NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

SECURITY OVER WIRELESS NETWORK

Graduation Project
COM- 400

Student: Obieda Zytoon (20042304)

Supervisor: Besime Erin

Nicosia - 2008

ACKNOWLEDGMENT

In the name of Allah I started my work and finished it as well inspiration to complete this project.

I would thank my supervisor Besime Erin For her advising, helping and supporting me to achieve this work.

To my parents who supported me and without their helping I couldn't perform my tasks.

To my brothers eng. Ra'ed ,Yousef and Mahmoud and my sister Ala'a.

To the computer department stuff who provide me a special knowledge and experience.

To all my friends in Jordan and Cyprus especially who provide me the suitable environment to proceed my work Hasham, Zaid, Ismael, Muath and mohammad.

To Amer, Ahmed Okasha , Muath and Mahmoud abu nawa .

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

Its obviously that security is the major word in our life, at home, at work and even in relation. So security starts to be our main concept in daily life.

We do focus in this project on a part of the security with is related to network (Security over wireless network).

Let's squeeze up the following chapters:

Hitting up in Chapter one overview of local area network and wireless network includes types of local area network, Components of Local Area Networks and the advantages – disadvantages of wireless network.

Chapter two discuses wireless LAN's technologies and network structure then we show some of technologies like spread spectrum technology, infrared LAN's technology

Throw chapter there we spot the light on wireless LAN implementations, wireless LAN PHY implementations and wireless LAN MAC implementations.

Chapter four briefing the history of wireless LAN standards, and discuses the standards, the differences between them.

Finally chapter five brings out the major concepts of security over wireless network and summarizes kinds of attacks that may occur to the wireless network. Also encryption and decryption-The WEP protocol.

CHAPTER ONE

1. OVERVIEW TO COMPUTER NETWORKS

1.1 Over View to Computer Networks

A computer network is a group of computers, printers, and other devices that are connected together with cables. Information travels over the cables or wireless, 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 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 LINUX, Solaris, and HRUX -- come with a package called

Internet Connection Sharing (ICS) that support controlled access to resources on the network.

1.3 Types of Local Area Networks

LANs are usually further divided into two popular types:

1.3.1 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.

1.3.2 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.

1.4 Components of Local Area Networks

1.4.1 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.

1.4.2 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.

1.4.3 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. Un-routable protocols can't be forwarded.

1.4.4 Brouters

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

1.4.5 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.

1.5 Overview to Wireless LANs

Over the last five years desktop computers have changed from stand-alone workstations into networked clients, which rely on connectivity. E-mail, remote storage and the Web are just a few of the uses that are commonplace in most institutions, both educational and commercial. In addition, computing is becoming more mobile, handheld and notebook computer sales are growing each year. And nowadays notebook sales have increased by 20% each year for the last three years and show no sign of slowing.

This move towards mobile use and a reliance on the network has caused increasing problems for computing departments in all areas of industry and education. To address these problems Radio and Infrared technology are being used to connect mobile users to the network and provide a network infrastructure in buildings that previously would have been impossible. What was once a fledgling technology is being transformed by improved systems into a viable and cost-effective solution.

Wireless networks can be divided into two areas in much the same way that traditional wired networks are: Local Area Networks (LANs) and Wide Area Networks (WANs). As with wired networks, wireless LANs have a higher data rate and are

confined to small areas such as a building or campus. Wireless WANs can cover anything from a city to a continent. This project concentrates on Local Area Networks and much of the content of this project is dedicated to wireless LANs.

1.6 Wireless LANs

Wireless networks are a reality, installations in hospitals and trading rooms are becoming common place. The recent ratification of the IEEE 802.11 Standard for Wireless LANs has legitimized the systems which are widely available and given consumers the confidence to start investing in wireless technology. The intention of the wireless LAN is not to replace the wired network, as reduced speed and other complications mean that wired systems will have a higher data rate transmission in a typical environment with our current available technology. However, a wireless network will be more cost effective in the long run. Wireless systems are designed to solve problems that wired solutions couldn't address. The most obvious scenario would be the mobile user who needs to access network resources from his or her portable computer. A wireless network would allow them to work from any location within the wireless LAN and access the network resources with the minimum of effort. In contrast to the mobile solution, a wireless system could be used with desktop computers, for example, in a building, where regulations prevent cables being installed. A wireless solution would allow the desktop computers to connect to a network without disturbing the structure of the building. Another use might be a temporary network, at an exhibition. A wireless LAN could be set up within minutes and then dismantled after the exhibition has finished leaving no trace.

Wireless networks can be implemented in two ways, Either Wireless WANs or Wireless LANs, which are examples of structured networks, where the wireless LAN is an extension of the existing LAN. They consist of Access Points (AP) spread around a building or campus and connected together or onto the wired LAN using copper cable. Mobile users in range of an AP can connect to other wireless users or to network resources. This type of WLAN is known as an infrastructure WLAN (See Figure 1.1).

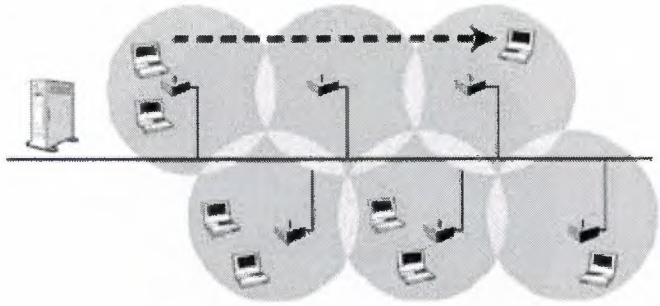

Figure 1.1 Infrastructures WLAN

In infrastructure WLANs, multiple access points link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. As a user moves around the building or campus, the AP hands off responsibility for that user to the next AP. Another type of wireless network, and the simplest form, is the ad-hoc, peer to peer network, which may be set up quickly between several computers for the duration of a meeting. The simplest WLAN configuration is an independent LAN that connects a set of PCs with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network (See Figure 1.2). These on-demand networks typically require no administration or pre-configuration.

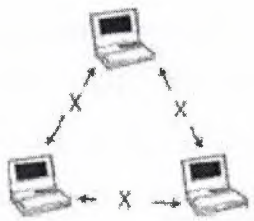

Figure 1.2 Independent WLAN

Access points can extend the range of ad-hoc LANs by acting as a repeater, effectively doubling the distance between wireless PCs (See Figure 1.3).

