NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE SECURITY ASPECTS OF WIRELESS LOCAL AREA NETWORK (WLAN)

by

Thoetsak Jaiaree

September 2003

Thesis Advisor:	Norman F. Schneidewind
Second Reader:	Douglas E. Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: The Security Aspects of Wireless Local Area Network (WLAN)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Thoetsak Jaiaree			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Wireless Local Area Networks (WLAN) are increasing in number in both home and business uses due to the convenience, mobility and affordable prices for wireless devices. Wireless technology allows the mobile stations to freely move within the range of Access Points without being physically connected to the wired network. Ideally, the WLAN gives mobility and flexibility to users in homes and hot spot environments, such as airports and campuses.

However, WLANs have serious security problems because the wireless signal of the WLAN is broadcast through the air in all directions simultaneously. An unauthorized user can easily capture this signal using freeware tools to exploit WLAN vulnerability.

This thesis provides an introduction to WLAN technology, security vulnerabilities in the WLAN, and the recommended countermeasures for the Software Metrics Laboratory in Ingersoll 158, in the Naval Postgraduate School, with particular emphasis on security concerns for the implementation of the WLAN extension to the existing wired LAN.

14. SUBJECT TERMS Wireless Local Area Networks (WLAN), WIFI (802.11b), Access Point, WLAN Security			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE SECURITY ASPECTS OF WIRELESS LOCAL AREA NETWORK (WLAN)

Thoesak Jaiaree
Captain, Royal Thai Army
B.S., Chulachomklao Royal Military Academy, Thailand, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2003

Author: Thoetsak Jaiaree

Approved by: Norman F. Schneidewind
Thesis Advisor

Douglas E. Brinkley
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Wireless Local Area Networks (WLAN) are increasing in number in both home and business uses due to the convenience, mobility and affordable prices for wireless devices. Wireless technology allows the mobile stations to freely move within the range of Access Points without being physically connected to the wired network. Ideally, the WLAN gives mobility and flexibility to users in homes and hot spot environments, such as airports and campuses.

However, WLANs have serious security problems because the wireless signal of the WLAN is broadcast through the air in all directions simultaneously. An unauthorized user can easily capture this signal using freeware tools to exploit WLAN vulnerability.

This thesis provides an introduction to WLAN technology, security vulnerabilities in the WLAN, and the recommended countermeasures for the Software Metrics Laboratory in Ingersoll 158, in the Naval Postgraduate School, with particular emphasis on security concerns for the implementation of the WLAN extension to the existing wired LAN.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere thanks to Professor Norman Schneidewind and Professor Douglas Brinkley for their advice during the research and completion of this thesis. I would also like to thanks Chye Bin Tay for the future work recommendations from his thesis. Finally, I would like to dedicate this work to my father and mother who have passed away. Additionally, I extend special thanks to my family that includs Col Suwan Jaiaree, Winate and Wilailak Tapapsanan, and Piengkamol Kraidej, who have always motivated and supported my efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. WIRELESS LOCAL AREA NETWORKS

Wireless technologies are becoming more popular in business and personal life than in the past. Wireless communications offer organizations and users many benefits, such as increased portability, flexibility, and productivity. The Wireless Local Area Network (WLAN) does not replace the wired infrastructure, but complements it and significantly increases its range and flexibility for connecting a wireless device (e.g., laptop, PDA) to a wired LAN. Today, wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. For instance, WLAN devices allow users to move their laptops from place to place within their office without the need for wires and without losing network connectivity. This results in an increasing number of government agencies, businesses, and home users using, or anticipating the use of wireless technologies in their environments.

Nonetheless, these groups need to be aware of the security risks associated with wireless technologies. They need to develop strategies that help mitigate those risks as they integrate these technologies in their computing environments.

1. Advantages of WLAN Over LAN

Wireless networks allow users to access and share networks without physically connecting to the network, so the existing LANs can be set up to work with a WLAN without installing new wires. This gives the users four primary benefits:

a. User Mobility

Users can access files, network resources, and the Internet without physically connecting to the network with wires. Users can be mobile yet retain high-speed, real-time access to the LAN.

b. Rapid Installation

The time required for installation is reduced because network connections are possible without moving or adding wires, or pulling these wires through walls or ceilings.

c. Flexibility

Users have the flexibility of installing and moving WLANs to any location as needed. Users can also quickly install a small WLAN for temporary use in conferences or meetings.

2. Disadvantages of WLAN Over LAN

Regardless of the benefits of the WLAN environment, there are several serious problems should be addressed prior to deploying a WLAN to supplement a wired system.

a. Electrical Interference

Frequency allocation for Radio Frequency (RF) WLANs present a problem because most spread-spectrum transmissions are in the frequency range established by the Federal Communications Commission (FCC) for Industrial, Scientific and Medical (ISM) usage [Ref 1]. In addition, other products, like microwave devices, transmit energy in the same spectrum that can potentially induce some level of interference. This interference is one of the factors that possibly causes degradation in throughput. Background noise comes from all kinds of sources, but the most prevalent types are caused by ordinary microwave ovens and cordless phones.

b. Quality of Service

WLANs typically offer lower quality than wired LANs. The main reason for this disadvantage is the lower bandwidth due to limitations in the radio transmission (only 1-11 Mbit/s), higher error rates due to interference, and longer delays due to multipath propagation. Moreover, overhead, configuration, and security factors can reduce the actual throughput to lower than 11 Mbit/s.

c. Slow Throughput Rate

Factors that affect throughput include airwave congestion (number of users), propagation factors such as range and multipath transmission, as well as the latency and bottlenecks on the wired portions of the WLAN. The common throughput rate for a WLAN is up to 11Mbps for the 802.11b and 54 Mbps for the 802.11a and the 802.11g; whereas, for a typical wired LAN, a throughput rate of up to 100Mbps is possible. Hence, a WLAN is suitable when dealing with text files or e-mail files.

However, if the use of multimedia graphics and sound is essential, a wired LAN is currently still the better choice.

d. Higher Initial Cost

The initial cost for a WLAN is more expensive than that of a wired LAN. The infrastructure costs depend primarily on the number of Access Points (APs) deployed, where the number of necessary APs typically depends on the required coverage area and/or the number and types of users to be serviced.

e. Security

The WLANs send their traffic over shared space, airwaves. This introduces interference from other traffic and the need for additional security. The open radio interface and several hundred feet of transmission distance make eavesdropping much easier than with a wired LAN. This unsecured area allows an unauthorized person to gain access to a network from outside a building or home. Even though some encryption protocols are implemented in WLANs, such as Wired Equivalent Privacy (WEP) to increase security, some anti-WEP technologies have been developed to break the encryption. In other words, WEP can be broken by skilled intruders who have the time and sufficient motivation to penetrate a network.

B. PROBLEM STATEMENT

In any wireless technology, some risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. The most significant difference, the main source of these risks, is that with wireless networks the organization's underlying communications medium, the airwave, is openly exposed to intruders, making it easier to be attacked by malicious hackers and unauthorized users. This thesis identifies vulnerabilities in WLANs and proposes methods to prevent these vulnerabilities. Administrative security and the protection of data should be considered during initial system planning.

C. THESIS OVERVIEW

Chapter II of this thesis surveys various technologies, topologies and standards used to build a WLAN. The known vulnerabilities of IEE 802.11b and WLAN in

Software Metrics Lab (SML) will be discussed in Chapter III. The methods to secure a WLAN in SML are explored in Chapter IV. Chapter V concludes with recommendations for securing WLANs.

II. BACKGROUND

Wireless technologies enable one or more devices to communicate without network cabling. Wireless technologies use radio transmissions as the means for transmitting data while wired technologies use cables. Wireless technologies range from complex systems, such as WLANs and cell phones, to simple devices, such as wireless headphones and microphones that do not process or store information. In addition, wireless technology includes Infrared (IR) devices like remote controls, some cordless computer keyboards and mice, and wireless Hi-Fi stereo headsets. These devices require a direct line of sight between the transmitter and the receiver to transmit on the link. This chapter presents a brief overview of the critical elements of wireless technology, wireless networks, and wireless standards.

A. WIRELESS NETWORKS

Wireless networks serve to transport information between wireless devices and between wireless devices and wired networks. Wireless networks are diverse; however, they are frequently categorized into three groups based on their coverage range: Wireless Wide Area Network (WWAN), Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN) [Ref 2]. The range of a WWAN includes wide coverage area technologies, such as 2G Cellular, Cellular Digital Packet Data (CDPD), and Global System for Mobile Communications (GSM). The range of a WLAN includes 802.11, Hyperlan, and several others, while a WPAN includes Bluetooth and Infrared. All of these groups receive and transmit information using Electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the Radio Frequency (RF) band up to and beyond the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 Kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of Gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. (See Appendix A for a list of common wireless frequencies.) Since wireless network and technology are so diverse, the primary focus in on WLAN technologies, which would be employed in SML (Ing 158)

1. WLANs

WLANs allow greater flexibility and portability than wired LANs. Unlike a traditional LAN, which requires wires to connect a user's computer to the network, a WLAN connects computers and other components to the network by using an AP device. An AP communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. The AP device typically covers areas of up to 300 feet (100 meters) [Ref 3]. This coverage area is called a cell or range. Users can move freely within the cell with their laptops or other network devices. As shown in Figure 1, the AP cells can be linked together to allow users to "roam" even within a building or between buildings.

