wired and wireless connectivity is employed. Because a client, wireless-networked computer could appear as a member of any number of potential networks due only to the clientís own mobility, the topology of the network in which the new client appeared is altered by the additional member as is the network geometry.

Although there are two basic types of wireless network components, the wide variety of possible client computer platforms require many variations. Within the IBM-PC compatible environment, the network adapter could be required to work with the ISA or PCI bus structures as well as the PCMCIA interface. Extending beyond the IBM-PC are other personal computers like the Apple Macintosh family, the evolving set of handheld or smaller format machines running the Windows CE operating system, and a wide range of workstation class machines. Each of these families of platform requires not only possibly unique hardware interfaces, but also unique driver software which works at the Transport layer in the OSI model. For Access Point products there is the requirement to interface with any of several possible wired LAN types and also be transparent to whatever higher layer software is in use elsewhere in the network.

4.3 Wireless LAN Technology

The most important requirement for any network structure is to provide adequate levels of service to each member of the network. This service requirement has dimensions of both access to the network and bandwidth on the network. As new users are added to the network, additional network capacity must be added to provide both convenient network access and the desired bandwidth. The methods of adding capacity are well known, and have been long employed by network managers. In a wireless network, additional capacity can be provided by a number of methods depending upon the WLAN technology employed. The options available for increasing capacity are functions of fundamental considerations made in the design of the MAC and PHY layers of the particular wireless network.

4.4 Wireless LAN PHY Implementations

Historically WLAN PHY layers have been designed around a combination of low cost semiconductor technology and available spectrum. To simplify the use of WLAN, frequencies have been conventionally chosen from the unlicensed ISM bands. Although the general rules for these bands are that everyone is free to use them and must accept the interference from other users, national regulatory bodies, like the Federal Communication Commission in the US, have set general standards governing types of modulation and maximum permissible power levels. Similarly in Europe the European Telecommunication Standards Institute has set guidelines for member of the European Union. Elsewhere, other governments have adopted the FCC or ETSI regulations to meet their local needs. In general, the 900 MHz band does not have sufficient bandwidth to allow usefully large networks with sufficient data rates to support most current networking requirements. At 2.4 GHz the FCC has allocated 83.5 MHz of bandwidth to WLAN applications. To operate successfully in competition with other interfering users in this band, WLAN are implemented using spread spectrum technology. Spread spectrum systems utilize two different techniques to spread the required bandwidth over a larger range of frequencies than would be necessary to simply transmit the data.

In a Frequency Hopping Spread Spectrum (FHSS) system, the data is modulated on to the carrier in a manner identical to that employed for standard narrow band communications. Most frequency hopping systems employ Gaussian Frequency Shift Keyed modulation, either two or four level. The carrier frequency is then changed (ìhoppedî) to a new frequency in accordance with a pre-determined hopping sequence. If the receiver frequency is then hopped in synchronism with the transmitter, data is transferred in the same manner as if the transmitter and receiver were each tuned to a single fixed frequency. If different transmitter-receiver pairs hop throughout the same band of frequencies, but using different hopping sequences, then multiple users can share the same frequency band on a non-interfering basis. The operation of a pair of frequency hopping transmitter-receiver pairs is shown schematically in Figure 4.2. The obvious

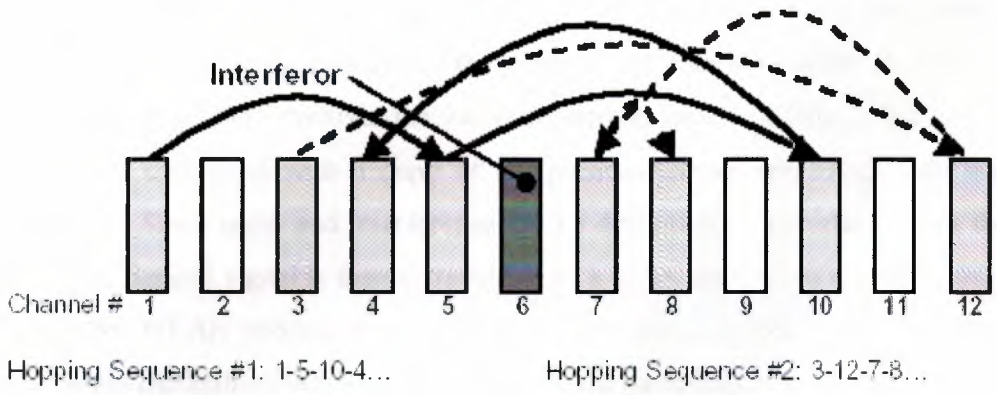

Figure 4.2: Frequency Hopping Spread Spectrum

Lies in how a FHSS responds to interferers. If a particular hop channel is noisy due to a fixed frequency source (e.g. a microwave oven), then information transferred in that particular channel can be lost. The system then hops to the next frequency, which is hopefully not occupied by an interferor, and information transfer continues. As will be discussed below, the communication protocol employed in the design of the system can offer means of further reducing the impact of a noisy channel. In the 2.4 GHz band, there are 79 1.0 MHz wide channels assigned, and a total of 78 different hopping sequences. In theory, all 78 hop sequences could be shared on a non-interfering basis, but statistically only about 15-20 (depending on individual user data traffic patterns) can be used. Thus a network manager could assign 15 different hopping sequences in the same physical area with minimal interference. This has the effect of multiplying the total available bandwidth by 15 times although each individual user would only experience a 2 Megabit per second maximum data rate.

The second type of spread spectrum is known as Direct Sequence Spread Spectrum (DSSS). In this system, the data stream is multiplied by a pseudo-random spreading code to artificially increase the bandwidth over which the data is transmitted. This is shown in Figure 4.3. The resulting data stream is then modulated onto the carrier using either Differential Binary Phase Shift Keying or Differential Quadrature Phase Shift Keying. By

spreading the data bandwidth over a much wider frequency band, the power spectral density of the signal is reduced by the ratio of the data bandwidth to the total spread bandwidth. In a DSSS receiver the incoming spread spectrum data is fed to a correlator where it is correlated with a copy of the pseudo-random spreading code used at the transmitter. Since noise and interference are by definition de-correlated from the desired signal, the desired signal is then extracted from a noisy channel. While the block diagram of a DSSS WLAN product is somewhat simpler than a FHSS product, there are some very subtle difficulties that come into play in the presence of strong interfering signals. The basis of the noise immunity of a DSSS system is the fact that the desired signal and interference or noise is uncorrelated. In complex interference environments which are becoming more common as usage increases, particularly ones in which very strong signals maybe present, non-linearities in the receiver generate intermodulation distortion products between the desired signal and the interfering signals.

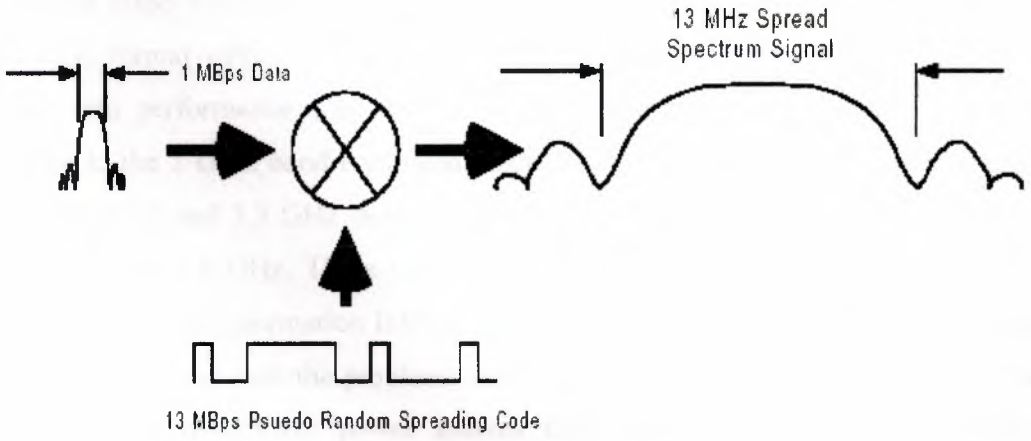

Figure 4.3: Direct Sequence Spread Spectrum

These IM products are now correlated with the desired signal thus reducing the resulting signal to noise ratio when processed in the receiver. The usual implementation of DSSS in the 2.4 GHz band employs a 13 MHz wide channel to carry a 1 MHz signal. Channels are centered at 5 MHz spacing, giving significant overlap. Within the designated 2.400 to 2.483 GHz band there are eleven available channels for users in the US. In a practical

network, there are typically three non-overlapping channels that can be utilized in deploying a network. In an analogous manner to that described for FHSS, the total bandwidth in a physical region could effectively be multiplied by a factor of three for DSSS networks, although each user would again only experience 2 Megabit per second throughput.