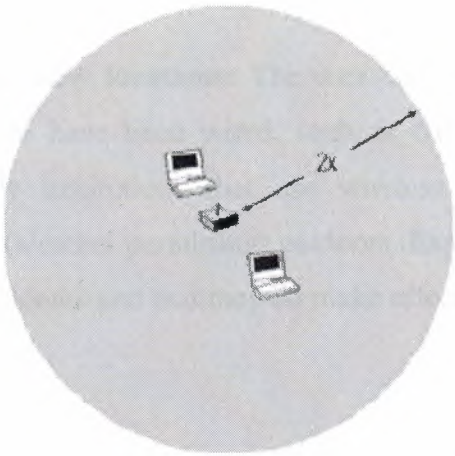

Figure 1.3 Independent WLAN Using Access Point as Repeater

1.7 Advantages

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 advantages:

- **Mobility**: Wireless LAN systems can provide users access to real-time information anywhere within the organization. This extra mobility supports productivity and service opportunities not possible with wired networks.

- **Flexibility & Scalability**: Deploying a wireless network eliminates the need to pull wires or cables through walls and ceilings. Wireless LAN gives organizations the flexibility to move people from office to office, re-organize departments or even entire campuses almost effortlessly. Once Wireless LAN base units are located strategically throughout building, users simply insert an adapter card into their computer and are free to move about.

- **Cost Savings**: With the simple and flexible architecture of WLAN, organizations can save network management costs related to adds, moves and changes, guaranteeing a short term return on investment.

- **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.

- **Extended coverage to new locations:** The user can be anywhere, including places that might never have been wired, such as corridors, cafes and even outdoor spaces. Many institutions that use wireless LANs have included coverage in cafes and (weather permitting) outdoors. Experience shows that this is very popular with students and that they do make effective use of these spaces for online learning.

1.8 Disadvantages of wireless LANs

- **Less secure than wired LANs:** Wireless introduces some additional security problems beyond those associated with a wired network (which a wireless LAN shares). Considerable effort has gone into providing security to meet these problems, and a more detailed discussion is provided below. Some of the key issues are highlighted here. The signal from a wireless LAN will pass through walls, which means hackers do not even need to be inside the premises to access the LAN. If they can make use of the wireless LAN they are on the college or university network. Once inside, hackers can monitor the traffic on the network and so acquire user names and passwords. These are normally encrypted, but there are some doubts about the effectiveness of encryption.

- **Standards are still evolving:** The standards for wireless LANs are still evolving and not always compatible with one another. A number of different standards are used or defined by organizations which sometimes communicate only with themselves. Europe has been working on some standards for use in the EU, while the IEEE, based in the US, has been defining worldwide standards.

- **Management of the network is more complex:** There are a number of issues associated with managing wireless networks which add to the complexity of network management in a mixed wireless and wired LAN environment. These include the need to manage the wireless LAN as a single subnet if roaming is to work,

- **Cost of network cards:** While cards for wired Ethernet start at around £10, wireless cards start at around £60. Although they will become cheaper, they will never be as cheap as wired LAN cards because they are inherently more complex. How the wireless part of the LAN relates to the rest of the network and managing security. With modern wireless LANs management is for the most part undertaken centrally. However, some changes need to be made at the access points themselves.

- **Network performances degrades with additional users:** If many users are connected to the LAN via the same access point, the performance of the LAN can degrade quite rapidly by comparison with wired Ethernet systems. This is because the available bandwidth is shared between all the users, and because of the nature of the communications protocols needed to support wireless working. The overheads associated with setting up each message are much larger for wireless LAN than for a wired LAN, and the protocols enforce waiting times (of microseconds) at certain points. The decline in network performance is particularly great when two PCs are hidden from each other (for instance at opposite sides of the cell) but both are trying to communicate with the access point at the same time, so corrupting each other's messages.

- **Multi-path fading:** can be caused by signals bouncing off walls and other surfaces. As the signal is transmitted to the receiver a reflection of the signal may take slightly longer to arrive and will interfere with the original transmission; it may even arrive out of phase and cancel out the signal all together. Antenna diversity attempts to solve this problem, it involves having two antennas built into the hardware, and allows the system to determine which signal is stronger and therefore the correct signal.

1.9 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.

1.9.1 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.

1.9.2 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.

1.9.3 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.

1.9.4 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.

1.9.5 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.

1.10 Wireless LAN factors

These are the factors of the wireless LAN system:

1.10.1 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.

1.10.2 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.

1.10.3 Simplicity and Easy 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 reconfigure 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.

1.10.4 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 microcells.

1.10.5 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 multi-path, 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).

CHAPTER TWO

2.WIRELESS LAN's TECHNOLOGIES

2.1 Introduction

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.

2.2 Network Structure

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 2.1. 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 2.1, 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 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.

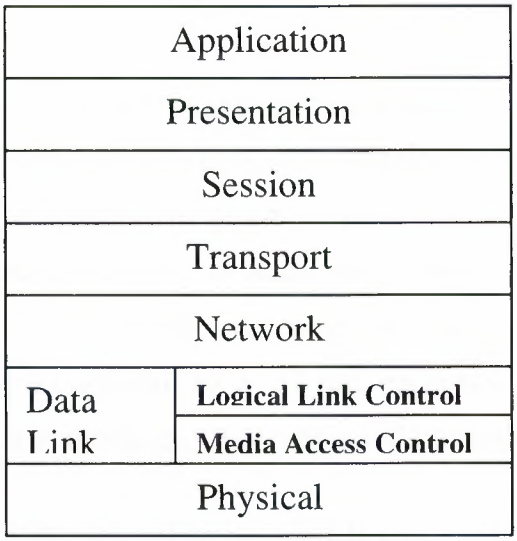

Figure2.1 Open System Interconnect Model

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 clients 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.

2.3 Technologies

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 as shown in Figure 2.2, 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.