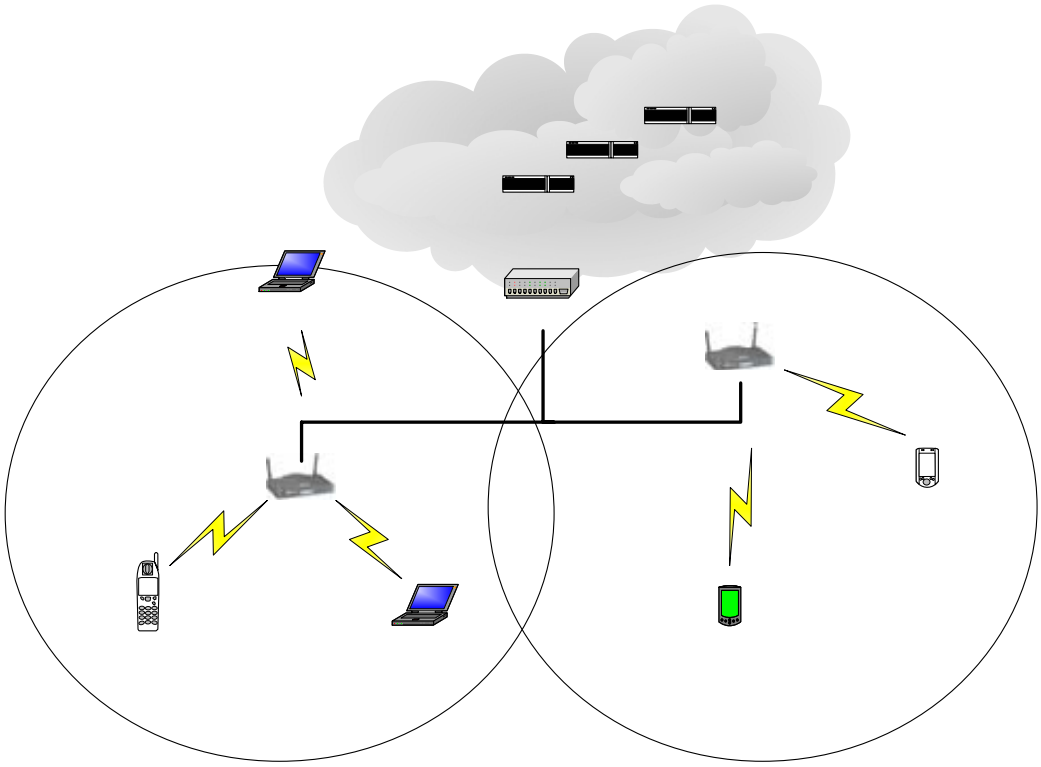

Figure 1. The WLAN Topology (From: Ref 2)

2. Ad Hoc Networks

In Ad Hoc networks, each mobile device communicates directly with other mobile devices within the network. No existing APs connect the Ad Hoc network directly with any wired LAN. The Ad Hoc mode is designed so that only the mobile stations

within transmission range (within the same cell) can communicate with each other without the associated AP as shown in Figure 2. If a mobile station in an Ad Hoc network wants to communicate outside of the cell, a member of the cell must operate as a gateway and perform a routing service [Ref 4]. While WLANs use a fixed network infrastructure, Ad Hoc networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. In a Bluetooth network, mobile routers control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured simultaneously to handle the dynamic topology. The routing protocol Bluetooth allows the routers to establish and to maintain these shifting networks.

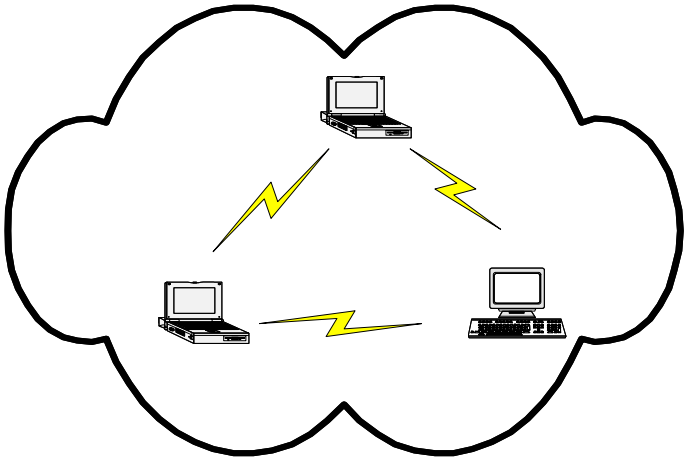

Figure 2. Ad Hoc Network (From: Ref 2)

B. WLAN INFRASTRUCTURE

A typical WLAN is set up as an extension of the existing corporate network, as shown in Figure 1. This enables mobile devices to remain connected to the wired network while mobile devices are moved. A basic WLAN configuration includes the following components:

1. Access Point (AP)

An AP is a router that enables wireless devices to access the wired network. The APs are usually placed outside the firewall to facilitate convenient access, but this also makes them vulnerable to attacks. In addition, APs support specific WLAN types, such as 802.11b. A Dual-band AP, which supports both 802.11b and 802.11a WLANs, is also available.

2. Mobile Device

Mobile Devices include laptops, Personal Digital Assistants (PDAs), Tablet PCs and other similar mobile devices. However, unless these remote devices are configured with wireless network capability, they cannot access a WLAN.

3. Wireless Network Interface Cards (NICs)

Wireless Network Interface Cards (NICs) enable mobile devices to communicate with the AP using radio frequency transmissions [Ref 2]. Each card has a unique Media Access Control (MAC) address, which can be used for authentication purposes. The wireless NIC must be compatible with the AP. For example, an 802.11b AP must be used with a 802.11b Wireless NIC. Dual-mode NICs, similar to dual-mode APs, are also available.

4. Security Server

A Security Server enforces and manages security policies to ensure that wireless users have access to the appropriate information on the corporate network while preventing threats from intruders. The server is a centralized security system for restricting access to resources. A Security Server replaces the security functions in individual applications with a centralized system, allowing simpler administration and management of secured functions. Instead of implementing changes in security policy from one workstation to another workstation, administrators can make changes in one location for all users in the network. This capability protects their system logic and data from unauthorized use.

C. WIRELESS STANDARD

Wireless, at its current relatively immature state, has a variety of standards. The principal advantages of standards are to encourage mass production and to allow products

from multiple vendors to communicate. The Advanced Mobile Phone System (AMPS) standard, which dominated first generation mobile telephone devices [Ref 2], allows devices from various manufacturers to work on a wireless network infrastructure developed by other manufacturers. The AMPS standard uses Frequency Division Multiple Access (FDMA) and requires a lot of bandwidth while operating in the 824–829MHz range (similar to FM radios). Other telephony standards include IS-136, a Time Division Multiple Access (TDMA) standard, IS-95, a Code Division Multiple Access (CDMA) standard, and Global System for Mobile (GSM), which is another TDMA standard. Many handheld devices (e.g., PDAs and cell phones) have followed the Wireless Application Protocol (WAP) standard, which provides secured access to e-mail and the Internet. All of these standards are different and offer varying levels of security features. For this thesis research, the discussion of wireless standards is limited to the IEEE 802.11 standard.

1. IEEE 802.11

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) approved the 802.11 WLAN standard [Ref 5], establishing a global standard for implementing and deploying WLANs. The throughput for 802.11 was 2Mbps, which was well below the IEEE 802.3 Ethernet counterpart. Late in 1999, the IEEE approved the 802.11b standard extension, which raised the throughput to 11 Mbps [Ref 5], making this extension more comparable to the wired networks. The 802.11b also supports the 2 Mbps data rate and operates on a 2.4GHz band radio frequency for high-speed data communications.

As with any of the other 802 networking standards (Ethernet, Token Ring, etc.), this 802.11 specification affects the lower layers of the Open Systems Interconnect (OSI) reference model, and the Physical and Data Link layers [Ref 6] as shown in Figure 3. The Physical Layer defines how data is transmitted over the physical medium. The IEEE assigned 802.11 two transmission methods for Radio Frequency (RF) and one for Infrared (IR) [Ref 7]. The two RF methods are Frequency Hopping Spread-Spectrum (FHSS), which operates within the Unlicensed National Information Infrastructure (UNII) and Direct Sequence Spread-Spectrum (DSSS), which operates within the ISM (Industrial, Scientific, and Medical) 2.4 GHz band for unlicensed use [Ref 8]. Other devices that operate on this band include remote phones and microwave ovens.

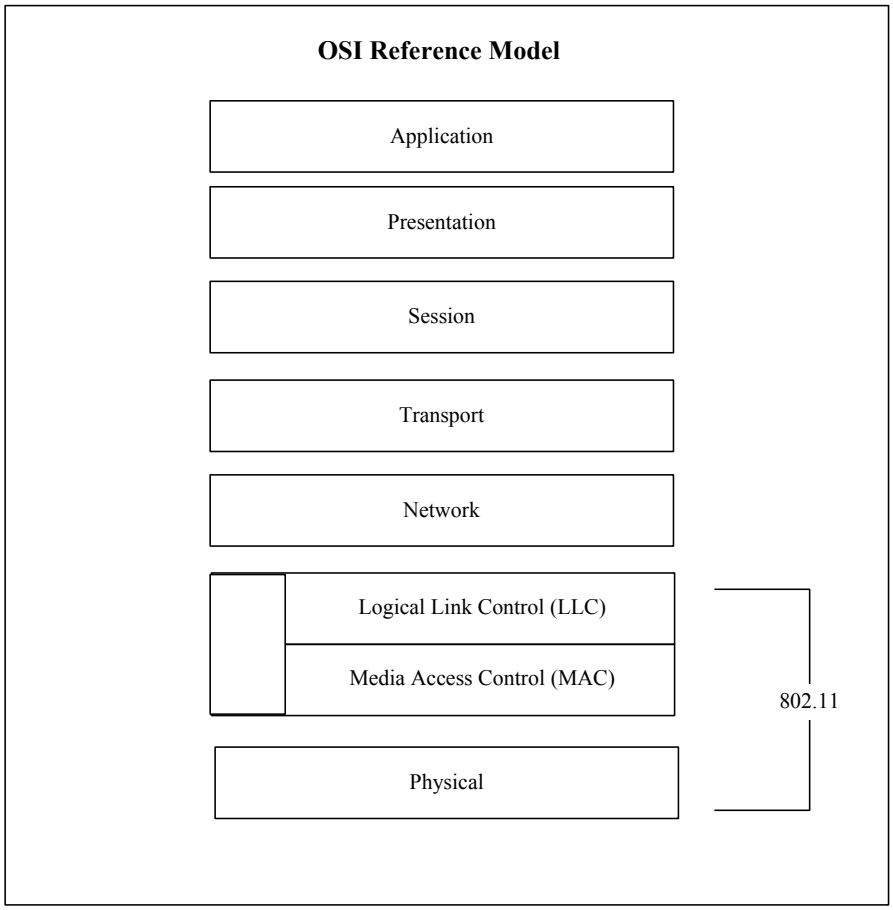

Figure 3. Open Systems Interconnect (OSI) Reference Model (From : Ref 4)

Both FHSS and DSSS are different techniques to transmit data over radio waves. For FHSS, a simple frequency hopping technique is used to navigate the 2.4GHz band, which is divided into 75 sub-channels of 1MHz each [Ref 5]. The sender and receiver negotiate a sequence pattern over the sub-channels.