In the 5 GHZ bands the PHY related issues become much simpler: there are fewer interferers and more bandwidth is available. Consequently, WLAN system designers have more options available to provide higher performance, lower cost networks. At present, there is only one 5 GHz WLAN manufacturer, Radio LAN Inc., but over the next one to two years, the ten or so manufacturers of lower frequency WLAN products may also announce 5 GHz products. Because of the advantages afforded by operation at 5 GHz, the Radio LAN product is able to offer 10 megabit per second performance at a price less than two megabit, 2.4 GHz products. This is accomplished by means of a Differential Pulse Position Modulation waveform that is elegant in its simplicity. This modulation format offers a number of advantages to WLAN system designers that translate into performance superior to systems operating at 2.4 GHz. An important advantage to the 5 GHZ band compared to the lower frequency bands is the creation of bandwidth at 5.2 and 5.3 GHz dedicated exclusively to data transmission in addition to the ISM band at 5.8 GHz. These three segments have been designated by the FCC as Unlicensed-National Information Infrastructure (U-NII) bands exclusively for high speed data transmission. As such the problems associated with either microwave ovens or high power industrial microwave power sources that exist at the lower bands have no relevance at 5 GHz. Further, the lack of interference in the 5 GHz bands frees WLAN designers to optimize system design in terms of data rate, energy efficiency, cost and other parameters of greater value to the WLAN user, rather than focusing design efforts on coexisting with high power interferes.

4.5 Wireless LAN MAC Implementations

WLAN MAC implementations try to follow the general intent of the Ethernet standard in terms of channel sharing. Ethernet uses a Carrier Sense Multiple Access/Collision Detection protocol to arbitrate attempted simultaneous channel usage. Thus if multiple users try to communicate at the same time, a collision is detected causing each user to wait a randomly chosen interval and then attempt transmission again. In wireless environments it is not feasible to detect collisions, so a collision Avoidance protocol is employed. In this protocol, a listen before send procedure is established each user listens to determine if the channel is in use before attempting to transmit data. If the channel is already in use by another network member, the user attempting to send data stops and, as in Ethernet, waits a randomly chosen time and then attempts the transmission again. This protocol fairly assigns channel capacity among all users and also affords a measure of interference protection. In the circuit implementation of the Collision Avoidance protocol, the receiver simply listens for the presence of a signal level, rather than actually trying to process the signal to determine its possible data content. Thus any signal level, above some preset threshold causes the user to stop and wait before transmission. The impact of this protocol on channel throughput is well behaved with performance degrading in a graceful fashion with traffic density. In the case of interference from some signal not obeying the Collision Avoidance protocol, the impact can be quite severe. Of particular importance at 2.4 GHz is the potential interference from microwave ovens.

Although most, if not all, WLAN MAC protocols start from the general precepts of the Ethernet, there are special implications in WLAN structures (like the Collision Avoidance vs. Collision Detection concept discussed above) that require some variations from the usual Ethernet features. For instance, in a wired network, there is no need for a roaming function, typical of laptop users, in which a user can move in and out of contact with other members of the network. In a wired network a user is either connected to the network at a particular location or not; it is not possible that the user might be able to move from one portion of the network to another. Several different MAC protocols have

been developed by different WLAN manufacturers, and while all are generally similar there is an important distinction in the extent to which they replicate the Ethernet functions. Since the overwhelming majority of corporate networks are built around Ethernet connectivity, it is highly important that any wireless overlay to the network support all the Ethernet functions expected by the network operating system.

This is even more important with high data rate networks since they offer the possibility of operating small to mid-sized networks in a totally wireless fashion. Several of the more widely used 2 megabit data rate WLAN MAC require the presence of an Access Point to perform the bridging function between the wireless protocol and the Ethernet. Thus, if a network is set up having only wireless members (the so called a d h o c mode) and no Access Point, there may not be support for all the Ethernet functions required by application software. This possibility does not exist in products like the Radio LAN WLAN product family that have been designed for total Ethernet compatibility.

4.6 Summary

The past decade has seen the emergence of wireless local area networks as A valuable adjunct to the wired LAN. Wireless LAN technology has evolved from low data rate, interference-prone products at 900 MHz and 2.4 GHz to RadioLANís fourth generation 5 GHz systems giving wired network data rates. In enterprises with a large installed wired network infrastructure, a wireless LAN overlay can heighten the value of the network to mobile, laptop PC equipped users. In a small business that is faced with frequent modifications to its LAN infrastructure, a wireless LAN offers a lower total cost of ownership through easy reconfigurability.

The technology for implementation of wireless LAN has evolved over the past decade driven by continued gains in semiconductor performance. The need to simplify installation has led to operation in the unlicensed Industrial-Scientific-Medical bands.

Both the 900 MHz and 2.4 GHz bands have been utilized for wireless LAN applications. The requirement of operating in competition with a number of interfering users like microwave ovens and other high power industrial applications has forced the adoption of spread spectrum technology. Unfortunately, even the most complex spread spectrum modulation schemes can not prevent performance degradation in the face of the increasing number of users at 2.4 GHz. The solution to this problem, which will eventually be adopted by other WLAN vendors, is to operate in the 5 GHz bands. A 5 GHz solution offers greater available bandwidth and freedom from much of the interference that exists in the lower bands.

Since the Radio LAN MAC protocol is based upon a wireless implementation of 802.3, long-term protection of a large investment in existing network software and the applications that run on the network is assured. To guarantee that network performance will not degrade over time, the best option is to choose a network solution that does not operate in a band shared with potential interferes like microwave ovens and cordless telephones. The selection of a 5 GHz WLAN offers the best alternative to the increasingly crowded 2.4 GHz band. Radio LAN offers the only 5 GHz solution available today.

NEAR EAST UNIVERSITY
LIBRARY
1988 - LEFKOŞA

CHAPTER FIVE

5. WIRELESS LAN STANDARDS

5.1 Overview

The topic of standards and their relevance to WLAN products is the subject of near endless discussion among the proponents of the many products and standards in the WLAN market. In the material that follows an attempt will be made to put in perspective the issue of standards, their function, the mechanism by which they are created and their importance to users of WLAN.

5.2 Why are Standards Needed?

What we know today as standards first evolved late in the Industrial Revolution. To enable suppliers to provide components for much of the new industrial machinery being developed, interchangeability of items like fasteners was required. Industry leaders agreed among themselves on a set of relevant specifications for items like nuts and bolts and suppliers then produced to them to those specifications. Thus suppliers are guaranteed multiple markets for the same product and customers are given the option of procuring interchangeable products from multiple sources. Ideally, a standard should allow interoperability among products from different manufacturers, or if that is impossible at least allow non-interfering coexistence among equipment from a mix of suppliers. If either of these two criteria is satisfied, then the customer's investment is protected because it would be possible to purchase products from multiple vendors offering the same or similar performance.

The heart of the standard setting process is the assumption of stability over time of the specifications that the standard is trying to control. In a technology as rapidly evolving as WLAN, standards are made obsolete soon after they are approved. In response, those setting standards often attempt to lead the technology or devise standards that have room for growth. This process often leaves the user faced with the uncomfortable option of adopting a new technology solution for which a standard does not yet exist in order to gain the advantage offered by the new technology. If a sufficient number of users adopt the newer technology then a d e f a c t o standard can be created. The d e f a c t o standard can then often be adopted by standards setting bodies. Examples of this are many in the quickly changing data communication world one of the better known examples is the adoption of the10Base-T Ethernet standard.

5.3 Who Sets Standards and How?

Standards for data communication networks are set by three different classes of organizations: government regulatory bodies who are given statutory authority to manage the aspects of communications impacting the general public; national or international standards organizations who maintain the large body of standards covering many other topics besides simply data communication; and voluntary groups of industry members who agree on a standard among themselves.

In the WLAN industry the governmental agency that has oversight of issues such as frequency allocation, output power levels, etc. is the Federal Communications Commission in the US and its counterparts in other countries. The US, in common with most other nations, is a member of the International Telecommunications Union that attempts to harmonize issues like frequency allocations among its members. This allows some degree of commonality of frequency usage in different countries. The regulatory trend in the US, as well as in other ITU member states, has been to open new frequency bands to facilitate new wireless communication services. For example, the US in 1997

statutorily mandated creation of new frequency bands in the 5 GHz region for the Unlicensed-National Information Infrastructure (U-NII). Other countries are currently studying the feasibility of allocating similar frequencies. In addition to the governmental Standards allocating frequency bands and usage, governmental regulations also cover the unintended emissions from electronic equipment. These regulations ensure that out-of-band emissions do not interfere with other equipment.