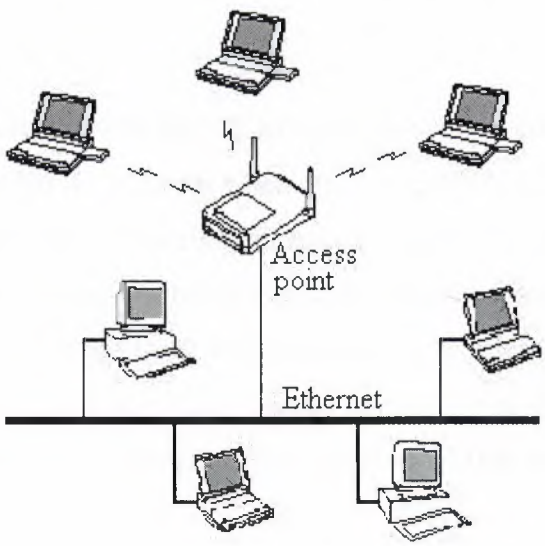

Figure 2.2 Infrastructure Network

2.3.1 Spread Spectrum Technology

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.

2.3.2 Infrared LAN's Technology

An alternative approach to radio-based wireless LANs 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 and this specified by the Infrared Data Association.

2.3.2.1 Infrared Data Association (IrDA) Technology

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.

2.3.3 Low-Power Narrowband Technology

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 milli-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.

2.3.4 HiperLAN Technology

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.

CHAPTER THREE

3.WIRELESS LAN IMPLEMENTATIONS

3.1 Introduction

Local Area Networks have evolved over the past 20 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; NORTEL 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 have 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 55 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 interferers 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 GHz 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.

3.2 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 (hopped) 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 3.1. The obvious question arises: why not just assign a fixed frequency to each user and share the bandwidth in that manner? The answer lies in how a FHSS responds to interferors. 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.

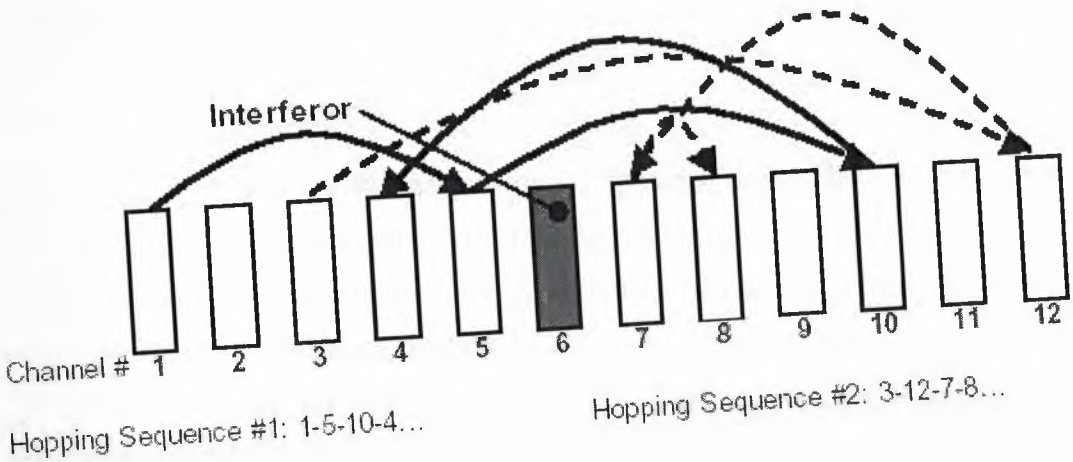

Figure 3.1 Frequency Hopping Spread Spectrum

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 3.2. 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 correlate 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-linearity in the receiver generate inter-modulation distortion products between the desired signal and the interfering signals.

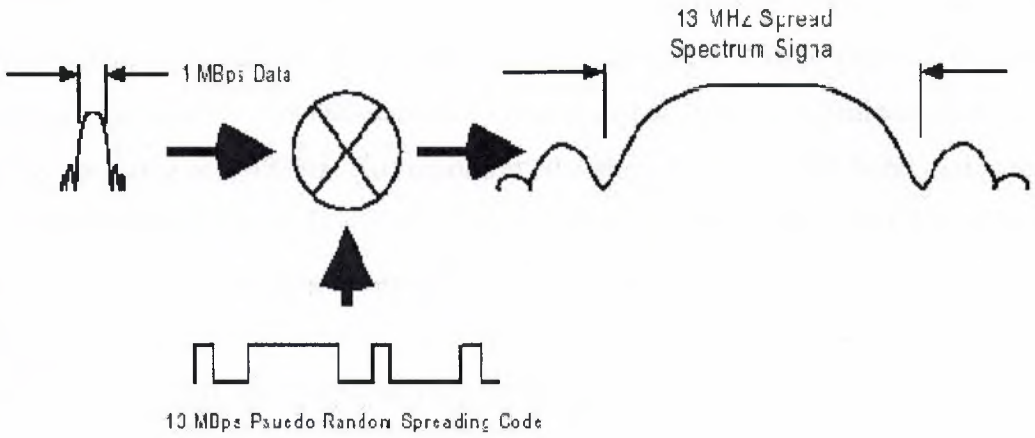

Figure 3.2 Direct Sequence Spread Spectrum

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, RadioLAN 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 RadioLAN 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 interferors.

3.3 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 ad hoc 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 RadioLAN WLAN product family that have been designed for total Ethernet compatibility.

3.4 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 RadioLAN is 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 interferers 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.

CHAPTER FOUR

4. WIRELESS LAN STANDARDS

4.1 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.

4.2 History of Wireless LAN Standards

Standards for data communication networks are set by three different classes of organizations:

1. Government regulatory bodies that are given statutory authority to manage the aspects of communications impacting the general public.
2. National or international standards organizations who maintain the large body of standards covering many other topics besides simply data communication.
3. 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 cover 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.

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.

4.2.1 The Aim of Standard

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 de facto standard can be created. The de facto 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.

4.3 Some Wireless LAN standards

A short gallery of the most famous Wireless LAN standard :

4.3.1 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 obsoleted 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 (multi-rate, 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

4.3.2 802.11-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.

- **802.11-b:** 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).

- **802.11 g**: Transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.

- **802.11 n:** Is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second.
-

4.3.3 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.

4.3.4 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 convolutional 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, Firewire 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.

4.3.5 OpenAir

OpenAir is the proprietary protocol from Proxim. As Proxim 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 OpenAir as an alternative to 802.11 through the WLIF (Wireless LAN Interoperability Forum). Proxim is the only one having all the detailed information's on OpenAir, and strangely enough all the OpenAir products are based on Proxim's module.

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

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

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

4.3.6 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.

4.3.7 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.