On the other hand, DSSS utilizes the same channel for the duration of the transmission by dividing the 2.4 GHz band into 14 channels at 22MHz each with 11 channels, which have eight overlapping and three non-overlapping channels [Ref 5]. To compensate for noise and interference, DSSS uses a technique called "chipping," where each data bit is converted into redundant patterns called "chips."

The Data Link layer is made up of two sub-layers, the MAC layer and the Logical Link Control (LLC) layer [Ref 1]. The Data Link layer determines how transmitted data is packaged, addressed and managed within the network. The LLC sub-layer uses the identical 48-bit addressing found in Ethernet, where the MAC sub-layer uses a unique

mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [Ref 1]. This mechanism is similar to the Carrier Sense Multiple Access Collision Detect (CSMA/CD) used in Ethernet, with a few major differences. As opposed to Ethernet, which detects collisions, CSMA/CA senses the airwaves for activity and sends out a signal when the airwaves appear to be free of transmissions. If the sender detects conflicting signals, it will wait for a random period plus a period proportional to the existing traffic before retrying transmission.

The 802.11 standard includes the RTS/CTS (Request To Send/Clear To Send) function as an optional feature to solve the hidden node problem [Ref 6], in which two stations on opposite sides of an AP can both hear activity from an AP but not from each other. Although the first station may sense the channel to be clear, the second station may in fact be transmitting to the AP. Therefore the collision may occur. This problem occurs when a wall and other structures create obscure radio coverage areas. When this feature is in use, a sending station transmits an RTS packet and waits for a reply from the AP with a CTS packet. Since all stations in the network can hear the AP, the CTS packet causes them to delay any intended transmissions. This allows the sending station to transmit and receive a packet acknowledgement without any chance of collision. However, the RTS/CTS packet adds additional overhead to the 802.11, especially at small packet sizes. It is typically used only on the largest-sized packets, for which retransmission would be expensive from a bandwidth standpoint.

In addition, the 802.11 MAC sub-layer provides other robustness features, Cyclic Redundancy Check (CRC) checksum and packet fragmentation [Ref 2]: a CRC checksum is calculated for each packet to ensure that the data was not corrupted in transit. Packet fragmentation makes it possible to split large packets into smaller packets before transmitting over the air. This is useful on a crowded transmission, since large packets are more easily corrupted; it also reduces the need to send packets again; this increases the throughput of the network.

a. 802.11a

The 802.11a extension operates on a different physical layer specification than the 802.11b. The 802.11a extension operates at 5GHz and supports data rates up to 54Mbps. The Federal Communication Commission (FCC) has allocated 300Mz of the RF spectrum for unlicensed operation in the 5GHz range [Ref 9]. Although 802.11a supports

much higher data rates, the effective distance of transmission is much shorter than 802.11b. Additionally 802.11a is not compatible with 802.11b equipment and, in its current state, is usable only in the United States. However, several vendors have embraced the 802.11a standard, and some have dual band support AP devices and network cards.

b. 802.11b

The 802.11b extension is currently the de facto standard for WLANs; it raises the data rate from 2Mbps to 11Mbps by using the 2.4 GHz frequency band, but the actual throughput is much less. The increased data rate from 2Mbps to 11Mbps is achieved by utilizing an advanced encoding technique called Complementary Code Keying (CCK) [Ref 9]. The CCK uses Quadrature Phase Shift Keying (QPSK) for modulation to achieve the higher data rates.

c. 802.11c

The 802.11c extension provides required information to ensure proper bridge operations by using 802.11 APs to bridge across networks within relatively short distances from each other. This project has been completed with related procedures as part of the IEEE 802.11c standard. Product developers utilize this standard when developing APs.

d. 802.11d

The 802.11d extension was introduced to facilitate the worldwide use of 802.11. It has an ongoing charter to define PHY requirements that satisfy regulatory requirements within additional countries. This extension allows APs to communicate on the permissible radio channels with acceptable power levels for user devices. Since the 802.11 standards are not legal in some countries, the purpose of 802.11d is to add features and restrictions that allow WLANs to operate within the rules of these countries. In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Moreover, since equipment manufacturers do not want to produce a wide variety of country-specific products and mobile users do not want to carry full country-specific WLAN PC cards, the result is country-specific firmware solutions. The standard was completed in 1999.

e. 802.11e

The 802.11e extension is a supplement to the MAC layer that provides Quality of Service (QOS) support for LAN applications. This extension will apply to 802.11 physical standards a, b and g. The purpose of this extension is to provide classes of service with managed levels of QOS for data, voice and video applications. Many WLAN manufacturers have targeted QOS as a feature that differentiates their products from others. Therefore many proprietary offerings will be available before 802.11e is complete, which is still in the developmental stage.

f. 802.11f

The 802.11f extension is designed to achieve AP interoperability within a multivendor WLAN network. This reduces vendor lock-in and allows multivendor infrastructures. This standard defines the registration of APs within a network and the interchange of information between APs when a user is handed over from one AP to another. Like 802.11e, 802.11f is still in the standard developmental stage.

g. 802.11g

The 802.11g extension offers wireless transmission over relatively short distances at speeds from 20 Mbps up to 54 Mbps. It operates in the 2.4GHz and 5GHz radio band ranges. The 802.11g standard uses Orthogonal Frequency-Division Multiplexing (OFDM) modulation [Ref 9]. However, for backward compatibility with 11b, it also supports Complementary Code Keying (CCK) modulation and, as an option for faster link rates, allows Packet Binary Convolutional Coding (PBCC) modulation. The 802.11g extension is still in the standard developmental stage.

h. 802.11h

The 802.11h extension is supplementary to the MAC layer to comply with European regulations for 5GHz WLANs. European radio regulations for the 5GHz band require products to have Transmission Power Control (TPC) and Dynamic Frequency Selection (DFS) [Ref 10]. This feature, TPC, limits the transmitted power to the minimum needed to reach the farthest user while DFS selects the radio channel at the AP to minimize interference with other systems, particularly radar. This extension is still in the standard developmental stage.

i. 802.11i

This extension focuses on enhancing WLAN security and on authenticating the 802.11, which includes Remote Authentication Dial-In User Service (RADIUS), Kerberos, and network port authentication (IEEE 802.1x). The 802.11i will apply to 802.11 physical standards a, b and g and will provide an alternative to Wired Equivalent Privacy (WEP), with new encryption methods and authentication procedures. This extension is still in the standard developmental stage, but it is expected to be approved in September 2003.

2. Bluetooth

Bluetooth is a simple peer-to-peer protocol created to connect multiple consumer mobile information devices (cellular phones, laptops, handheld computers, digital cameras, and printers) without wire connection. It uses the IEEE 802.15 specification in the 2.4 to 2.5 GHz band with FHSS technology [Ref 2]. Bluetooth enables mobile devices to avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet.

Bluetooth is a low-power-consuming technology with transmission distances of up to 30 feet and a throughput of about 1 Mbps. The range is extended to 300 feet by increasing the transmit power to 100 mW (milli Watt). It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band.

D. THE APPLICATION OF THE WLAN IN A SOFTWARE METRICS LABORATORY (ING 158)

This lab provides hands-on instruction in computer networks and software engineering. It is also used for faculty research and for student thesis research in computer networks, and in software metrics and reliability. The lab supports the following courses: Software Design (IS3020), Computer Networks: Wide Area and Local Area (IS3502) and Software Reliability (SW4581).

1. Existing LAN

The SML is divided into two compartments, Segment 1 and Segment 2. Segment 1, closer to the entrance, consists of twelve workstations while Segment 2 consists of eight workstations and one server. The SML is equipped with two 16-port Ethernet switches – one for each segment. These 16-port Ethernet switches are connected to a 3com Ethernet switch (running at 155 Mbps on its output) via a Cat 5 cable and a Patch Panel as shown in Figure 4.

Transmission Control Protocol/Internet Protocol (TCP\IP) is a protocol suite used in the Internet that provides application programs with access to a connection-oriented communication service. A Domain Name Server (DNS) is an automated system used to translate computer names into equivalent IP addresses.

The existing LAN uses static Class B IP addresses, in a range of 131.120.43.111 to 131.120.43.131. Only 21 (20 mobile stations and 1 server) of the 254 IP addresses are used. The IP Address of DNS is 131.120.254.58 and 52; the IP Address of the Server is 131.120.43.123; the subnet address is 131.120.43.x and the subnet mask is 255.255.252.0

The SML has TCP/IP applications, network design, network monitoring, network management and application tools, software design, and software reliability programs installed and distributed throughout the LAN. Examples of the software and network applications employed by the SML are Visio (for network drawings), Telnet, FTP, Traceroute, and Ping. In addition, a Windows NT 4.0 Server is the server operating system, and Microsoft XP and Windows NT 4.0 Workstation are the mobile station operating systems.

2. Planning a WLAN

In order to stay current with the latest advances in networking technologies, SML needs to have both a wired LAN and a WLAN. The WLAN will supplement the existing wired LAN capabilities.

To implement this plan, ten laptops with the Microsoft XP Operating System will be added (five in each segment). This means that ten wireless Network Interface Cards (NIC) will be used for this WLAN. In addition, SML will use the ISM 2.4 GHz band Spread Spectrum for the WLAN by connecting Ethernet Category 5 cables from the AP to the switchs, as show in Figure 5.

Since the static IP addresses in SML ranges from 131.120.43.111 to 131.120.43.254. Of these 254 addresses, only 21 (20 desktops and 1 server) of these are utilized, leaving 233 addresses available to use between the APs and the laptops.