The primary standards body creating and maintaining standards for the data networking industry is the Institute of Electrical and Electronic Engineers. Within the IEEE standards structure, data networking standards fall under the general category 802. Thus, all IEEE data networking standards have a general category of 802, followed by another designator signifying the specific topic. In this context, 802.1 covers certain aspects of network organization, 802.3 is the IEEE standard for the Ethernet, 802.11 covers WLAN and there are many others. In addition to the IEEE there are other organizations setting standards relating to WLAN. The European Telecommunications Standards Institute (ETSI) is engaged in creating standards to cover a high speed WLAN service called Hiperlan. Within other nations, the national telecommunications authority has taken some level of control over WLAN standards. For instance, in Japan local regulations require the periodic transmission of the individual WLAN transmitterís call sign, thus requiring changes in both the MAC and PHY layers of the WLAN products for the Japanese market.

A third category of standard setting organization is the industry consortium. In this structure a group of industry members agree among themselves on a set of common specifications for their products. These specifications are then published by the consortium as a standard for use by anyone wishing to make products in that category. There are several examples of this structure; one of the better known ones is Personal Computer Memory Card Interface Association or PCMCIA. Originally set up to coordinate standards for laptop computer plug-in memory cards, the PCMCIA standard now defines the interface specification for a wide range of portable computer accessories. In the WLAN area there are two significant consortia defining standards for next

generation WLAN. The first group is the HomeRF Working Group. The HomeRF Working Group was created in late 1997 to provide a set of standards for wireless consumer electronics products. The Bluetooth Special Interest Group was created by the major cellular telephone companies to provide a replacement for the cable connection between mobile PC platforms and cellular telephones. These two groups are similar in that they have goals of creating standards for very specific set of applications, not the more general specifications envisioned by the IEEE standards.

In addition to understanding the various organizations that create standards, it is also important to understand how the standards are created. Standards set by governmental organizations generally follow the process used by the FCC. The legislative branch grants statutory authority in the form of general guidelines. The FCC then formulates proposed regulations and public comments are solicited. Following the period of public comments, the FCC formally issues the new regulations often reflecting the input from the public comments. In the case of the IEEE standards, a committee is formed from industry and academic interests and the specifications for the standard are drafted. Because of the breadth of the standards addressed by organization like the IEEE, the deliberations are often lengthy the 2 megabit 802.11 deliberations took seven years. The final decision on the standard is reached by vote of the committee members. The voting rules within the IEEE committees vary somewhat, within the 802.11 committee voting membership is granted to anyone attending three consecutive meetings. The venue of each meeting changes to locations around the world to accommodate the global membership of the committee. Individual companies can send as many representatives as they wish, so the voting process tends to favor large companies who can afford to send numbers of representatives to consecutive meetings. Because, industry consortia are generally more focused around the goal of the standard being created, the voting process is usually on a one-company-one vote basis. Again because the goals of the standard process are tightly focused, the standards setting process proceeds rapidly to conclusion.

5.4 Are There Standards Truly Relevant to the Wireless LAN User?

From the preceding sections it is clear that there are a number of standards from a number of sources that impact the WLAN market and the user's choice of WLAN products. The question arises as to which standards are of importance in the selection of a WLAN product. At the highest level, compliance to the requirements of the governmental regulatory agencies is a legal requirement for the sale and use of a WLAN product. In common with its competitors, Radio LAN products are fully compliant with all the unintended emissions requirement of Part 15 of the Code of Federal Regulations. Radio LAN has the only products available at the present time approved under the new U-NII sections of Part 15.407. In the European Union, ETSI I-ETS 300 440 governs operation of Low Power Devices, Radio LAN products have been accepted as compliant with this standard.

Reflecting back to the original intent of the standards setting process, interoperability and interchangeability among products from different vendors, it would seem that the IEEE 802.11 WLAN standard is the most relevant standard. Unfortunately, the 802.11 standard offers three different PHY implementations: Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum and Infrared. Since the FHSS, DSSS and Infrared systems are fundamentally incompatible, the three classes of 802.11 compliant products cannot interoperate. Extreme generality was built into the 802.11 standard because of the requirement of handling a wide variety of potential applications visualized by the standards creators. This generality has made it very difficult for manufacturers of 2.4 GHz WLAN product to configure products to demonstrate interoperability. Interoperability trials for FHSS 802.11 products have been held on a regular basis at the Wireless Interoperability Laboratory at the University of New Hampshire since late in 1997. While minimal interoperability in the sense of ability to transfer data packets from one vendors product to another's has been demonstrated, the ability to seamlessly construct a network with products from multiple vendors has proven elusive. The DSSS vendors have fared only slightly better. With time and maturity of products the goal of

true interchangeability may be reached for 2.4 GHz products, but that time is not yet at hand. Further, there seems no urgency among the 2.4 GHz vendors that their products interoperate.

If the existing WLAN standards cannot guarantee interoperability among products from various vendors, can products from different standards coexist in the same bands? Again the answer is no. The presence of a FHSS 802.11 network operating in the vicinity of a DSSS network will degrade the performance of the DSSS network. [1] The emerging HomeRF 2.4 GHz standard will interfere with an 802.11 FHSS network. Bluetooth products are now thought to be especially disruptive to DSSS products, in particular to the new generation of 802.11 High Data Rate 2.4 GHz DSSS products. Recently published simulations indicate that a busy Bluetooth network co-located with an 802.11 High Data Rate network will reduce the throughput of the 802.11 network by about 45% under the most optimistic assumptions. [2] There are also several proprietary FHSS WLAN products currently operating in the 2.4 GHz band which can interfere with other FHSS products as well as DSSS systems. However serious the problem is today, the increasing utilization of the 2.4 GHz band will only increase the severity of the problem.

If the current 802.11 WLAN standard cannot offer the degree of interoperability that will allow WLAN users to mix and match equipment from different vendors or ensure coexistence with other similar WLAN products, how does the WLAN customer select a WLAN solution that will protect the value of the investment? First by making sure that chosen WLAN product fully supports all the networking standards to make the wireless network fully compatible with the wired network to which it may be attached. These standards include 802.3, the Ethernet standard and 802.1d (spanning tree) and the new extensions to 802.1 (802.1p and 802.1q) that will support IP-based priority queuing and IP-based Virtual LAN.

5.5 Some Wireless LAN standards

A short gallery of the most famous Wireless LAN standard (but unfortunately not necessarily the most widespread...).

5.5.1 IEEE 802.11

The main problem of radio networks acceptance in the market place is that there is not one unique standard like Ethernet with a guaranteed compatibility between all devices, but many proprietary standards pushed by each independent vendor and incompatible between themselves. Because corporate customers require an established unique standard, most of the vendors have joined the IEEE in a effort to create a standard for radio LANs. This is IEEE 802.11 (like *Ethernet* is *IEEE 802.3*, *Token Ring* is *IEEE 802.5* and *100vg* is *IEEE 802.12*).

Of course, once in the 802.11 committee, each vendor has pushed its own technologies and specificities in the standard to try to make the standard closer to its product. The result is a standard which took far too much time to complete, which is overcomplicated and bloated with features, and might be obsoletes before products come to market by newer technologies. But it is a standard based on experience, versatile and well designed and including all of the optimizations and clever techniques developed by the different vendors.

The 802.11 standard specifies one MAC protocol and 3 physical layers : Frequency Hopping 1 Mb/s (only), Direct Sequence 1 and 2 Mb/s and diffuse infrared (can we really call it a "standard" when in includes 3 incompatible physical layers ?). Since then, it has been extended to support 2 Mb/s for Frequency Hopping and 5.5 and 11 Mb/s for Direct Sequence (802.11b). The MAC has two main standards of operation, a distributed mode (CSMA/CA), and a coordinated mode (polling mode - not much used in practice). 802.11 of course uses MAC level retransmissions, and also RTS/CTS and fragmentation.

The optional power management features are quite complex. The 802.11 MAC protocol also includes optional authentication and encryption (using the WEP, Wired Equivalent Privacy, which is RC4 40 bits - some vendors do offer 128 bits RC4 as well). On the other hand, 802.11 lacks to defines some area (multirate, roaming, inter AP communication), that might be covered by future developments of the standard or complementary standards. Some 802.11 products also implement proprietary extensions (bit-rate adaptation, additional modulation schemes, stronger encryption...), those extensions may or may not be added to the standard over time.