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.

CHAPTER FIVE

5. WIRELESS LAN SECURITY

5.1 Introduction

Wireless technologies have been around us since the discovery of the electromagnetic waves. Inventions like radio and TV have proved that air can be a good and convenient medium to dissipate information. However, it was not until the digital era when wireless has become a part of everybody's way of life. Infrared enabled keyboards and mice, digital mobile phones, two-way pagers, wirelessly capable Personal Data Assistants (PDAs) or laptop computers equipped with wireless PC cards are just some of the devices that can be readily seen in an office, on the street or at home.

Over the years, industry has clearly distinguished two applications of wireless communications: voice and data. Voice devices have been traditionally mobile phones. With the introduction of the paging services, messaging and IP telephony applications have shifted into data, with the intention to merge both applications into one.

New technologies that will seize our imagination in the upcoming years are 2.5 and 3G, 802.11a based WLAN, Bluetooth, MMDS and LMDS. Many of these technologies have cryptic names that most people don't even know what they stand for. However, everybody knows that wireless is probably going to be a preferred way of connecting people around the world. Well, this will be true at least for the majority of casual users. High-speed data networking will still require wired connectivity. After all, as somebody said, the word "wireless" contains in it the word "wire". Another twist on it is that it just means "less wire".

5.2 IEEE 802.11 based WLAN

IEEE has adopted the 802.11 standard in 1997. This is the first WLAN standard that IEEE has adopted. IEEE 802.11 standard defines the media access control (MAC) and physical (PHY) layers for a WLAN. It addresses local area networking where the connected devices communicate over the air to other devices that are within close proximity to each other. This standard is similar to the IEEE 802.3 standard that defined Ethernet, but it addresses certain issues that are specific to wireless data transmission, some of which will be explained in this paper.

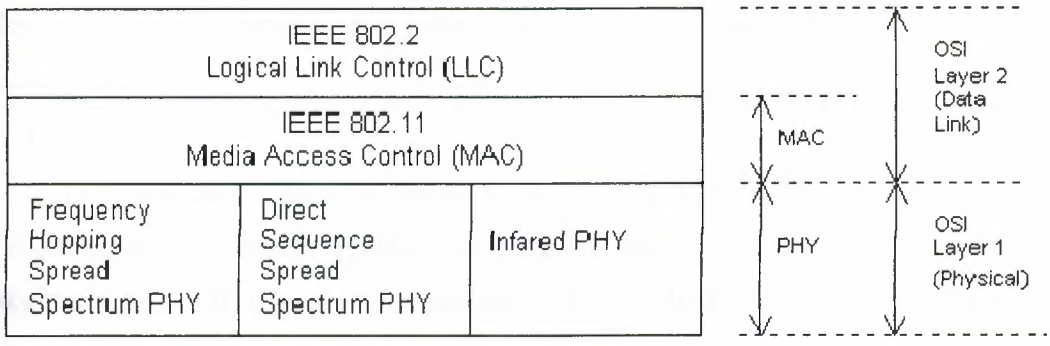

Figure 5.1 IEEE 802.11 standards mapped on the OSI reference model

WLAN standard describes three types of physical layers (Fig. 5.1): Infrared, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Infrared physical layer has never been massively utilized and it stayed on the margin due to a limitation that it has a very small coverage (single room). Spread Spectrum is a technology developed during WWII for the military to provide interference resistance and signal shape that resembles the white noise to lower the chance of detection/interception by the enemy. Spread Spectrum reduces the peak transmit power, but keeps the total power the same. Primary use of the Spread Spectrum in WLANs is its interference resistance.

There were a few WLAN solutions in the early 90s in the 915 MHz Industrial, Scientific and Medical (ISM) band, providing data rates of 1-2 Mbps even before 802.11 standards. Some of the adopters were Aironet and AT&T Bell Labs. The advantage of ISM bands is that these are license-free bands in most of the world. FCC has given away these bands for public use, but some regulations on transmit power and proper filtering are still in place. However, these rules are considered to be fairly

flexible and that is believed to be one of the most important reasons of why WLANs have become so popular. 802.11 standards chose for RF PHY part of the ISM spectrum in the 2.4 GHz range. The band is 83 MHz wide (US only) and it is also the same band in which microwave ovens operate.

Frequency Hopping utilizes a set of narrow channels and "hops" through all of them in a predetermined sequence. For this purpose, 2.4 GHz frequency band is divided into 79 channels, each 1 MHz wide. Every 20 ms the system "hops" to a new channel following a predetermined cyclic pattern. This physical layer can achieve data rates of 1, and 2 Mbps.

The principle of direct sequence is to spread a signal on a larger frequency band by multiplexing it with a signature or code to minimize localized interference and background noise. To spread the signal, each bit is modulated by a code. In the receiver, the original signal is recovered by receiving the whole spread channel and demodulating with the same code used by the transmitter. Spectrum is divided in the US into 11 channels of which only three are non-overlapping. It also provided rates of 1, 2, 5.5, and 11 Mbps.

802.11 standards define frame format and MAC scheme that differ from the 802.3 Ethernet standards. Frame format is more robust and enables a number of new features including fast acknowledge, handling hidden station, power management and data security. 802.11 standards adopted Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, as opposed to only Collision Detection (CSMA/CD) in the Ethernet standard. Also, 802.11 MAC layer provides frame receipt acknowledgement by the receiving station, while in Ethernet standard that is handled by upper layers.

WLAN configurations vary from simple, independent, peer-to-peer connections between a set of PCs, to more complex, intra-building infrastructure networks . There are also point-to-point and point-to-multipoint wireless solutions. A point-to-point solution is used to bridge between two local area networks, and to provide an alternative to cable between two geographically distant locations (up to 30 miles). Point-to-multi-point solutions connect several, separate locations to one single location or building.

In a typical WLAN infrastructure configuration, there are two basic components:

- Access Points

An access point/base station connects to a LAN by means of Ethernet cable. Usually installed in the ceiling, access points receive, buffer, and transmit data between the WLAN and the wired network infrastructure. A single access point supports on average twenty users and has a coverage varying from 20 meters in areas with obstacles (walls, stairways, elevators) and up to 100 meters in areas with clear line of sight. A building may require several access points to provide complete coverage and allow users to roam seamlessly between access points.