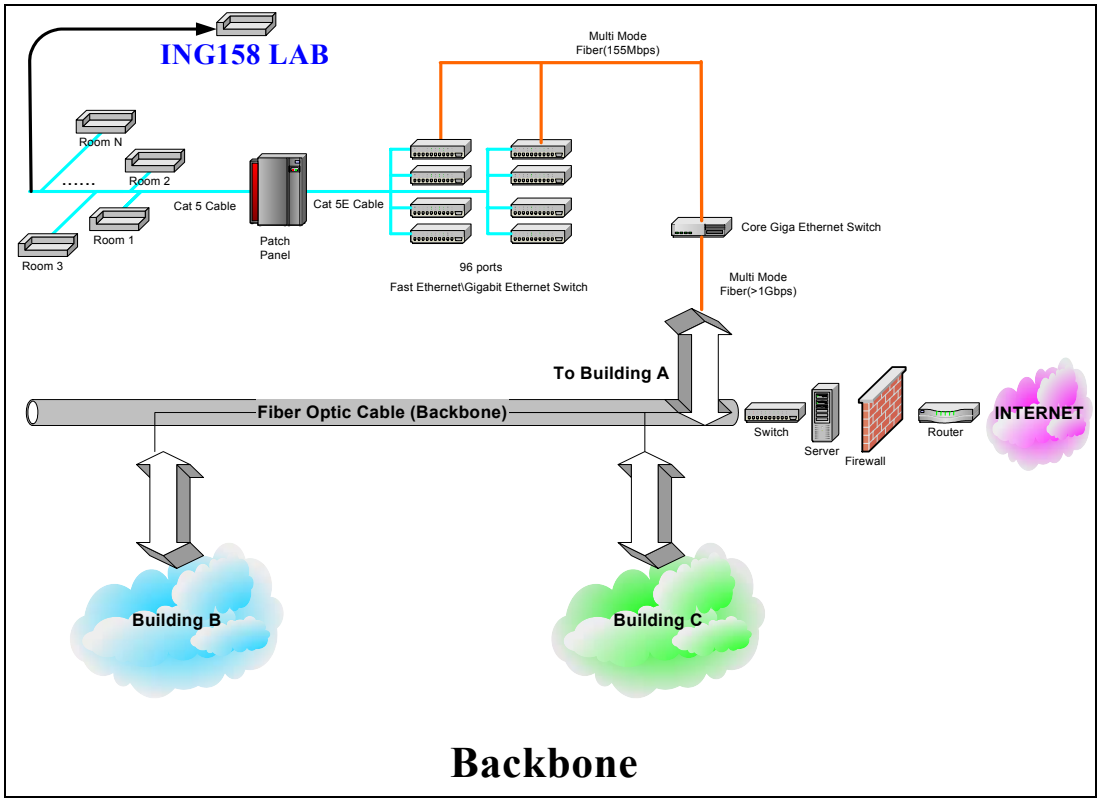

Figure 4. The Connection of SML through NPS Backbone (From: Ref 11)

In order to have the service covered for the entire SML, two APs will be needed for use. The two Cisco Aironet 1200 Series APs (with radius of 300 feet) are planned for the WLAN design, which is adequate for continuous roaming within the space of 400 square feet of the SML area. The Aironet 1200 Series APs will be compatible with both IEEE 802.11a and 802.11b standards. For the SML WLAN design, the IEEE 802.11b standard will be used with speeds up to 11Mbps at 2.4 GHz. The 802.11b standard will be presented in greater detail in Appendix B.

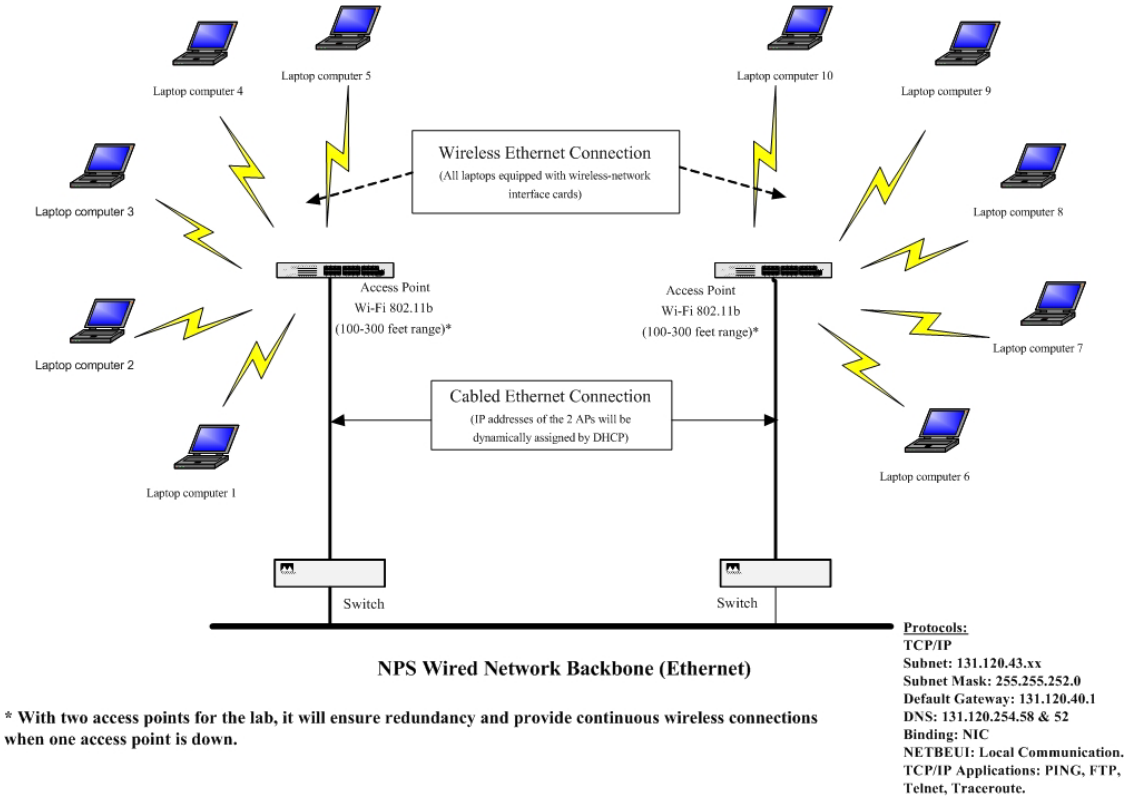

Figure 5. SML WLAN Design Architecture (From : Ref 11)

THIS PAGE INTENTIONALLY LEFT BLANK

III. SECURITY CONCERNS FOR WLAN IN SML

In this discussion, note that a WLAN does not currently exist in the Software Metrics Lab (SML). Thus, the discussion of security concerns is hypothetical (i.e., vulnerabilities that might exist *if* a WLAN were installed in SML).

In a wired LAN, electrical and optical communication is confined to a physical link between the workstations with the wired connection. Traditionally, a firewall attempts to prevent unauthorized access to the network by protecting the workstations and the physical link. The security in a wired LAN is easy to visualize and to understand; on the other hand, WLANs are completely different. Communication is not confined to a physical link, but is broadcasted through the air in all directions simultaneously. Hence, the unauthorized user can easily capture this signal over the air.

Security in a WLAN is important and, as with any wired LAN, should be given a high priority. No wired LAN or WLAN can provide complete security. Despite the various security measures being implemented into the standards, the security issues still remain due to the boundary-less nature of a WLAN. An intruder will likely have more access to the network when attempting to break the security measures. There are many security risks associated with WLAN technologies, so the administrator in SML should have a broad understanding of the various weak points that exist in the WLAN standards. This ensures that informed decisions can be made as to whether this type of technology would ultimately be of benefit in the uses of a WLAN in SML.

A. THE CONCEPTS OF C.I.A.

Confidentiality, Integrity, and Availability (C.I.A.) are three fundamental tenets of the information systems security process [Ref 4]. These three tenets must be considered in the security of a WLAN in SML because this is the first step in identifying potential threats and protection that should be implemented to mitigate and control risk.

1. Confidentiality

Confidentiality is the ability to hide information from unauthorized persons, which means the information is limited to those that need it. Confidentiality is the tenet most often attacked. Cryptography and Encryption methods are attempts to ensure the confidentiality of data transferred from one computer to another.

2. Integrity

Integrity is the ability to ensure that information is an accurate and unchanged representation of the original information. One type of security attack is to intercept some important information and modify it before sending it on to the intended receiver, without both ends knowing that the data had been changed.

3. Availability

Availability is the guarantee that the information is readily accessible to the authorized user when it is needed and that it is ready for use. Some types of security attacks attempt to deny access to the appropriate user, such as the Denial-of-Service (DoS) attack, which tries to bring a network or server down.

B. TYPES OF HACKER

WLAN security is in many ways so weak that people easily exploit it. The combination of low barrier against wireless hackers and available freeware tools permits these hackers to penetrate WLANs easier. Unauthorized users can be divided into four categories [Ref 12]:

1. Accidental Users

Accidental users are just unauthorized users of a WLAN. They are not trying to hack into WLAN, and they might not even know that a WLAN exists

2. Script Kiddies

The term script kiddies refers to people who want to be a hacker but do not have much skill and experience. They simply download some available freeware tools, which they are able to learn how to use. In addition, they are not able to write their own malicious codes.

3. Casual Hackers

Casual hackers are more capable than script kiddies. They know how hacker tools work. These hackers are able to decode a wireless packet log and analyze the wireless packages not for the purpose of stealing, but for entertaining themselves. Although the casual hackers are capable, they will target the easiest WLAN, which has minimal or no security measures implemented.

4. Skilled Hackers

The skilled hackers are capable and determined, since they can be employed by a competitor who wants to break into a network. They can write their own malicious codes, which require patience and insight to exploit cryptographic weaknesses. However, these types of hackers are less numerous than the other types of hackers. When securing a WLAN in the SML, the administrator needs to decide which of these people to keep out.

C. THE HACKER'S WLAN TOOLS

When the new IEEE 802.11 standard has been release, the hackers as well as white hat hackers are eager to experiment with tools to break the security standard. This effort also introduces new and more sophisticated tools for breaking the security standard. This section provides a few examples of these hardware and freeware tools available on the Internet.

1. Available Freeware Tools

New WLAN hacking tools are introduced on the Internet every week, where anyone can download them. Some of these freeware tools, such as WEPCrack and AirSnort, can exploit vulnerabilities in the WEP encryption algorithm [Ref 13]. When breaking the WEP, the WLAN traffic must be captured sufficiently to recognize a repetition pattern and break the encryption key. Administrators need to become familiarized with these tools to know the WLAN's vulnerability posed by these tools. Table 1 shows the freeware tools that are well-known, with websites and a description of each freeware tool.

2. Antennas

Antennas help the hackers receive a stronger wireless signal from longer distances: more than 300 feet. These antennas are either available commercial antennas or homemade antennas, which are built with available material, such as cans or aluminum tubing, as shown in Figure 6 and 7. The later antenna can pick up 802.11 signals from up to 2,000 feet away [Ref 14].