When 802.11 was finalized (September 97), most vendors were slow to implement 802.11 products because of the complexity of the standard and the number of mandatory features (and in some cases they also need to provide backward compatibility with their own previous line of products). Some of the optional features (encryption and power saving) did only appear months after the initial release of the product. But things seem to be sorted out and we now have fully featured products on the market. The complexity of the specification, the tightness of the requirements and the level of investment required made 802.11 products expensive compared to the previous generation of wireless LANs, but because of the higher standardization and higher volumes, prices are now dropping.

Even if vendors eventually have launched 802.11 products, the standard doesn't fully guarantee inter-operability: the products have to use at least the same physical layer, the same bit rate and the same mode of operation (and there are so many other little important details...). The most cooperative vendors have been busy lately sorting out interoperability issues with independent testing labs, but it is still a touchy subject

5.5.2 802.11-b and 802.11-a (802.11 at 5 GHz)

After 7 years of arguing in sub-committees making 802.11, you would think that most people would had enough of it. In fact no, the 802.11 committee is now busy pushing a new standard at 5 GHz and also higher speed at 2.4 GHz (by tweaking the

Direct Sequence physical layer). Both standards make changes only to the physical layer, so that the 802.11 MAC can be reused totally unmodified, saving costs.

802.11-a (802.11 at 5 GHz) was standardized first (spring 99), based on *OFDM*, and using the UNII band. The OFDM physical layer is a very close copy of the one used in *HiperLan II* ,using 52 sub carriers in a 20 MHz channel, offering 6, 12 and 24 Mb/s and optional 9, 18, 36, 48 and 54 Mb/s bit-rates. No products are yet on the market.

Very soon after, 802.11 did standardize **802.11-b** (802.11 HR), based on a modified DS physical layer. The goal was to extend the life of the 2.4 GHz band by overcoming the major drawback: low speed. On top of the original 802.11-DS standard, 802.11-b offer additional 5.5 Mb/s and 11 Mb/s bit rates. It was approved by the FCC and they are now products on the market (which are quite popular).

5.5.3 HiperLan

HiperLan is the total opposite of 802.11. This standard has been designed by a committee of researcher within the ETSI, without strong vendors influence, and is quite different from existing products. The standard is quite simple, uses some advanced features, and has already been ratified a while ago (summer 96 - we are now only waiting for the products).

The first main advantage of Hiperlan is that it works in a dedicated bandwidth (5.1 to 5.3 GHz, allocated only in Europe), and so doesn't have to include spread spectrum. The signaling rate is 23.5 Mb/s, and 5 fixed channels are defined. The protocol uses a variant of CSMA/CA based on packet time to live and priority, and MAC level retransmissions. The protocol includes optional encryption (no algorithm mandated) and power saving.

The nicest feature of Hiperlan (apart from the high speed) is the ad-hoc routing: if your destination is out of reach, intermediate nodes will automatically forward it through the optimal route within the Hiperlan network (the routes are regularly automatically

recalculated). Hiperlan is also totally ad-hoc, requiring no configuration and no central controller.

The main deficiency of Hiperlan standard is that it doesn't provide real isochronous services (but comes quite close with time to live and priority), doesn't fully specify the access point mechanisms and hasn't really been proved to work on a large scale in the real world. Overhead tends also to be quite large (really big packet headers).

HiperLan suffers from the same disease as 802.11: the requirements are tight and the protocol complex, making it very expensive.

5.5.4 HiperLan II

HiperLan II is the total opposite of HiperLan. The first HiperLan was designed to build ad-hoc networks; the second HiperLan was designed for managed infrastructure and wireless distribution systems. The only similarities is the HiperLan II is being specified by the ETSI (Broadband Radio Access Network group), operate at 5 GHz (5.4 to 5.7 GHz) and the band is dedicated in Europe.

HiperLan II was the first standard to be based on OFDM modulation .Each sub-carrier may be modulated by different modulations (and use different convolution code, a sort of FEC), which allow to offer multiple bit-rates (6, 9, 12, 18, 27 and 36 Mb/s, with optional 54 Mb/s), with likely performance around 25 Mb/s bit-rate. The channel width is 20 MHz and includes 48 OFDM carriers used to carry data and 4 additional are used as references (pilot carriers - total is 52 carriers, 312.5 kHz spacing).

HiperLan II is a Wireless ATM system, and the MAC protocol is a TDMA scheme centrally coordinated with reservation slots. Each slot has a 54 B payload, and the MAC provides SAR (segmentation and reassembly - fragment large packets into 54 B cells, and ARQ (Automatic Request - MAC retransmissions). The scheduler (in the central coordinator) is flexible and adaptive, with a call admission control, and the content of the TDMA frame change on a frame basis to accommodate traffic needs. HiperLan II also defines power saving and security features.

HiperLan II is designed to carry ATM cells, but also IP packets, Fire wire packets (IEEE 1394) and digital voice (from cellular phones). The main advantage of HiperLan II is that it can offer better quality of service (low latency) and differentiated quality of service (guarantee of bandwidth), which is what people deploying wireless distribution system want. On the other hand, I'm worried about the protocol overhead, especially for IP traffic.

5.5.5 Open-Air

Open-Air is the proprietary protocol from Proxy. As Proxy is one of the largest Wireless LAN manufacturer (if not the largest, but it depends which numbers you are looking at), they are trying to push Open-Air as an alternative to 802.11 through the WLIF (Wireless LAN Interoperability Forum). Proxy is the only one having all the detailed information's on Open-Air, and strangely enough all the Open-Air products are based on Proxy's module.

Open-Air 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 Open-Air 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.

Open-Air 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 Proxy controls the way all the implementation behave (they don't provide a way

to synchronize to any network as 802.11 manufacturers do). Open-Air also provide coarse power saving.

5.5.6 HomeRF & SWAP

The HomeRF is a group of big companies from different background formed to push the usage of Wireless LAN in the home and the small office. This group is developing and promoting a new Radio LAN standard: SWAP.

The Home is a good market for Wireless LAN because very few houses are nowadays cabled with Ethernet wire between the different rooms, and because mobility in the home is desired (browse the web on the sofa). The use of the 2.4 GHz band allows a free worldwide deployment of the system.

The HomeRF has decided to tackle the main obstacle preventing the deployment of Wireless LAN: the cost. Most users just can't afford to spend the money required to buy a couple of Radio LAN cards to connect their PCs (without talking of the access point).

The main cost of a radio LAN is the modem. As this is analog and high power electronics, it doesn't follow Moore's law (the market trend that allows you to buy a Cray at the price of a calculator after a few years) and modems tend to be fairly stable in price. Frequency Hopping modems tend to be less expensive, but the 802.11 specification impose tight constraints on the modem (timing and filtering), making it high cost. The SWAP specification, by releasing slightly those constraints, allows for a much cheaper implementation, but still keeps a good performance.

The MAC protocol is implemented in software and digital so doesn't contribute that much to the final cost of the product (except in term of development cost). Releasing some hardware constraints prevented the use of the 802.11, which anyway was much too complex and including too many features not necessary for the task.

The main killer application that the HomeRF group envisages is the integration of digital cordless telephony and the computing word, allowing the PC to reroute the phone calls in the home or to offer voice services to the users.

A new MAC protocol has been designed, much simpler, combining the best feature of DECT (an ETSI digital cordless phone standard) and IEEE 802.11: a digital cordless phone and ad-hoc data network, integrated together.

The voice service is carried over a classical *TDMA* protocol (with interference protection, as the band is unlicensed) and reuse the standard DECT architecture and voice codec. The data part use a *CSMA/CA* access mechanism similar to 802.11 (with MAC level retransmission, fragmentation...) to offer a service very similar to Ethernet.

The 1 Mb/s Frequency Hopping physical layer (with optional 2 Mb/s using 4FSK) allows 6 voice connections and enough data throughput for most users in the Home. The voice quality should be equivalent to DECT in Europe and much better than any current digital phone in the US. Data performance should be slightly lower than 802.11. The MAC protocol has also been designed in a very flexible way, allowing developing very cheap handset or data terminals and high performance multimedia cards for PCs.

The SWAP specification is an open standard (in fact, more open than 802.11, because there should be no royalty or patent issues), quite simple and straightforward. In fact, the combination of voice and data gets already most marketing people drooling! The only drawback is that you will have to wait a bit before seeing SWAP products in your favorite supermarket.

5.5.7 Bluetooth

Bluetooth should not even be mentioned in this document, but people keep thinking that Bluetooth is a Wireless LAN. Bluetooth is a cable replacement technology mostly developed and promoted by Ericsson with the help of Intel, offering point to point links and no native support for IP (need to use PPP). It may be good for some applications, but not for Wireless LANs.