- Wireless Client Adapter

A wireless adapter connects users via an access point to the rest of the LAN. A wireless adapter can be a PC card in a laptop, an ISA or PCI adapter in a desktop computer, or can be fully integrated within a handheld device.

802.11 Standard has also built-in provisions for client node to be able to roam between access points without loosing connectivity. Client has to sense different access point channels as it roams. This is provided by a beacon, which is regularly transmitted by an access point. Client roams to another access point as the signal of the nearby station becomes stronger.

Early on after the standard, there was a fierce battle between FHSS and DSSS. Still, price was the most prohibitive factor in wide deployment. Cost per access point was on the order of a few thousand dollars and client adapter of around $800. By changing the modulation scheme, DSSS was able to achieve rates of up to 11 Mbps. This eventually led to the new standard issued by IEEE. It is called 802.11b and was adopted in the Fall of 1999. It provided only DSSS as a PHY layer. It required a rate fallback to 5.5 Mbps, 2 Mbps and 1 Mbps. This standard is also known as the High-Rate DSSS (HR/DSSS).

To insure interoperability of devices an independent body was formed. It is called Wireless Ethernet Compatibility Alliance (WECA) and it brands compliant products as "Wi-Fi".

It is also worth noting that while in Ethernet MAC overheads are fairly small; in RF these are fairly big, so that 11 Mbps rate translated in maximal useful data rate of 5-6 Mbps, or up to about 7 Mbps if short radio preambles are used (Aironet). Also, RF is a shared medium ("half-duplex"), so data rates are still much lower than 10/100 Mbps full duplex Ethernet.

But, WLAN story does not end here. Before the end of 2001, a new IEEE standard is going to be ratified - 802.11a. It defines PHY that will utilize ISM band in the 5 GHz range. It will provide more non-overlapping channels and data rates of 54 Mbps.

5.3 Data Security Provisions in WLANs

As with any type of data transmission there is a concern of the security of the data being transmitted. This is very important in WLAN because information is being transmitted by means of RF. This is true even for DSSS – data can be intercepted more easily than wired transmission.

In the wired LAN, physical security of the link is provided by limiting access to the facility, i.e. an Ethernet port. In the WLAN, anybody can sit in front of a building, on a public land and intercept data.

The IEEE 802.11b standard defines two mechanisms for providing access control and privacy: Service Set Identifier (SSID) or simply Network Name (NN) and Wired Equivalent Privacy (WEP).

Network Name is a naming handle and provides a rudimentary level of access control. Default configuration on most shipped devices is "ANY", which means that no NN is set. By default, this name is being broadcasted in a beacon. If the name is set, the client must know it before being able to join the network. Standard allows for the NN not to be broadcasted, and that is usually known as a "closed system". For example, at the University of Tennessee, network name is set to be "utkwireless" and closed system is applied. It is worth noting that this name is easily visible to the user – client software shows it with a few keystrokes.

WEP is an optional link-layer encryption scheme that offers a mechanism for securing wireless LAN data streams. WEP uses a symmetric scheme where the same key and algorithm are uses for both encryption and decryption of data. WEP has three key goals:

1. Access control: Prevent unauthorized users, who lack a correct WEP key, from gaining access to the network resources.
2. Privacy: Protect WLAN data streams by encrypting them and allowing decryption only by users with the correct WEP keys.
3. Data integrity: Prevent tempering of data by using CRC-32 checksum.

Although WEP is optional, support for WEP with 40-bit encryption key is a requirement for Wi-Fi certification. Most vendors have usually different hardware to support no encryption, 40-bit or extended 128-bit encryption (which is in reality only 104-bit key). WEP is based on RC4 cipher, which was chosen by IEEE because at the time US government did not restrict the export of products using RC4 encryption method. RC4 is still believed to be a secure stream cipher especially if longer key (128-bit) is used.

RC4, like other stream ciphers operate by expanding a secret key (in case of WEP, a public Initialization Vector or IV and a secret key) into an arbitrarily long "key stream" of pseudorandom bits. Encryption is performed by XOR-ing the generated key stream with the plaintext. Before the XOR-ing a CRC-32 checksum is attached to the plaintext. Decrypting consists of generating the identical key stream based on the IV and secret key and XOR-ing it with the cipher text. Checksum is also verified.

Some vendors, like Cisco, use hardware accelerators to minimize the performance degradation of encrypting and decrypting data streams. Generally, vendors using Intersil chipset suffer only about 2% performance loss, while vendor products using lucent chipset show 15-20% performance degradation measured by useful data rate.

WEP is usually implemented with up to four keys, which are shared by all stations, both clients and access points. A client with the default keys can communicate securely with other stations in the subsystem. It is also possible to set one key to be a transmit key, the other one to be a receive key. It is optional to have clients with 40-bit and 128-bit keys simultaneously, but access point must use the lower (40-bit) key when transmitting to insure that 40-bit client can decrypt messages. Also, since WEP is only optional, most access point can simultaneously support clients who opt for WEP and ones who send data in plain, i.e. unencrypted. There is also an option to allow only clients with WEP enabled – "full-encryption" or "deny non-encrypted data" options.

Some vendors allow for WEP keys to be stored hidden within OS ("security by obscurity"), while others allow for keys to be stored in the PC card non-volatile memory. For example, Cisco claims that these WEP keys are write-only, i.e. cannot be read form the card and has provided a password protected client software for changing the key. However, client software reinstallation resets this password to a well-known default. Cisco also allows volatile keys that have to be entered upon the client power-up.

Before a client is allowed to "join" the network a client must be authenticated. There are two mechanisms for that:

- Open authentication

This is a default authentication method and the whole process is done in clear-text. There are two steps to the authentication. First client sends an authentication management frame containing client identity. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.

- Shared key authentication

This type of authentication assumes that each station has received a secret shared key through a secure channel independent of the 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of shared key authentication requires implementation of encryption via the WEP algorithm. Access point sends the client a challenge packet that the client must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, it will fail the authentication and will not be allowed to associate with the access point ("join the network").

Some wireless vendors like Avaya (formerly Lucent) allow authentication based on the MAC address of the client via a central RADIUS server or based on an Access Control List on the access point. However, almost all clients have in software an easy option to set their MAC to a desired one.