Tool	Web site	Description
NetStumbler	www.netstumbler.com	Freeware wireless AP identifier – listens for SSIDs & sends beacons as probes searching for APs
Kismet	www.kismetwireless.net	Freeware wireless sniffer and monitor – passively monitors wireless traffic & sorts data to identify SSIDs, MAC addresses, channels and connection speeds
Wellenreiter	http://packetstormsecurity.nl	Freeware WLAN discovery tool – uses brute force to identify low traffic APs, hides your real MAC, integrates with GPS
THC-RUT	www.thehackerschoice.com	Freeware WLAN discovery tool – uses brute force to identify low traffic APs, "your first knife on a foreign network"
Ethereal	www.ethereal.com	Freeware WLAN analyzer – interactively browse the capture data, viewing summary and detail information for all observed wireless traffic
WEPCrack	http://sourceforge.net/projects/wepcrack/	Freeware encryption breaker – cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling
AirSnort	http://airsnort.shmoo.com	Freeware encryption breaker – passively monitoring transmissions, computing the encryption key when enough packets have been gathered
HostAP	http://hostap.epitest.fi	Converts a WLAN station to function as an AP (Available for WLAN cards that are based on Intersil's Prism2/2.5/3 chipset)

Table 1. Freeware Tools (From: Ref 14)

Figure 6. The Commercial Antenna (From Ref: 15)

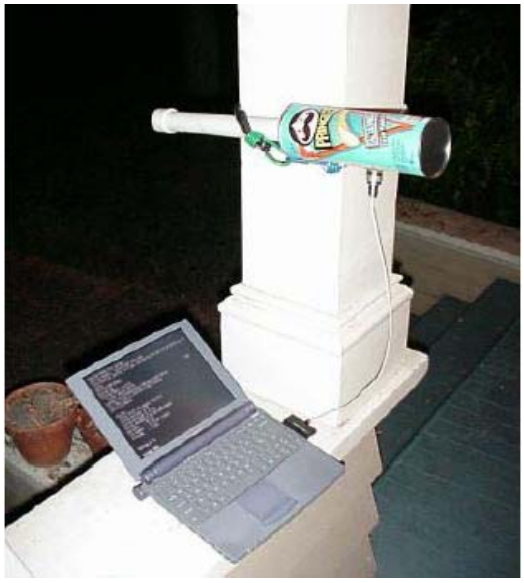

Figure 7. Homemade Antenna (From Ref: 16)

D. TYPE OF ATTACK ON WLAN

A number of security vulnerabilities have unfortunately been discovered in 802.11 by malicious hacker exploits. These security threats to the WLAN can range from relatively harmless free Internet access to malicious intrusion, snooping, interference, destruction of data, and a virus attack. The WLAN may be subject to different kinds of attacks, which are usually divided into two broad categories: passive and active [Ref 2]. Figure 8 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

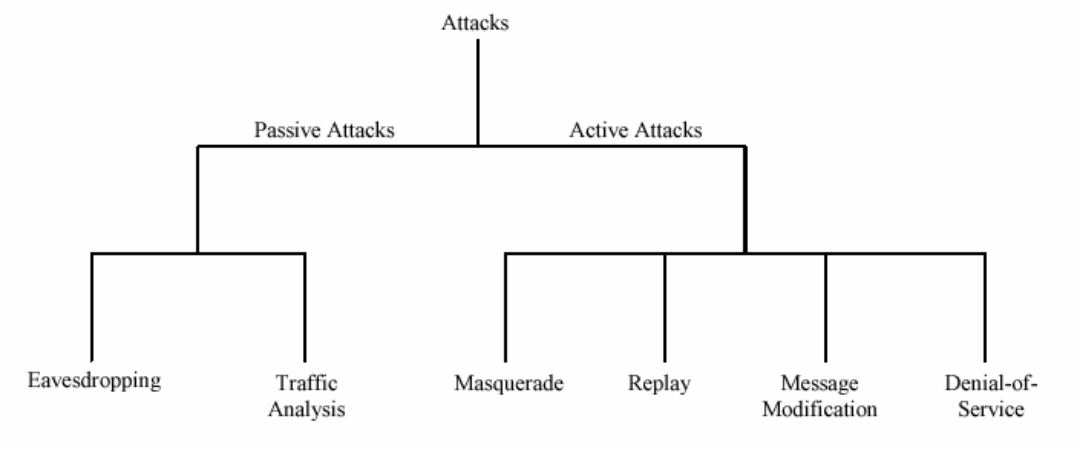

Figure 8. Taxonomy of Security Attacks (From Ref:2)

1. Passive Attack

A passive attack is the method of analyzing the traffic by intercepting and extracting the raw data. The hacker uses a sniffer tool, such as an AiroPeek, to analyze this data. Due to the physical transmitting properties of a WLAN, the traffic can easily be captured at any location as long as the signal reaches the hacker's system. An attack simply gains access to the network but does not modify the data (i.e., eavesdropping). Passive attacks can be either simple eavesdropping or traffic analysis (sometimes called traffic flow analysis) [Ref 2]. These two passive attacks are as follows.

a. Eavesdropping

Eavesdropping is the most obvious threat for a WLAN [Ref 17]. The hackers simply monitor transmissions for message content in real time, since there are no boundaries on the wireless medium to acquire information flowing from a mobile station to the AP. In addition, the hacker can record this message content for future cryptanalysis**.**

b. Traffic Analysis

Traffic analysis is a more sophisticated way than eavesdropping to gain intelligence. The hacker analyzes the traffic by monitoring the transmissions for patterns of communication. The hacker uses this information to gain access to the traffic from each user on the WLAN.

2. Active Attack

An Active attack relates to modifying and falsifying a message in the traffic [Ref 2]. Modifying and falsifying transferred information means that a part of the message is changed or delayed, re-organized, and resent to enable the desired unauthorized function. Detection of this type of attack is possible, but it may not be preventable [Ref 18]. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and Denial-of-Service (DoS) [Ref 2]. These attacks are as follows.

a. Masquerading

Masquerading occurs when the attacker impersonates an authorized user to gain access as privileged user. In this type of attack, the hacker can modify accounts, configuration data, network signaling, and billing and usage data. Masquerading includes the use of spoofing, rogue APs, and redirection attacks[1].

b. Replay

In this type of attack, the attacker intercepts transmissions (passive attack) in the WLAN traffic and retransmits messages as the legitimate user. The hacker does not modify the messages, just resends altered messages to an authorized user pretending to the system host.

c. Message Modification

Message modification is accomplished when the attacker modifies the message by adding, deleting, changing, or recording it. In addition, an attacker may wish to alter the configuration of a device using, for example, Simple Network Management Protocol (SNMP) to configure APs.

d. Denial-of-Service

A Denial-of-Service (DoS) attack on availability prevents or prohibits the users from the normal use or management of the WLAN systems. The attacker issues

---

[1] An attacker on the route between the mobile station and the AP may redirect mobility bindings to a desired address simply by modifying the IP and User Datagram Protocol (UDP) headers of the Registration Request message. This vulnerability may be used by an attacker to read traffic destined to a mobile station, and to send traffic impersonating the mobile station.

malicious commands or injects a large amount of traffic that fills up the radio frequency spectrum. In addition, the attacker can create radio interference by using microwave ovens or other WLAN equipment to attack the WLAN.

E. VUNERABILITY OF THE WLAN IN SML

A WLAN in SML will face all of the security challenges of any wired network in addition to the new risks introduced by the wireless medium that connects stations and APs. In addition, there are several vulnerabilities of the security mechanism of the IEEE 802.11b, which will be used in SML; this issue is discussed in Appendix B. Because security risks for the WLAN in SML can come from the most malicious hackers as well as from staff or students with the best of intentions, threats to WLAN security can be susceptible to internal vulnerabilities and external threats

1. Internal Vulnerabilities

The internal vulnerabilities will open the door for intruders and hackers to pose serious threats to the WLAN in SML.

a. A Rogue WLAN

A rogue WLAN is an unauthorized entry point in the NPS network, and poses the risk of unauthorized use of service. Staff or students can easily plug their rogue APs into the network for convenience of wireless fast computing, without going through the SML approvals. Although adding the rogue AP does not cost much, it will introduce vulnerabilities to the NPS network. The rogue AP is a security risk because it allows access straight into the NPS network because the default setting of most APs will broadcast SSID settings with no encryption. This also makes it easier for the attacker from outside to gain access to the NPS network.

b. Insecure Network Configurations

Insecure configurations introduce a significant security concern to a WLAN in SML. Default settings, including default passwords of the APs, open broadcasts of SSIDs, weak or no encryption, and lack of authentication configuration in order to emphasize ease of use and rapid deployment, can open the SML to vulnerability.

For instance, the default of Cisco APs, which will be used in SML, is a "tsunami[2]" [Ref 19]. Most of the hackers knew this default SSID.

c. Accidental Associations

Accidental associations between a station and a neighboring WLAN in SML is a security concern when the signal is overlapping networks. This occurs when neighboring WLANs located on adjacent floors operate a WLAN that emanates a strong RF signal broadcasting over into SML space. The WLAN Windows XP operating system enables wireless users to automatically associate and connect to the neighbor's network without their knowledge. A mobile station in SML connecting to a neighboring WLAN can reveal passwords or sensitive documents to unauthorized users in SML from the neighboring network.

2. External Threats

The external threats come from unauthorized users who are not NPS staff and students. These attackers may or may not be located inside the NPS premises. These threats include espionage, identity theft, and other attacks, such as Denial-of-Service and Man-in-the-Middle attacks. Furthermore, the most secure WLANs are not 100 percent safe from the continuously evolving external threats that include eavesdropping and espionage.

a. Eavesdropping & Espionage

If a WLAN were installed in SML it would be vulnerable to eavesdropping, because SML, located in the Ingersoll building, is close to Sloat Avenue (approximately 300 feet) as shown in the circled area in Figure 9. This area is the most vulnerable to attacks. Walls and doors do not provide sufficient containment of the wireless signal. An AP placed inside SML can transmit a signal anywhere up to 300 feet indoors and 1000 feet with an antenna outdoors, hence, the attackers do not have to enter the NPS premise. Attackers could capture the wireless signal from Sloat Avenue, since wireless communication is broadcast over radio waves. The attacker may also use antennas to increase the wireless signal strength. The attacker could passively sniff a WLAN in SML, without gaining physical access. In addition, messages encrypted with

---

[2] "tsunami" is the SSID of an AP, which is used as a default by Cisco Systems Corp. for its WLAN products.

the Wired Equivalent Privacy (WEP) security protocol can be decrypted with available hacking tools; these tools will be discussed later in this chapter.