I personally read the Bluetooth specification, and I was not impressed, expect by the size of the thing (more than 1500 pages!). My take is that Bluetooth offers the functionality of a Wireless USB, and in fact looking into the huge specification we can see some similarities in the design.

Bluetooth offers the possibility to create a set of point to point wireless serial pipes (RfComm) between a master and up to 6 slaves, with a protocol (SDP) to bind those pipes to a specific application or driver. The Bluetooth mindset is very vertical, with various profiles defining every detail from bit level to application level. TCP/IP is only one profile, implemented through PPP in a specific pipe. There are other pipes for audio, Obex. With Bluetooth, nodes need to be explicitly connected, but they remember bindings from one time to another.

This is miles away from the current wireless LAN approach (connectionless broadcast interface, native IP support, cellular deployment, horizontal play), so Bluetooth doesn't fit TCP/IP and wireless LAN applications too well. On the other hand, as a wireless USB, it fulfills a role that regular wireless LANs can't, because TCP/IP discovery and binding protocols are more heavyweight.

Currently, Bluetooth is moving very slowly due to its complexity and the inherent limits due to the protocol design, but eventually some products should reach the market and later on software support should come.

In summary, if all you want is to run TCP/IP, you may find it cheaper and more effective to NOT wait for Bluetooth and live without the hype

CHAPTER SIX

6. SECURITY IN WIRELESS (LANs)

Overview

When the wireless communications is coming to the offices and the homes, there are some new security issues to be taken care of. Today we have continuously growing markets for the wireless LANs, but there is big black hole in the security of this kind of networks. This paper gives an overview of the security functions specified in two wireless LAN standard, namely in the IEEE 802.11,the HIPERLAN and IPSEC protocol. There is also some discussion about the threats and vulnerabilities in wireless networks compared to wired networks. And last but not least the protocols and mechanisms needed in the secure wireless LAN are described.

6.1 Introduction

Around 1980 was the concept of the wireless LAN introduced and since 1985 have many companies tried to implement variety of wireless LAN applications using spread spectrum, infrared and traditional wide band radio technologies. Now is the real breakthrough of the wideband wireless applications happening; the IEEE 802.11 standard, approved June 1997, gives a solid platform for new applications and the chips supporting IEEE 802.11 are already in the market. The wireless office market revenue was year 1996 $390 million from which $218 million belonged to wireless LANs and it is expected to break a billion dollar in early next millennium.

The commercial wireless LAN applications can be divided in five categories:

- LAN extension - indoor wire replacement
- Inter-LAN bridges - outdoor wire replacement
- Campus Area Networks (CAN) - wireless LANs with infrastructure

- Ad-hoc networking - wireless LANs without infrastructure
- Nomadic access - a wireless LAN service

Today's existing applications aims at four categories of applications:

- Healthcare industry
- Factory floors
- Banking industry
- Educational institutions

The security issues in the wireless environment are much more stressed than in the wired networks, but there are still products without any security functions and even the IEEE 802.11 specifies the security functions as an optional feature. Anyhow the security in the Internet is coming more and more vital and the IPSEC concept and IPv6 are going to demand the ciphering and authentication as mandatory functions in the network equipment. So there is a real need for developing the security in the wireless networks.

6.2 Abbreviations and Definitions

In this document are following abbreviations (table 1) and definitions (table 2) used.

Table 6.1: Abbreviations

AP	Access Point
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BSS	Basic Service Set; A set of stations communication wirelessly on the same channel in the same area. (in IEEE 802.11)
CA	Certificate Authority
CAC	Channel Access Control (in HIPERLAN)
CAM	Channel Access Mechanism (in HIPERLAN)

CCITT	Comite Consultatif International Telegraphique et Telephonique (now ITU-T)
ESS	Extended Service Set; A set of BSSs and wired LANs with Access Points that appear as a single logical BSS. (in IEEE 802.11)
ETSI	European Telecommunications Standards Institute
ETR	ETSI Technical Report
GSM	Global System for Mobile communications
HIPERLAN	High Performance Radio Local Area Network
HM-entity	HIPERLAN MAC entity
ICV	Integrity Check Vector
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standard Organization
IV	Initialization Vector
LAN	Local Area Network
MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
PEM	Privacy Enhanced Mail
PHY	Physical layer
PRNG	Pseudo Random Number Generator
bps	bits per second
SKCS	Shared Key Cryptography System
UMTS	Universal Mobile Telecommunications System
WEP	Wired Equivalent Privacy

Table 6.2: Definitions

ad-hoc	In ad-hoc configuration the wireless LAN has no fixed components
authentication	The identification of the parties
base	Usually fixed base station of the wireless LAN, sometimes referred as Access Point
cipher text	The data after ciphering
confidentiality	Only intended parties can access the data
coverage	The area where the transmission of the node can be heard
denial of service	An attack preventing the system from being used
eavesdropping	Capturing the data by an unintended party
end-to-end	From the sending node to the intended receiver
integrity	The message can not be modified or replaced by unintended parties
key management	The policy to distribute and save the private and public keys
plain text	The data to be send before ciphered
pre-arranged	In pre-arranged configuration the wireless LAN has some fixed components, like bases
private key	A sensitive key that must not be compromised
public key	A non-sensitive that can be published
shared key	A secret key common to many users or network nodes
station-to-station	From one node to the next one in the network
transitive trust	An attack exploiting the host-host or network-network trust

6.3 Standards

This section describes two existing wireless network standards concentrating on the security functions they provide. The proprietary solutions (like Lucent Technologies Wave LAN), existing mobile telephone networks (like GSM) and future technologies (like wireless ATM or UMTS) are out of the scope of this paper.

6.3.1 HIPERLAN

HIPERLAN is ETSI's wireless broadband access standard, which defines the MAC sub layer, the Channel Access Control (CAC) sub layer and the physical layer. The MAC accesses the physical layer through the CAC, which allows easy adaptation for different physical layers. Currently defined physical layers use 5.15 - 5.30 GHz frequency band and support 2 048 Kbps synchronous traffic and up to 25 Mbps asynchronous traffic. HIPERLAN has following properties:

- It provides a service that is compatible with the ISO MAC service definition in ISO/IEC 15 802-1
- Its operations are compatible with the ISO MAC bridges specification ISO/IEC 10 038 for interconnection with other LANs
- It may be deployed in pre-arranged or an ad-hoc fashion
- It supports node mobility
- It may have a coverage beyond the radio range limitation of single node
- It supports both asynchronous and time-bounded communication by means of a Channel Access Mechanism (CAM) with priorities providing hierarchical independence of performance
- Its nodes may attempt to conserve power in communication by arranging when they need to be active for reception

The HIPERLAN specification defines an encryption-decryption scheme for optional use in the HIPERLAN. In this scheme, all HM-entices of a HIPERLAN shall use a common set of shared keys, referred as the HIPERLAN key-set. Each of these

keys has a unique key identifier. Plain text is ciphered by XOR operation with random sequence generated by confidential algorithm by the following structure:

Throughout out this section. the following notations are used.

- & : bitwise AND
- + : addition in modular 2^{32}
- - : subtraction in modular 2^{32}
- ⊕ : bitwise exclusive OR
- & : bitwise AND
- << n : left circular rotation by n bits
- >> n : right circular rotation by n bits
- || : concatenation

The structure of confidential is shown in Figure 6.1.