5.4 Security Features of Wireless LANs

A message traveling by air can be intercepted without physical access to the wiring of an organization. Any person, sitting in the vicinity of a WLAN with a transceiver with a capability to listen/talk, can pose a threat. Unfortunately, the same hardware that is used for WLAN communication can be employed for such attacks. To make the WLANs reliable the following security goals were considered:

- Confidentiality
- Data integrity
- Access control

The following security measures are a part of the 802.11 IEEE protocol:

- Authentication

- Association

- Encryption

The need of a client to be mobile brought in the separation of authentication and association processes. Since a client frequently changes AP boundaries, he can be authenticated to various AP at a given point, yet remains associated to his chosen one. Before a client gets associated to other, he must be first authenticated.

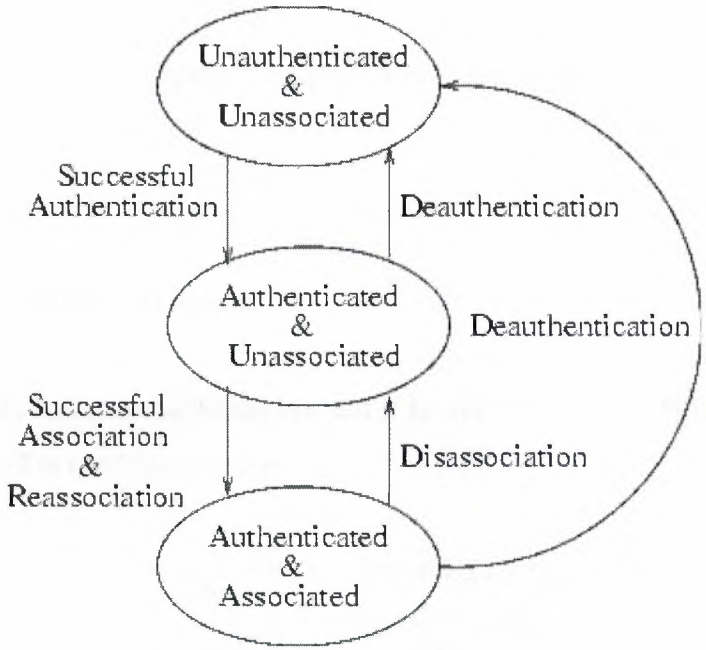

Figure 5.2 Authentication & Association

5.5 Authentication

802.11 specify two authentication mechanisms:

1. Open system authentication

2. Shared key authentication

- Open system authentication

A client needs an SSID for successful Association. Any new client that comes in an EBSS areais provided with an SSID. This is equivalent to no security.

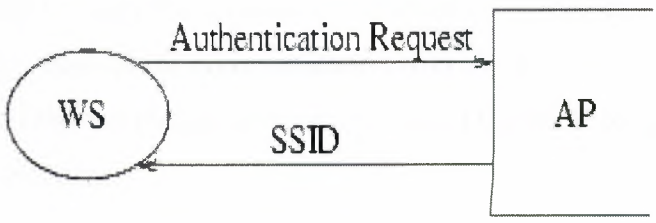

Figure 5.3 Open System Authentication

- Shared system authentication

The client cannot authenticate himself if he doesn't have the WEP shared secret key. WEP protocol is used for encryption.

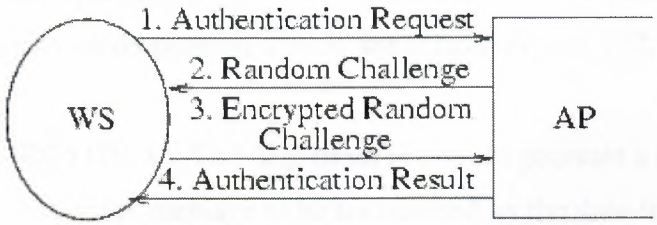

Fig 5.4: Shared key authentication

5.6 Association

An SSID is used to differentiate two networks logically. To successfully associate to a WS, one must have the SSID of the other WS. This was not intended to be a security feature, and in fact SSID is sent in open in the beacon frame of the AP.

5.7 Encryption and Decryption-The WEP Protocol

The WLAN administrator has an option (if the administrator decides to send the packets Unencrypted to make all the communication over the air encrypted, i.e. every frame that is below the Ethernet Header is encrypted using the WEP protocol. The WEP protocol has three components:

1. A shared secret key, k (40bit /104 bit): The fact that the secret key is shared helps reduce the load on AP, while simultaneously assuming that whoever is given the secret key is a trusted person. This shared key is never sent over the air.802.11 doesn't discuss the deployment of this key onto Work Stations. It has to be installed manually at each WS/AP. Most APs can handle up to four shared secret keys.

2. Initialization vector, IV (24 bit): IV is a per-packet number that is sent in clear over the air. This number is most effective if generated randomly, because it is used as one of the inputs to the RC4 algorithm. 802.11 don't specify generation of IV. In fact, many cards generate IVs in linear fashion, i.e., 1, 2, 3...

3. RC4 algorithm, RC4 (IV, k): This algorithm is used to generate a key stream K, length equal to that of the message to be transmitted by the data-link layer. It takes the IV and k as inputs

5.8 Known Attacks on WEP

WEP is considered to be very vulnerable to attackers. Any attacker sitting in the parking lot of a building can attack the building's WLAN security. This is unlike the wired case where by the attacker needs a physical access to the wires. The following known attacks have been employed on WEP.

5.8.1Type of Attacks

The following known attacks are known to be effective:

- Passive Attacks
    1. Dictionary based attacks
    2. Cracking the WEP key

- Passive Attacks
    1. Authentication Spoofing
    2. Message Injection
    3. Message Modification
    4. Message Decryption
    5. Man in the Middle Attack

As with other networks, the active attacks are riskier but provide greater powers to the attacker.

Passive Attacks	Active attacks
No risk involved	Riskier
No need to be the part of networks, because the WLAN cards support monitor mode, whereby one can listen to the communication without being a part of the network	The attacker has to first get into the network, before doing damages
The attacker can only listen to whatever is going on. He can not fiddle with the network	The attacker can interrupt, hijack and control the network at his will

Table 5.1 passive attacks vs Active attacks

- **Authentication Spoofing**

This attack is another form of Message Injection. By sniffing the shared key authentication process, the attacker knows a pair of Plaintext (Random Challenge) and Cipher text (Challenge Response) and the corresponding IV. Thus he knows the required <IV, K> pair. This pair can be used for authentication purposes.