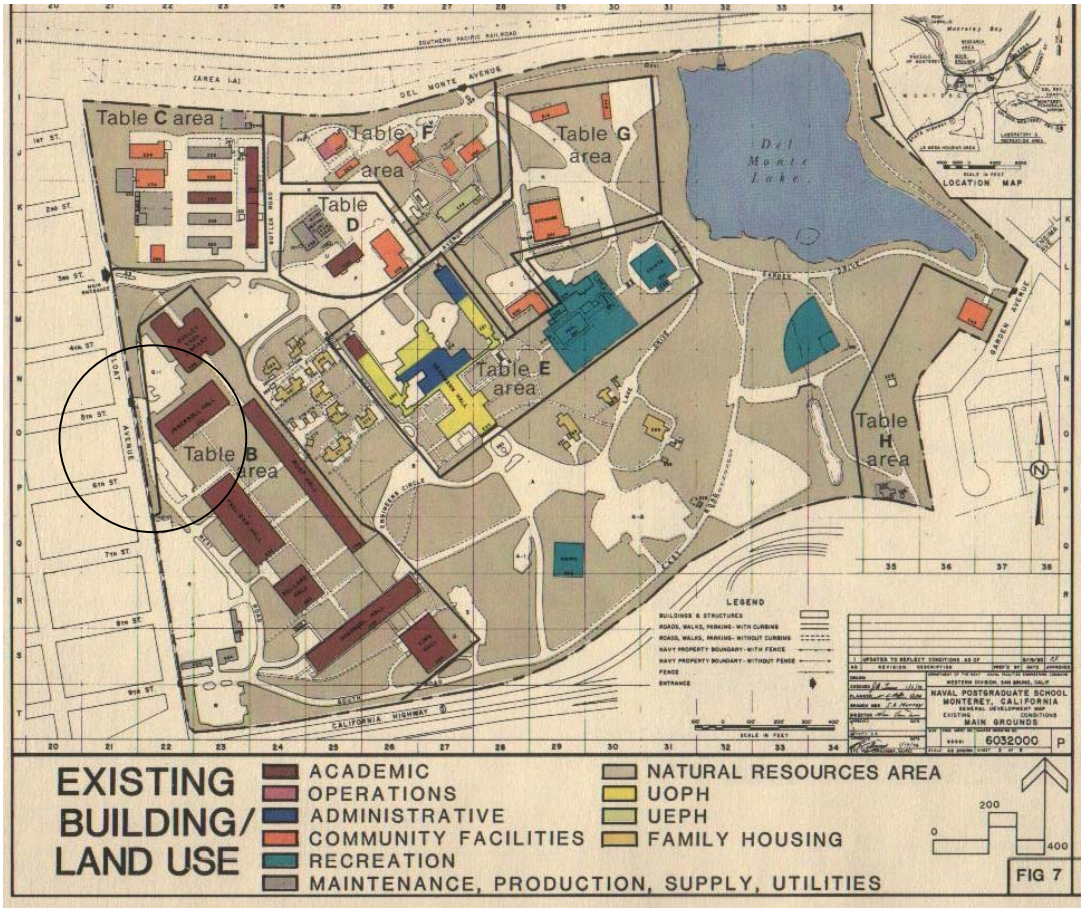

Figure 9. Map of NPS (From Ref:20)

b. SSID and MAC Address Theft

A WLAN in SML, is vulnerable to the theft of a Service Set Identifier (SSID) and MAC address. The SSID is an identification value programmed in the AP or group of APs to identify the local wireless subnet; it acts as a crude password to verify that mobile stations are authorized to connect to an AP, with the MAC address acting as personal identification numbers used to verify the authorized connection with the AP. The SSID is shared among the staff and students. Hence, the attackers might know the SSID of a WLAN in SML. Some APs broadcast the SSID for initial usage, and some use default SSID; these SSIDs can be found on the Internet at http://www.doc-x.de/cgi-

bin/wiki.pl?DefaultSSID. When the SSID broadcast is enabled, any mobile station without a SSID is able to receive it to access an AP.

c. War Driving

War driving is a term used to describe a hacker who is equipped with a laptop, wireless card, and antenna [Ref 4]. These hackers drive around a city in a vehicle to discover unprotected WLANs. To find WLAN signal in the Ingersoll building, a hacker can easily use Digle software. This software can be downloaded free from www.wigle.net, and it can run on the Windows XP operation system. However, the software requires a graphic (Java(tm) version 1.3.0 and up). The Digle software is integrated with a geographic dataset call a "MapPack". The MapPack is updated by the members of the wigle website and is available in any county in the United States.

This software can provide enough information to launch an attack on a WLAN, since the vital information such as SSID, MAC address, and Channel is revealed. In some WLANs, an SSID can not be seen, since the AP does not broadcast the SSID. By using Digle software, the SSID broadcast from Ingersoll building can be identified as GPP, as shown in Figure 10. This map reveals SSID (GPP), MAC Address (00:30:ab:21:d0:d8), Channel (6). In addition, other tools are available to discover a WLAN signal, such as Netstumbler and Kismet. Both Netstumbler and Kismet work in tandem with a Global Positioning System (GPS) to map exact locations of the identified WLANs [Ref 14].

d. Evolving Attack [Ref. 14]

An evolving attack is the sophisticated attack by skilled hackers or casual hackers who can write their own malicious codes. The following section describes the well-known type of attacks, such as malicious association, Denial-of-Service, MAC Spoofing and Man-in-the-Middle attacks, which might make a WLAN in SML vulnerable.

(1) Malicious Association. Malicious association is an attack in which the hackers force a mobile station in SML to connect to an unauthorized AP or alter the configuration of the mobile station to operate in the Ad Hoc mode. The hackers use the freeware tool HostAP to convert the hacker's mobile station to operate as an AP function. When the mobile stations of the SML broadcast a probe to associate with an authorized AP, the new hacker AP responds to the request of SML for association. Then

the connection between the mobile station of the SML and the new hacker AP will begin by providing an IP address to the victim mobile station. At this point, the hackers can exploit all vulnerabilities on the mobile station of the SML

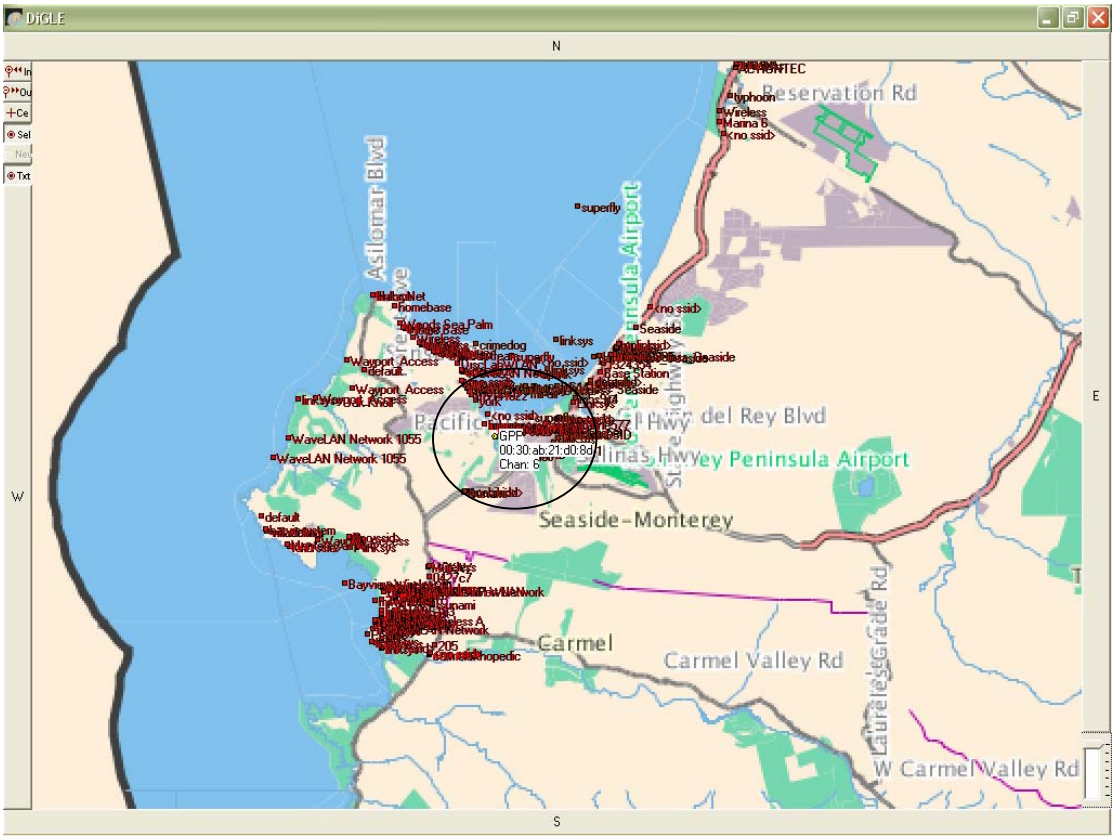

Figure 10. The Detected Wireless Signal in Monterey, CA

(2) MAC Spoofing. Mac spoofing is an attack in which casual or minimal skilled hackers can spoof their MAC address to be legitimate to gain access to the network. This presents unique opportunities for hackers to attack a WLAN in SML that is difficult to detect, since the hackers can present themselves as an authorized mobile station by using an altered MAC address. The hackers capture traffic that is generated by freeware tools, such as Kismet or Ethereal; these are available for hackers to easily pick off the MAC addresses of an authorized user in SML. The hackers can then assume the identity of that user by asserting the stolen MAC address as their own. The hacker then connects to the WLAN in SML as an authorized user.

(3) Man-in-the-middle. Man-in-the-middle is one of more sophisticated attacks by skilled hackers. The hackers begin the attack by monitoring the

traffic of the WLAN in SML between a mobile station of the SML and an AP. They gather frame information to send back and forth about the wireless card and AP, such as the IP address of both devices, the association ID for wireless card, and the SSID of the WLAN in SML.

The hacker tries to associate with the AP by sending a request that pretends this request packet comes from the legitimate mobile station. Then the AP sends the challenge to the legitimate mobile station that sends an appropriate authentic response to the AP to get access. The AP then sends the station a success packet with an imbedded sequence number. At this point, the hackers observe the valid response and act as the AP in presenting a challenge to the legitimate mobile station. In the next step, the hacker sends a spoofed reply with large sequence number, which pushes the legitimate mobile station off the WLAN in SML and keeps this legitimate mobile station from re-associating. The hacker then enters the WLAN in SML as the authorized station.