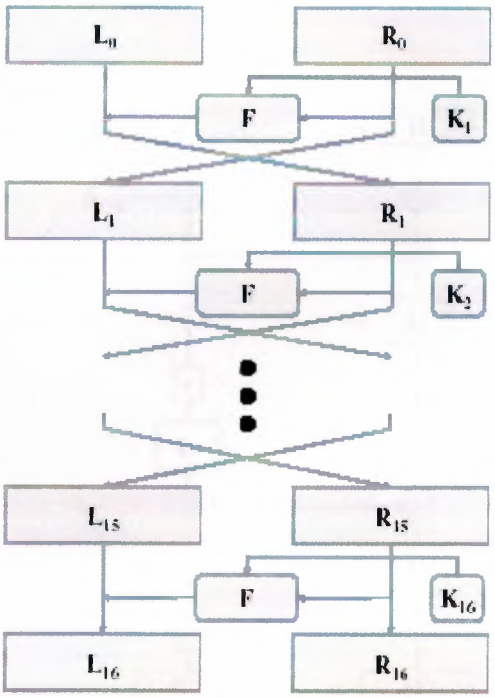

Figure 6.1: Structure of Confidential

❖ **Round function F**

A 64-bit input block of the round function is divided into two 32-bit blocks (C, D) And wrapped with 4 phases: a mixing phase of two 32-bit sub key blocks (Ki,0 , Ki,1) and 3 layers of function G with additions for mixing two 32-bit blocks. The Outputs C', D' of function F with two 32-bit input blocks C, D and two 32-bit Sub keys Ki,0 , Ki,1 are as follows:

$$C' = G[G[G_1(C \oplus K_{i,0}) \oplus (D \oplus K_{i,1})]_1 + (C \oplus K_{i,0})] + G[G_1(C \oplus K_{i,0}) \oplus (D \oplus K_{i,1})]_1]$$
$$+ G[G_2(C \oplus K_{i,0}) \oplus (D \oplus K_{i,1})]_2 + (C \oplus K_{i,0})]$$
$$D' = G[G[G_2(C \oplus K_{i,0}) \oplus (D \oplus K_{i,1})]_2 + (C \oplus K_{i,0})] + G[G_2(C \oplus K_{i,0}) \oplus (D \oplus K_{i,1})]_2]$$

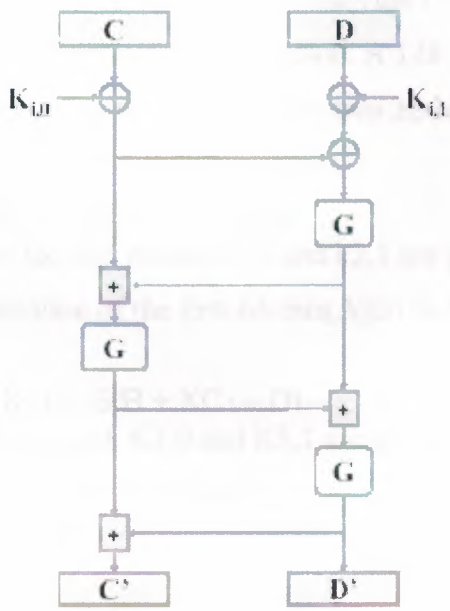

Figure6.2: Round Function F

The function G has two layers: a layer of two 8 × 8 S-boxes and a layer of Block permutation of sixteen 8-bit sub-blocks. The first layer of two S-boxes is Generated from the Boolean functions x247 and x251. The second layer is a set of permutations in each s-boxes.

The output s Z0, Z1, Z2, Z3 of the function G with four 8-bit inputs X0, X1, X2, and X3 are as follows:

$$Z_0 = (S_1(X_0) \& m_0) \oplus (S_2(X_1) \& m_1) \oplus (S_1(X_2) \& m_2) \oplus (S_2(X_3) \& m_3)$$
$$Z_1 = (S_1(X_0) \& m_1) \oplus (S_2(X_1) \& m_2) \oplus (S_1(X_2) \& m_3) \oplus (S_2(X_3) \& m_0)$$
$$Z_2 = (S_1(X_0) \& m_2) \oplus (S_2(X_1) \& m_3) \oplus (S_1(X_2) \& m_0) \oplus (S_2(X_3) \& m_1)$$
$$Z_3 = (S_1(X_0) \& m_3) \oplus (S_2(X_1) \& m_0) \oplus (S_1(X_2) \& m_1) \oplus (S_2(X_3) \& m_2)$$

where. m_0 = 0xfc. m_1 = 0xf3. m_2 = 0xcf and m_3 = 0x3f.

❖ 2.4 Key schedule

The key schedule generates each round sub key. It uses the function G, Addition, subtraction, and (left/right) circular rotation. A 128-bit input key is Divided into four 32-bit blocks (A, B, C, D) and the two 32-bit sub keys of the 1st Round, K1,0 and K1,1 are generated as following:

$K_{1,0} = G(A + C - KC_0)$, $K_{1,1} = G(B - D + KC_0)$.

The two 32-bit sub keys of the 2nd round, k2,0 and k2,1 are generated from the input key with 8-bit right rotation of the first 64-bits(A||B) as follows:

A||B ⟵ (A||B)>>8.

$K_{2,0} = G(A + C - KC_1)$, $K_{2,1} = G(B + KC_1 - D)$.

The two sub keys of the 3rd round, K3,0 and K3,1 are generated from the 8-bit left rotation of the last 64-bit(C||D) as follows:

C||D ⟵ (C||D)<<8.

K3,0 = G(A + C – KC2) , K3,1 = G(B – D + KC2).

The rest of the sub keys are generated iteratively. A pseudo code for the key Schedule is as follows:

```
for (i=1; i<=16; i++){
    K_{i,0} ← G(A + C – KC_{i-1});
    K_{i,1} ← G(B – D + KC_{i-1});
    if (i%2 == 1) A||B ←(A||B) >>8
    else C||D ←(C||D) <<8
}
```

Where, each constant KCi is generated from a part of the golden ratio Number

$\frac{\sqrt{5}-1}{2}$.

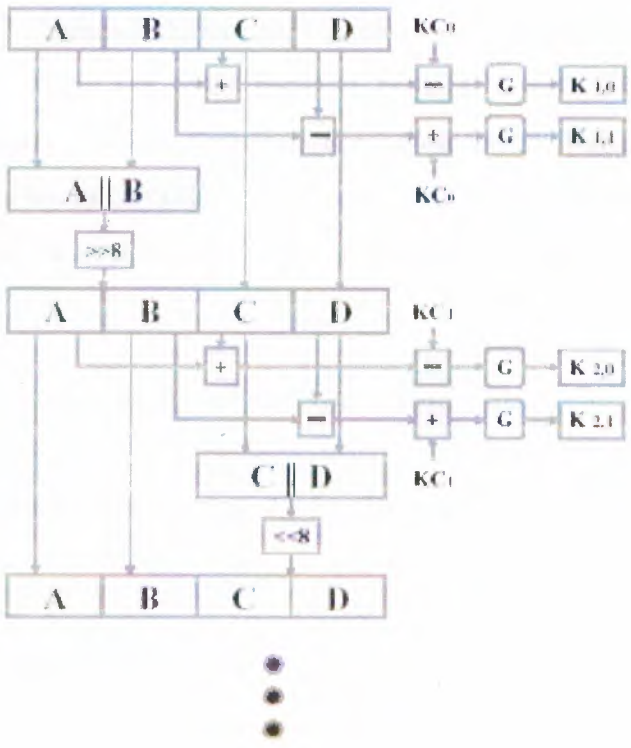

Figure 6.3: Key Schedule

6.3.2 IEEE 802.11

Sponsored by the LAN MAN Standards Committee of the IEEE Computer Society, the 1999 edition of the 802.11 standard defined the physical layer (PHY) and the medium access control layer (MAC) for WLANs. It defined PHYs for 1 and 2 Mb/s data rates in the unlicensed 2.4-GHz radio frequency (RF) band and in the infrared (IR). The 802.11 standard is a member of the family of 802 standards issued by IEEE that include 802.3 (Ethernet) and 802.5 (token ring). It was extended twice in 1999 by 802.11a, which defined the PHY for the 5-GHz band at 6 to 54 Mb/s, and 802.11b, which defined the PHY for the 2.4-GHz band at 5.5 and 11 Mb/s.

The purpose of the 802.11 standard as defined by IEEE is "to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area."

The IEEE 802.11 standard defines the physical layers and the MAC sub layers for the wireless LANs. There are three different physical layers: Frequency Hopping Spread Spectrum Radio, Direct Sequence Spread Spectrum Radio and Base band Infrared. All physical layers can offer 2 Mbps data rate, the radio PHYs uses 2 400 - 2 483.5 MHz frequency band. The MAC layer is common for all three PHY and has the following features:

- Support of Isochronous as well as Asynchronous data
- Support of priority
- Association/Disassociation to an AP in a BSS or ESS
- Re-association or Mobility Management to transfer of association from one AP to another
- Power Management to save in the battery time
- Authentication to establish identity of the terminals
- Acknowledgment to ensure reliable wireless transmission
- Timing Synchronization to coordinate the terminals
- Sequencing with duplication detection and recovery

- Fragmentation / Re-assembly

The PRNG algorithm used in IEEE 802.11 is RC4 from RSA Inc. The actual algorithm is not public, the general structure as the following:

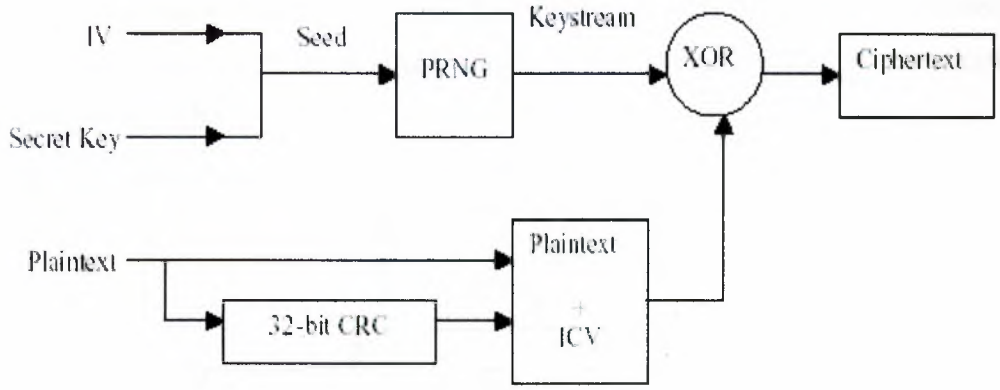

Figure 6.4: PRNG

But has been studied in independent research laboratories under nondisclosure agreements and no weaknesses has not yet been reported, which does not guarantee that these does not exist. Anyway the secret key used is only 40 bits long, which can be solved by brute-force attack in 2 seconds with $100 000 hardware and 0.2 seconds with $1 000 000 hardware according the 1995 figures ; today the hardware prices are significantly lower. And even with some additional strength gained with variable IV the protection level of WEP may not be considered strength enough for the most sensitive applications. The Shared Key Authentication scheme could be easily fooled using for example the play-back attack. So anyway an additional authentication mechanism is needed.

6.4 IPSEC protocol

IPSec is a family of protocols that can be used to secure a connection between any Two Internet hosts. For example, IPSec can be used to secure the link between a Client and a server, a home user and a corporate network, or two Internet routers. In

The Reef Edge Connect System, IPSec is used to secure the links between the Wireless client and the wired network.

There are two types of protocols used by IPSec: a control protocol for establishing Secure connections, and data protocols for communicating securely. The standard Control protocol used by IPSec is called Internet Key Exchange, or IKE. The standard Data protocols are the Encapsulating Security Protocol (ESP) and the Authentication Header protocol (AH).

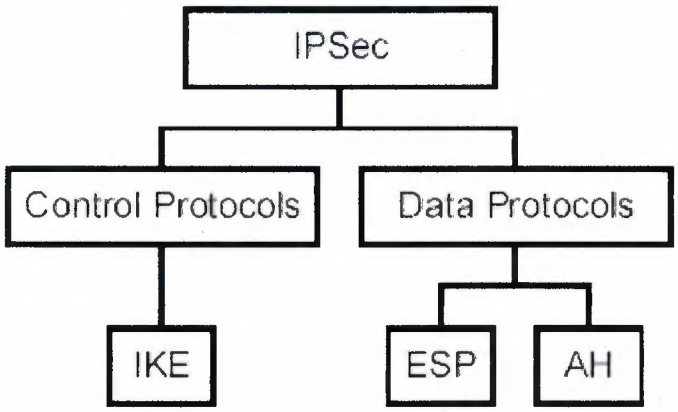

Illustration: Internet Protocol Security (IPSec) Architecture

Figure 6.5: IPsec Architecture

IKE is used to establish a secure connection, called a Security Association (SA), Between two Internet hosts. It is a combination of several different protocols: ISAKMP, which provides a framework for negotiating parameters, and Oakley, which Is used for mutual authentication and SKEME, which is used for key exchange. IKE allows many different options to be set for the connection establishment process, and For the connection being established. The two hosts can negotiate encryption Algorithms, key sizes, and message integrity checks.

The IKE protocol allows the two hosts to exchange encryption keys securely. The Diffie-Hellman key exchange algorithm is used, so that no session keys are ever sent directly over the network. Additionally, the two hosts authenticate each other using a shared secret, digital signature, or public keys, in order to prevent unauthorized users from establishing connections, and to prevent man-in-the-middle attacks.

An additional feature of IKE called Perfect Forward Secrecy (PFS) helps assure that keys are secret. At regular intervals, the two hosts will renegotiate encryption keys using a new Diffie-Hellman exchange. This assures that even if an attacker discovers one encryption key, they will not be able to derive future keys.

The data between the two hosts can be secured either by AH or ESP. AH assures message integrity, but not privacy. ESP assures both message integrity and privacy. Computers use a variety of different algorithms to secure data.

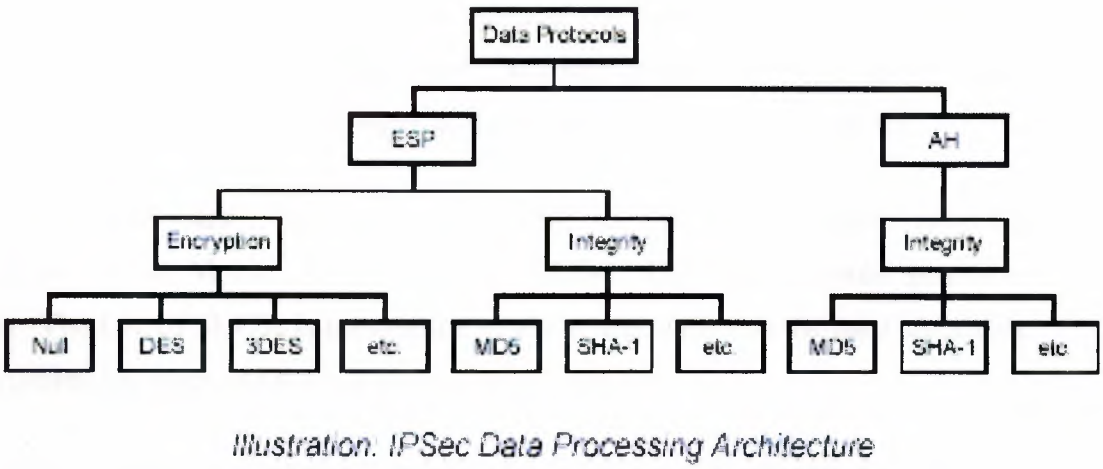

Figure 6.6:IPSec Data Processing Architecture

6.5 Authorization

Table 6.3 defines nomenlactures used in this chapter.

Table 6.3: Nomenlactures

E(X,Y)	Encryption of Y under key X
MD(X)	Message Digest of X
Pub_CA	Public Key of Certification Authority
Priv_CA	Private Key of Certification Authority
Pub_Mobile	Public key of Mobile Host

Priv_Mobile	Private Key of Mobile Host
Pub_Base	Public key of Base Station
Priv_Base	Private Key of Base Station
Cert_Mobile	Certificate of Mobile Host
Cert_Base	Certificate of Base Station
Sig(X,Y)	signature of Y with key X where Sig(X,Y) = E(X, MD(Y))
Signed(X,Y)	resulting signed message {Y, Sig(X,Y)}

The authorization mechanism uses certificates formatted according to CCITT X.509 used in X.500 and PEM. A certificate contains the following information: {Serial Number, Validity Period, Machine Name, Machine Public Key, CA name}. Each certificate is signed by CA which might in our case be the enterprise's own CA.

The first message send from the mobile to the base contains following information: {Cert_Mobile, CH1, List of SKCSs}. CH1 is randomly generated number. The List of SKCSs is transmitted to allow negotiation of the used algorithm; the algorithm identifier and the key size are sent in the list.

When the base has received the first message, it will attempt to verify the signature on Cert_Mobile. A valid signature proofs the public key in the certificate belongs to a certified mobile host but it is not sure if the certificate actually belongs to the mobile that submitted it. If the certificate is invalid, the base rejects the connection attempt.

Now the base will reply to the mobile by sending the message containing {Cert_Base, E(Pub_Mobile, RN1), Chosen SKCS, Sig(Priv_Base, {E(Pub_Mobile, RN1), Chosen SKCS, CH1, List of SKCSs}}}. Random Number RN1 is saved internally for later use. Chosen SKCS is one from the list sent by mobile and includes the algorithm identifier and the key size; the Chosen SKCS is the most secure from those supported by both the base and the mobile.

The mobile validates Cert_Base, if certificate is valid, the Mobile will verify using the public key of the Base the signature off the message. The signature is valid and the base authenticated if the CH1 and the List of SKCSs matches with those sent

by mobile to the base. Since the list of SKCSs is included in the signature, the attacker cannot send the weakened list of SKCSs by jamming original message and sending his own, and we need not to sign the first message.

Now the mobile sends to the base message containing: *{E(Pub_Base, RN2),* Sig{Priv_Mobile, {E(Pub_Base, RN2), E(Pub_Mobile, RN1)}}}. The RN2 is a random number generated by the mobile. The mobile will use the RN1 XOR RN2 as a session key for now on.