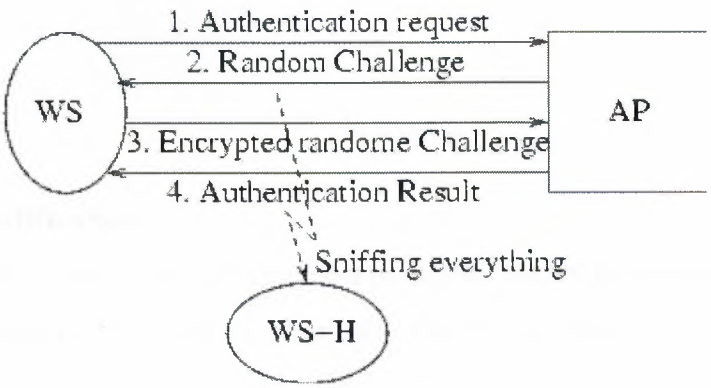

Figure 5.5 Authentication Spoofing

- **Message Injection**

The attack assumes that the attacker has a pair of K, IV. This pair can be reused over and over again without arousing suspicions, because there is no mechanism to check continuous repetition of IVs. Again the fact that CRC (M) is an unkeyed function of M.

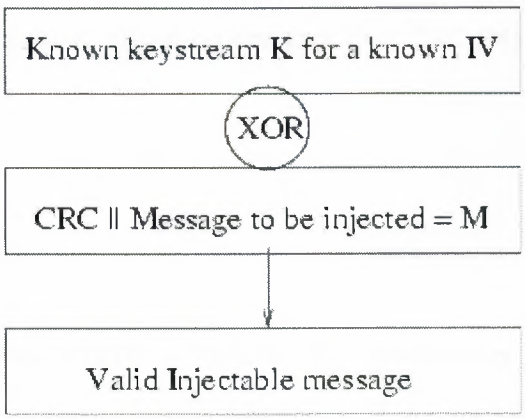

Figure 5.6 Message Injection

- **Message Modification**

This active attack is used to change a particular part of the message M that is known to the attacker, along with its position in the packet. This field can be an email ID, HTML form.

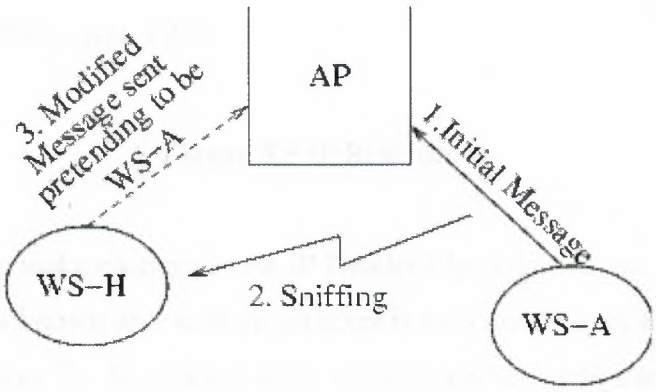

Figure 5.7 Message Modification

The attacker doesn't need to have the knowledge of key stream K or the secret key k for the attack. The attack is based on the fact that CRC (M) is an unkeyed function of M

- **Message Decryption**

There are two methods of decrypting the message by active attacks.

1. IP Redirection
2. Reaction Attack

- **IP Redirection**

This attack is an extension to message modification. The attacker modifies the destination IPin the IP header of the packet. By doing this, the attacker sends a packet from WEP encrypted zone to No WEP zone, where he holds a machine.

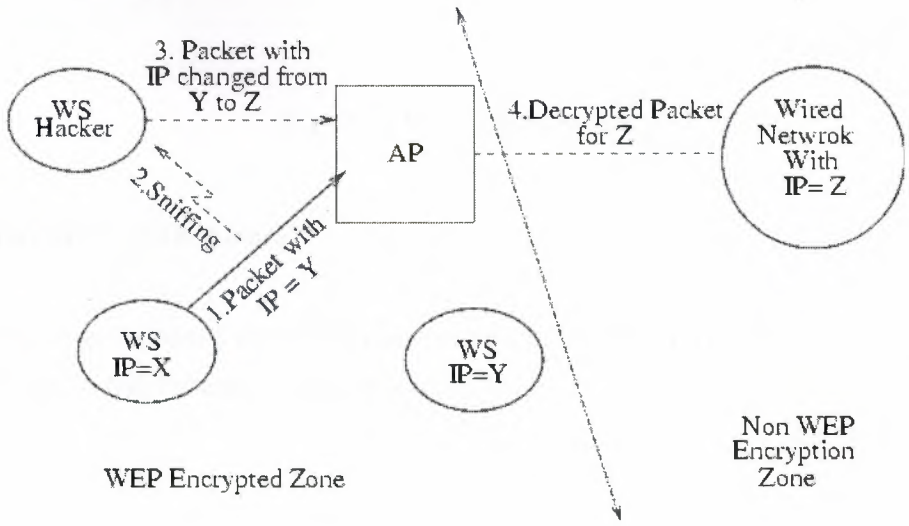

Figure 5.8 IP Redirection

To do this he has to make changes in the IP Header Checksum. In most cases the initial IP Checksum is not known although the attacker is assumed to have the initial destination IP address. So the attacker keeps sending packets with various values of checksum till he gets the packet across to his machine in No WEP Zone.
We did a simulation of this attack. The number of packets required, as a function of initial and final destination IPs, before getting a hit is open for interpretation.

- **Reaction Attack**

This attack only works for TCP Packets. If TCP checksum is valid w.r.t. to the checksum, an ack is sent, otherwise the packet is dropped silently. This attack is based on the receiver's willingness to decrypt arbitrary cipher text and feed them to another component of the system that leaks a tiny bit of information about it's inputs. The attack is rightly called reaction attack as it works by monitoring the recipient's reaction to our forgeries.