(4) Denial-of-Service Attacks. Denial-of-Service attacks can range from basic to more sophisticated attacks. For the basic attack, the hackers can use electronic devices, such as microwave, and cordless phones to cause interference on the 2.4 GHz frequency. These devices can jam airwaves and shut down the WLAN in SML.

For more sophisticated DoS attacks, the hackers configure their mobile station to operate as an AP. By doing so, the hackers flood the airwaves with persistent disassociated commands to force all mobile stations in SML to disconnect from the WLAN. In addition, the hackers can launch other DoS attack methods by broadcasting periodic disassociated commands every few minutes. The result is to push mobile stations in SML off the WLAN.

F. SUMMARY

The attacks and malicious threats against a WLAN are continually increasing in number and sophistication along with computer technology. New hacking activities seem to arise daily that block the growth of the WLAN. The security measures for the WLAN must continue to improve to keep up with these threats. There are many WLAN security issues that require attention when employing a WLAN in SML. The next chapter will discuss how to minimize the risk of deploying a WLAN in SML.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SECURITY IN THE SOFTWARE METRICS LAB

As discussed in the previous chapter, numerous methods are available to exploit the security of a WLAN in SML. However, most of these vulnerabilities can be addressed by reasonable security precautions. The first step to make WLAN in SML secure is to define a security policy prior to actual deploying the WLAN. The effective security policy involves defining, disseminating, and enforcing WLAN security policies and practices. These include specifying a configuration and the settings of the WLAN equipment authorized for use, as well as documenting and managing the APs and the connected network infrastructure. Security education for staff and students also increases awareness of security risks. Some staff members and students may not realize that deploying an unauthorized WLAN or using a WLAN devices form a default setting may increase security risks.

In establishing security of a WLAN in SML, the defined security policies should include three key components: WLAN Usage, Network Configuration, and Security policies.

A. WLAN USAGE POLICIES

The WLAN security policy in SML must first define the proper use of WLANs. This includes the applications that run across the WLAN and the exact locations where WLANs should and should not be deployed in the SML. Another consideration is determining where staff and students can use WLAN devices in environments outside the control of the SML. For some applications, WLANs can provide connections to the campus backbone to run most applications. However, WLANs may not be well suited for applications with sensitive information, since WLAN security standards have not yet been fully proofed.

In addition to security concerns, bandwidth for WLAN is a limited resource. Bandwidth intensive applications and network misuse, such as the downloading of MP3 files, can significantly slow down the network and limit the WLAN's ability to serve multiple users.

B. NETWORK CONFIGURATION POLICIES

Before the WLAN in SML is deployed, the network configuration policies should be determined to guide the installation and configuration of the WLAN. Properly configured networks can minimize security risk and maximize the network's performance.

1. User Authentication

Because a WLAN operates in an uncontrolled medium, authentication is an essential measure in securing a WLAN. This authentication allows only authorized users such as staff and students to use the WLAN in SML. To make the WLAN in SML secure, the following measurements are recommended.

a. Turn Off SSID Beacons

The SSID is the wireless identification that distinguishes it from nearby WLANs. Most APs broadcast their SSIDs several times each second by configured default [Ref 12]. The problem with this type of broadcasting is that anyone can join the WLAN to obtain broadcasted SSID. Hence, the WLAN in SML must turn off SSID to prevent the APs from broadcasting the network name. It also prevents users from using the WLAN accidentally, since they have to enter the correct SSID prior to joining the WLAN.

b. Change the SSID

Most APs come with default SSIDs, such as the Cisco APs that use the default SSID "tsunami" and Linksys that uses the name "linksys" [Ref 21]. The problem with using a default SSID is that hackers can easily use the WLAN in SML or even accidentally join a neighboring WLAN in the Ingersoll Building.

To change the default SSID, it is important to select a meaningless SSID that an outside observer would see. However, when the SSID is turned off, it can still be sniffed by the hacker who can use freeware tools, such as Kismet. Therefore, changing the SSID will not prevent anyone from eavesdropping. However, doing this will make it less convenient for hackers to gain access, causing them to configure a SSID manually instead of joining with a preconfigured default SSID.

c. Implement Network Authentication

All the mobile stations in SML must be set to disable Auto-Logon. The Auto-Logon features of Windows 2000 and Windows XP have an option in the operating system to automatically log on when a user boots the system, which is very convenient. However, if unauthorized users can reach these mobile stations, they can also log on automatically.

In addition, the Network Authentication of the Window 2000 Server must be set up to protect against an unauthorized user. In order to gain the access to the WLAN in SML, staff and students must provide valid user names and passwords.

d. Implement MAC Filtering

The Media Access Control (MAC) address is a physical address that uniquely identifies each computer or attached device on a network. Many APs include the ability to limit access by MAC ACLs that are stored and distributed across many APs. The MAC ACLs of WLAN in SML should be limited to ten MAC addresses of mobile stations in order to authenticate only authorized MAC addresses. Any mobile station with a MAC address that is not in the ACLs will not be permitted the use of the WLAN in SML. Nonetheless, the MAC ACLs do not provide a strong security mechanism by themselves, since MAC addresses are transmitted in the clear from a wireless NIC to an AP.

The MAC address can be easily captured by using freeware tools, such as Kismet or Wellenreiter. As a result, hackers can spoof a captured MAC address to be legitimate, thus gaining access to the WLAN in SML. MAC ACLs may provide some level of security; however, an administrator in SML should use this with caution. MAC filtering may be enough defense against normal eavesdropping, but it may not be prevent a sophisticated attack. Therefore, MAC filtering is used as part of an overall defense-in-dept to add security levels of the WLAN in SML.

e. Manage the APs Unavailable on Wireless Connections

Many APs have web-based management interfaces[3] allowing configuring with user name and password authentication for convenient. This makes any wireless access for configuration on the APs vulnerable if the hackers can sniff user name and password. Therefore the web-base management interface of the APs in SML should not be available from the wireless connection to minimize the risk. The administrator should configure the APs through the wired LAN by using only certain workstations to obtain the web-base management interface.

2. Confidentiality and Integrity

Due to the broadcast and radio nature of wireless communication, the confidentiality and integrity of information are more difficult to protect from unauthorized users. The usage of cryptographic protection can minimize the risk by using a WEP method to encrypt the data between two ends. However, the weaknesses of WEP and the availability of numerous freeware tools are the critical vulnerabilities of the WLAN. To maintain confidentiality and integrity of the WLAN in SML, the following measures are recommended.

a. Use WEP

Wired Equivalent Privacy (WEP) has is vulnerable to attack due to the lack of key management and the lack of an adequate authentication method (see Appendix B for greater detail). Although the WEP has weaknesses in protecting confidentiality and integrity, it is better than no protection for the WLAN. In addition, although hackers can use freeware tools for cracking WEP keys, the process of breaking the keys is more difficult with WEP. Therefore, the WEP can be still useful to protect against casual hackers.

In addition to protecting the confidentiality of WEP keys for distribution, these keys should be protected during the distribution of keys to the staff and students. Distributed keys must be encrypted by secure means to prevent unauthorized access to the key.

---

[3] The web-based management interface allows users to manage and configure the advanced features in the AP, such as AP Bridging, Gateway, DNS settings, or name and password authentication etc

b. Establish Proper Encryption Settings

The WEPs are basically passwords to share among staff and students. The WEP keys must be carefully selected because they are subject to the same kinds of attacks as passwords. Two rules should be considered when selecting the WEP keys. First, a user should avoid meaningful words that can be deciphered.

Second, the WEP keys should be put in a hexadecimal format, which has a larger key space than alphanumeric keys. The number of alphanumeric characters is more limited than hexadecimal characters -- about a hundred million times [Ref 12]. As many as 128 bits can be used in the hexadecimal keys. In addition, the administrator should use the stronger 128-bit rather than 40-bit encryption.

c. Change Default WEP Keys

The manufacturer may provide one or more keys to enable shared key authentication between devices trying to gain access to the network and the AP. Using a default shared key setting is a security vulnerability because Cisco uses the identical shared keys "cisco" for factory settings. The hacker may know the default shared key and use it to gain access to the WLAN. Therefore, the default WEP key of Cisco Aironet APs, which will be used in SML, must be changed from "cisco" to the proper WEP key.

d. Rotate WEP Keys

Changing the default WEP key to the proper WEP key will mitigate the risk. However, the longer this WEP key is being used, the more vulnerable the key is. After using the proper WEP key for a period of time, the WEP key should be changed regularly. This rotation of the WEP key will reduce the impact of staff and students in SML giving away the WEP key, and will limit the time for hackers to crack a given WEP key.

The standard compromise is to rotate WEP keys every 30-60 days [Ref 12]. This is usually enough to keep the WEP key relatively fresh while minimizing the amount of time a compromised key grants access to the network. In addition, WEP keys should also be changed whenever a wireless device is lost or stolen, or when one or more of the staff and students leave the NPS, or when staff and students are no longer authorized to use the WLAN in SML.

3. Disable SNMP

Simple Network Management Protocol (SNMP) manages the settings and status of network devices. Many APs allow configuration through SNMP. The SNMP for the AP has security problems. First, the SNMP can display or possibly change AP settings, including WEP keys. Second, implementating SNMP possibly allows hackers the privilege of administering access to devices. This vulnerability allows hackers to read or change settings on the AP; this adds or changes the WEP key for a possible DoS attack. Therefore the SNMP should be disabled on the APs for the WLAN in SML. If using the SNMP is necessary, the community string[4] should be changed from the default by using the same policies as for other passwords. In addition, the SNMP should be configured through the wired LAN since the community string is sent over the network in plain text, and should use the access list to limit SNMP access to the wired side of the AP.

4. Setting the Firewall

A firewall is a barrier that separates sensitive components from attack. It can improve security and reduce vulnerability for the WLAN in SML. The firewalls should be implemented to segregate the WLAN from the NPS network (as shown in Figure 11) by putting the APs outside the firewall and setting up rules that permit only the IP and/or MAC addresses of legitimate users and authorized network traffic from the WLAN or legitimate APs. However, this is not a final or perfect solution because MAC and IP addresses can be spoofed. The benefit of the firewall is that it is used as part of an overall defense-in-dept to add security levels to the WLAN in SML.