The Base verifies the signature of the message using Pub_Mobile obtained from Cert_Mobile in the first message. If the signature is valid, the mobile is authenticated. Next the base will decrypt E(Pub_Base, RN2) with it's own private key. Now the base can form the session key RN1 XOR RN2.

The session key is formed from two parts sent in different messages to gain better protection. Now the compromising of the mobile's private key does not compromise the whole traffic between the base and the mobile. Since the both halves of the session key are random and equal length, knowing either RN1 or RN2 tells nothing about the session key.

If all these steps have succeeded the mutual authentication has been done and the session is established. Figure 6.3 summarizes the authentication protocol. The correctness of this protocol is proofed in.

This authentication should be done in the MAC layer, before any network access is granted to the mobile. If we give to the mobile IP address before the authentication, it may be used as a launch pad even if it's authentication request is rejected.

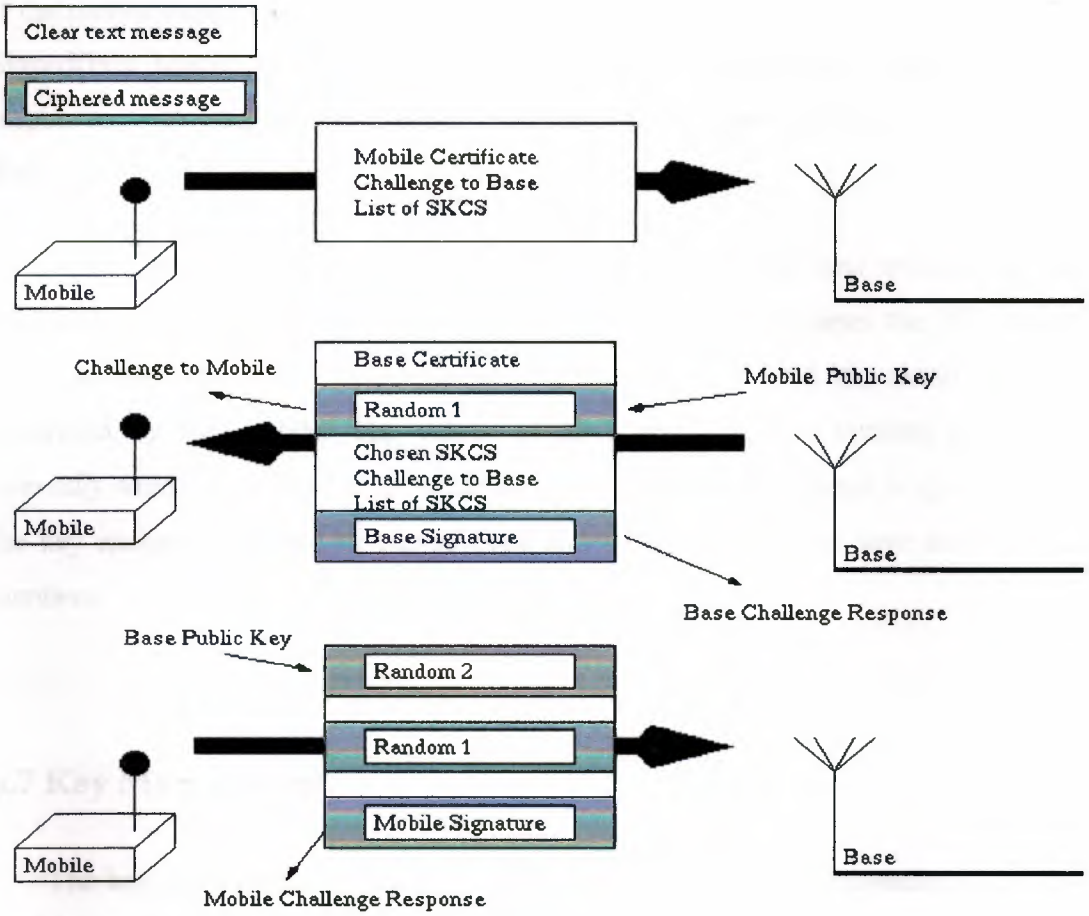

Figure6.7: Authentication Protocol

6.6 Key Change Protocol

The nomelactures defined in the table 6.3 are used here. The key exchange may be initialized from both ends of the communication; the base initialized case is handled first.

First the base sends to the mobile a message: Signed(Priv_Base, { E(Pub_Mobile, New_RN1), E(Pub_Mobile, RN1) }) and the mobile responses with message: Signed(Priv_Mobile, { E(Pub_Base, New_RN2), E(Pub_Base, RN2) }).

If the mobile initializes the key exchange procedure, then it send to the base message: Signed(Priv_Mobile,{E(Pub_Base, New_RN2),E(Pub_Base,RN2) })and the base responses with: Signed(Priv_Base, { E(Pub_Mobile, New_RN1), E(Pub_Mobile, RN1) }).

Again the value new_RN1 XOR new_RN2 is used as the new session key. The values RN1 and RN2 are always the last ones used. In both cases the RN1 always refers to the random number generated by the base and RN2 the random number generated by the mobile. The values of RN1 and RN2 are verified against the internally saved values and if those do not match, the key exchange is ignored. Now the key exchanges cannot be played back and we do not need to save any sequence numbers.

6.7 Key Management

The key management is one of the stuffiest part implement convenient way. One possible procedure using the smart card technology is described below:

1. CA creates the private and public keys inside the smart card by the way that the private key is never readable from the smart card.
2. CA signs the public key with his private key and stored the signed public key to the smart card.
3. The smart card is given to the end user, which may now use the smart card in any wireless LAN mobile.

In order to avoid reading the private key from the smart card the public key cryptography system must be run inside the smart card and the calculation power of the smart cards sets some limitations for the efficiency of this approach. Of course the smart card reader is needed for each mobile used in the wireless LAN. But it is not very wild guess that the smart card technology will become more efficient and cheaper in the near future.

The concept described here is not the only one: it is also possible to use the Wep of Trust scheme for the key management or the user may generate the key par by himself and then give the public key to the CA for the certificate signing, but the user identification must be somehow done also in this case.

6.8 Summary

The current wireless LAN standards offer very unsatisfactory level of security and one could not truly trust them. When using products based on these standards must the security issues been taken care in the upper layers. The authentication mechanism described may be used over IP to perform end-to-end authentication, as described in, but this approach gives a potential launch pad for the attacker.

Some commonly used attacks are more stressed in wireless environment and some additional effort should be used to prevent those. The nature of the radio communication makes it practically impossible to prevent some attacks, like denial of service using radio interference. When the wireless networks are used in strategic applications, like manufacturing or hospitals, the possibility of this kind of attack should be taken into account with a great care.

As showed the quite secure wireless LAN is possible to implement with current technology. The current hardware could be used with only some modifications in the MAC layer protocols and over that new MAC the current IP may be used without any problems. Anyway it is not probable that products supporting this level of security come to the markets soon.

CONCLUSION

Wireless LANs come in many types: infrared, microwave and radio. Radio is further broken down in to direct sequence and frequency hopping spread spectrum. The MAC layer protocol used by Wireless LANs as standardized in 802.11 is CSMA / CA. A number of topologies for wireless LANs have been discussed. Traditional wired LANs will become a thing of past as more and more users become mobile. There is great interest in the research community regarding the interoperability of Wireless LAN with the current Wide Area Networks such as Internet and ATM. Meanwhile there is lot of effort going on to increase the throughput, reliability and security of Wireless LANs.

Wireless LAN provides high speed data communication. The minimum data rate specified by the IEEE Project 802.11 is 1Mbps. NCR's waveLAN operates at 2Mbps, while Motorola's ALTAIR operates at 15Mbps.Because of their limited mobility and short transmission range, wireless LANs can be used in confined areas such as a conference room. In the U.S, almost all WLANs products use spread spectrum transmission. Therefore they transmit information on the ISM band. But with this frequency band, users can experience interference from other sources using this band.

REFERENCES

[1] Tanebaum Andrew S., Computer Networks, 1998

[2] Martin Michael J., Understanding the Network: A Practical Guide to Internetworking, Macmillan Computer publishing, USA, 2001

[3] Microsoft, Networking Essentials, Microsoft Corporation, Washington, 1996

[4] Draft standard IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 1999

[5] K. Pahlavan, A. Zahedi, P. Krishnamurthy. Evolving WLAN Industry Products and Standards. Invited paper PIMRC'97, Worcester Polytechnic Institute, 2001

[6] A. Zahedi, P. Krishnamurthy, S. Bagchi, K. Pahlavan. An Update on the Evolution Of the Wireless LAN Services. Worcester Polytechnic Institute, 2000