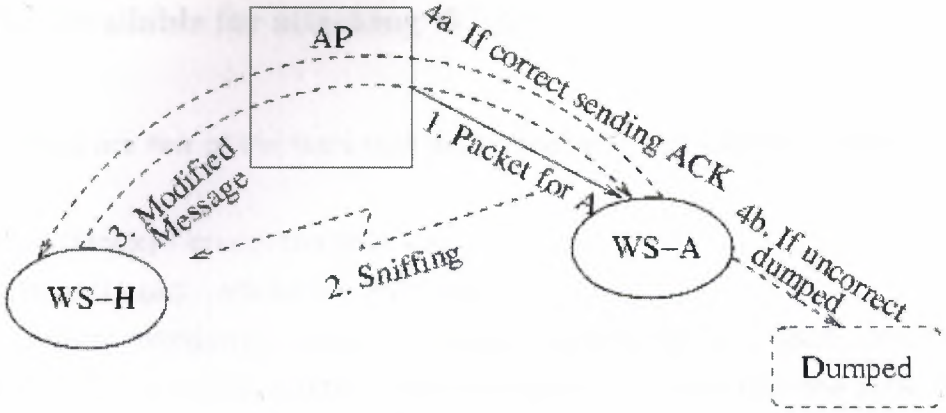

Figure 5.9 Reaction Attack

- **Man in the Middle Attack**

This is a standard attack employed on all sorts of networks. In WLANs, the attack works in the following fashion.

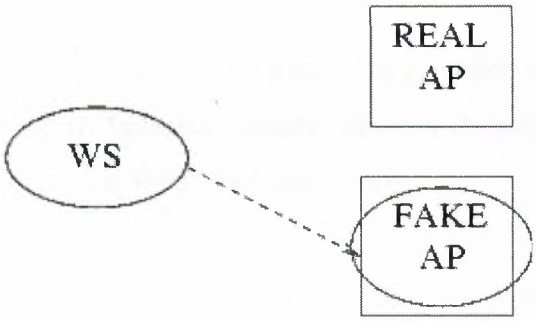

Figure 5.10 Man in the Middle Attack

Steps in Man in Middle attack:

1. The attacker sets up a fake AP near to existing AP using a WS to masquerade network logons.
2. The user connects, in error, to the fake AP, and enters username and password.
3. The intruder collects data and informs user of incorrect password, then sleeps for five minutes, and successfully logs on to the real AP.

5.9 Tools available for attacking WLANs

These are few of the tools that are available for attacking the WLANs:

1. Airsnort (Linux) - cracks the WEP key.
2. WEPCrack (Linux) - cracks the WEP key.
3. NetStumbler (Windows) - finds the network parameters like, SSID, Channels, MACAddresses, Type of Encryption used, Vendor of the card, tells the default secret key of the vendor can be used with a GPS for locating APs.
4. Kismet (Linux) - a WLAN sniffer
5. Thc-Wardrive (Linux) - for war driving
6. dsniff (Linux) - counterpart of NetStumbler
7. dstumbler (FreeBSD) - counterpart of NetStumbler

5.10 So, our WLAN is secure, right?

The idyllic picture of security provided for WLANs lasted for years. Not really! In addition to fallacies already mentioned, administrators were immediately aware of some issues that WEP does not resolve.

First, some people had impression that WEP encrypts data end-to-end, not understanding that WEP is only a first-hop encryption solution. Once data is decrypted on the access point it keeps flowing through the Ethernet un-encrypted. And with that come all insecurities that Ethernet brings. However, everybody was immediately aware that stolen hardware means unauthorized user can easily join and sniff data on the network. Also, since it is based on a shared key, all users associated on the same access point can sniff each other's data. Access point is just a wireless hub, not a switch.

From the management side, it is a nightmare to distribute safely all WEP keys to users. For example, UT started a full-encryption model, but then lowered to optional encryption to accommodate Apple users. Apple as an early adopter of the technology opted that user has to login to the WLAN with login name equal to Network Name and password, which is hashed plaintext alphabet key, every time he/she wants to join the

WLAN. Since the keys were hexadecimal, it was impossible for Mac users to join, plus even if keys were alphabetical they would have to be known to individuals and that is not secure. Apple has only one WEP key, as opposed to usual choice of four WEP keys. Still, in a non-Apple environment, if properly administered, WEP was thought to be a secure enough solution.

5.11 Conclusion

Demand for wireless access to LANs is growing due to a rapidly increasing number of mobile devices, such as laptops and PDAs. Users want untethered network access at all times and everywhere. WLAN is a solution that is very attractive to satisfy needs of such users. Due to the fact that data are transmitted through such an open medium, special measures need to be put in place to insure data security and integrity. Current widely deployed 802.11b standard was shown to have significant security flaws in its implementation. Vendors have already put out new solutions to resolve some of the issues with the 802.11standard, but those solutions have been available for only a few months and it is hard to say if they will pass the test of time. Data security in wireless LANs will continue to be an exciting field of research for the scientific community and the wireless industry in general.

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 802.11x 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.

Wireless LAN security has a long way to go. Current Implementation of WEP has proved to be flawed. Further initiatives to come up with a standard that is robust and provides adequate security are urgently needed. The 802.1x and EAP are just mid points in a long journey. Till new security standard for WLAN comes up third party and proprietary methods need to be implemented.

REFRENCES

[1] Tanebaum Andrew S., Computer Networks, 1996

[2] B.Egan (Digital Corp), "Wireless Data Communications" 1995

[3] J.O'Dwyer (Dataquest Inc.), "PC Quarterly Statistics European Overview" 1996

[4] Introduction to IEEE 802.11,

http://www.intelligraphics.com/articles/80211_article.html, 1997,

[5] Overview: Wireless LAN Security,

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm, 2001,

[6] Nikita Borisov, Ian Goldberg and David Wagner: (In) Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2/6/2001,

[7] Cisco: http://www.cisco.com/univercd/cc/td/doc/pcat/ao350ap.htm, 2/2001.

[8] IEEE 802.11 Working Group for Wireless Local Area Networks,

www.grouper.ieee.org

[9] Joel Conover, Wireless LAN Works,

http://www.networkcomputing.com/1113/1113f2full.htm , 2000.

[10] Wireless Standard

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless Overview-Some Wireless LAN standards.htm

[11]. L.M.S.C. OF THE IEEE COMPUTER SOCIETY. Wireless LAN Medium Access Control

(MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE std. 802.11, 1999 edition.

[12] Fluhrer, Mantin, Shamir. Weakness in the key-scheduling algorithm of RC4.

[13] Stubblefield, Ioannidis, Rubin. Using the Fluhrer, Mantin and Shamir attack to break WEP.

[14] Borisov, Goldberg, Wagner. Intercepting Mobile communications: The Insecurity of 802.11 - Draft.

[15] http://airsnort.shmoo.com