5. Keep Firmware Updated

Keeping firmware updated is one of the more important steps in keeping the WLAN in SML secure. Software updates are a good way for a company to fix security problems, when there are bugs or protocol weaknesses. Since software bugs continue to be one of the biggest areas of security weakness [Ref 12], keeping up to date with the latest firmware patches is one way to make sure that WLAN in SML systems are not running. The administrator of the SML should frequently check firmware updates for a

---

4 The community string, an octet string that is between 0 and 255 in the American Standard Code for Information Interchange (ASCII) characters in length, is used to authenticate access to the Management Information Base (MIB). Community strings function as a “password” embedded in every SNMP packet.

NIC and an AP which venders often implement via patches to firmware in order to fix security issues.

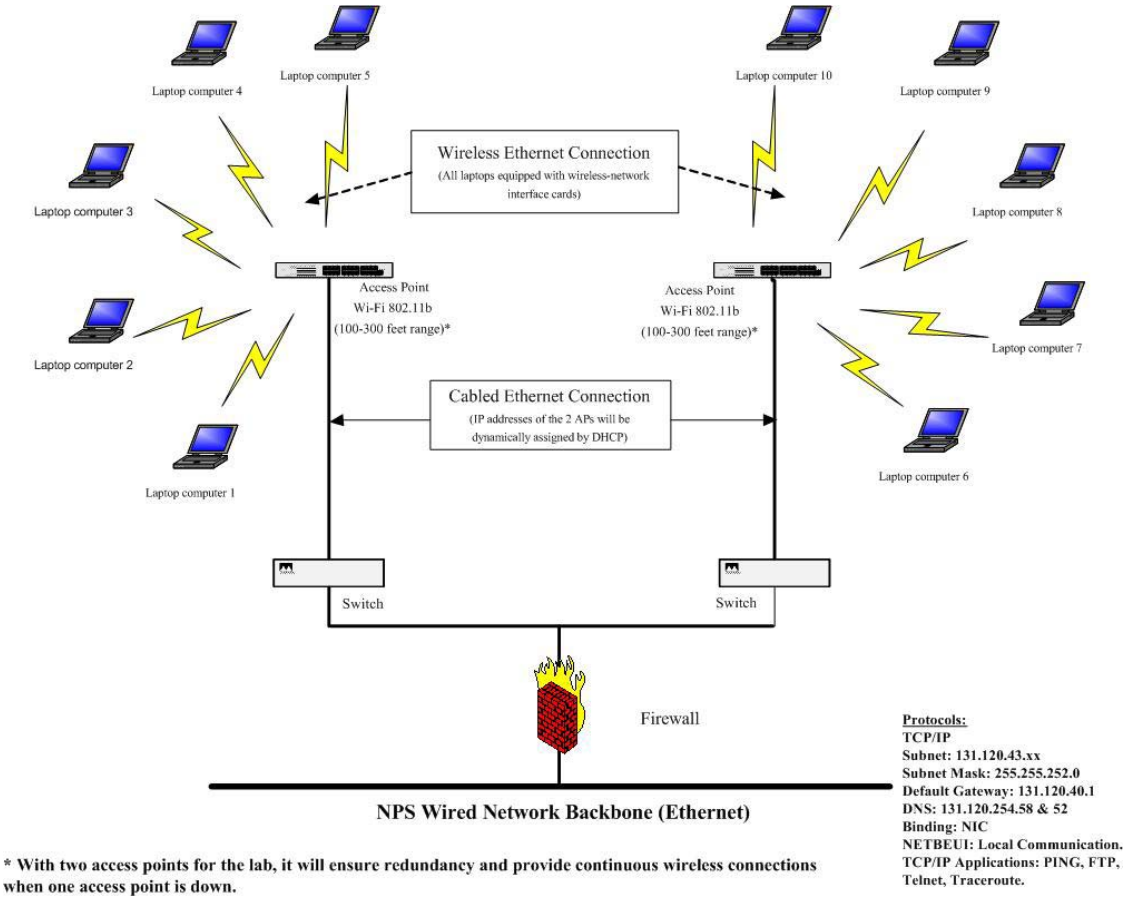

Figure 11. Setting the Firewall in SML

In addition, the administrator of SML should frequently check for operating system patches for mobile stations, work stations, and servers. The SML administrator can check with the National Institute of Standards and Technology (NIST) and the Internet Categorization of Attack Toolkit (ICAT) vulnerability database (http://icat.nist.gov) for a listing of all known vulnerabilities in the software or hardware being implemented [Ref 2].

C. SECURITY POLICIES

A number of security issues of a WLAN can be addressed with the proper configured network. However, the WLAN in SML should also provide additional security policies to educate staff and students about security, and prohibit unauthorized WLAN hardware, software, and activities in SML.

1. Security Education

Security education for staff and students, who are authorized to use the WLAN in SML, is very important. This helps staff and students to understand the security limitations of the WLAN technology so that they will be aware of the vulnerabilities of the uses of the WLAN. Effective security education can be accomplished in two ways. First, provide copies of the security policy to staff and students. Second, establish a short security educational program, a 15-30 minute session to go over the highlights of the security policy.

2. Prohibit Unauthorized APs

Users can connect their APs to the WLAN in SML for their convenience. A single unauthorized AP or rogue AP attached to the WLAN in SML can expose the vulnerability to the NPS network, since the default setting of most APs will broadcast an SSID setting with no encryption. This rouge AP can enable the hackers to view, modify, or steal data from outside the NPS premises. Hence, any AP that is not approved and configured by administrator must be prohibited from being installed on the WLAN in SML.

3. Prohibit Ad Hoc Networks

Ad Hoc networks allow mobile stations to connect to other such stations by using mobile devices instead of the APs. This Ad Hoc network permits staff and students to transfer data without going over the NPS network, while offering poor authentication. Therefore, the Ad Hoc network should be treated as a rogue AP which can put the WLAN in SML at risk without security managers ever seeing the vulnerability. For these reasons, security policies must be enforced to prohibit Ad Hoc networks.

4. Secure APs Physically

The two APs should be properly secured within the SML to prevent any unauthorized access and physical tampering. These APs should be placed in a very secure location where they can't be tampered with.

Moreover, these two APs should be placed away from electromagnetic interference devices, such as microwave or cordless phones, since these devices can cause degradation in throughput.

5. Limit User's Privileges and Access Rights

The user's privileges and access rights to the systems and network resources must be restricted. The principle of least privilege must be considered: grant no user greater access to the system than his or her duty demands [Ref 22]. This principle can be applied to users' modes of access, such as whether they receive read or write privileges.

The privileges for configuration of APs and a WLAN key distribution program, and any utility or operating system, must be restricted to the SML administrator. This also prevents a compromise to the security of other systems with which information resources are shared.

6. Log and Audit

The Logging and auditing of the WLAN in SML could help to detect unauthorized network traffic by using freeware tools, such as AirSnort, Ethereal, or AeroPeek. These tools could analyze the traffic of the WLAN in SML, even though they are also an important tool for hackers. The sniffed information from WLAN traffic can indicate suspect activities, such as invalid SSIDs, unfamiliar MAC addresses, rejected DHCP requests, or ICMP[5] port unreachable. These signatures might well indicate intruder activity, which aids analysis and investigation in the event of a SML network problem. The SML administrator should periodically perform audits to detect any exceptions or abnormal network activities.

---

5 Internet Control Message Protocol (ICMP) A protocol used to pass control and error messages back and forth between nodes on the Internet. Perhaps the most used ICMP command is ping.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

A WLAN may provide portability, flexibility, increased productivity and lower installation costs. Wireless technology provides the ability to move laptops from place to place within the office environment without wires and without lost connectivity.

Deploying the WLAN in SML will be suitable for its roles and functions as a teaching facility for students undergoing computer network related-classes. The design of the WLAN was meant to be simple, and at the same time, achieve its desired objectives. As a result, the laboratory will be able to demonstrate to the students not only its wired but also its wireless networking capabilities. However, the biggest challenge facing WLAN technology today is its security vulnerabilities. Some of these vulnerabilities are the same as for wired networks, while others are unique to WLAN technology. In WLAN technology, because the medium is the air, the radio signal can propagate from outside Sloat Avenue to the Ingersoll Building. Therefore the hackers would possibly access the WLAN in SML outside of NPS. Loss of confidentiality, integrity and availability are typical risks.

Users may intentionally or accidentally spread viruses or launch attacks that prevent staff and students from accessing the network because their laptops are compromised. Staff and students may also create a vulnerability for the WLAN in SML when installing APs for the WLAN in SML. In addition, the Internet contains several public web sites that provide maps of unsecured APs. Intruders or hackers can use this information to gain access to the WLAN in SML, which can result in the loss of data confidentiality, integrity, bandwidth, and network performance. Security must be achieved by defining and enforcing WLAN usage, network configuration, and security policies. Although all the countermeasures in Chapter 4 can be effective in reducing the risks associated with the WLAN, these countermeasures will not prevent all adversary penetration, nor will these necessarily guarantee a secure WLAN environment. Therefore improving security and discovering new security standards of the WLAN to deploy in SML is an area for further research.

B. FUTURE WORK

Future work on security is warranted as follows: First, the WEP is inadequate for security. Second, WLANs are very difficult to manage as the size of the installation grows. To minimize these two problems, two security methods are suggested for future research of this thesis.

1. The IEEE 802.11i Standards-Based Wireless Security

Currently the WEP is the only standards-based security offered defining a shared key for encryption over the wireless air interface. The keys can range from 40 to 128 bits. Recently, WEP has been proven to be inadequate in security, even if the key is increased to 128 bits.

A new working group within the IEEE, the IEEE Taskgroup I (TGi), is developing a new security standard to address the user authentication and encryption weaknesses of WEP-based wireless security [Ref 23]. The IEEE 802.11i addresses the security requirements of AP-based and Ad Hoc wireless networks. The formal completed 802.11i standard is expected in the second half of 2003 [Ref 8]. The components of 802.11i are as following [Ref 24].

a. The IEEE 802.1x Port-based Authentication Framework

The IEEE 802.1x port-based authentication framework is a method for transporting an authentication protocol between the mobile station and the AP, and the Transport Layer Security (TLS) protocol. This TLS protocol handles user authentication and key distribution between the end-user device and the TLS authentication service, which will sit on a back-end Remote Authentication Dial-In User Service (RADIUS) server.

b. The Temporal Key Integrity Protocol

The Temporal Key Integrity Protocol (TKIP) is a security protocol used within the IEEE 802.11i specifications for Wi-Fi networks. It introduces a sophisticated key generation function that encrypts every data packet sent over the wireless medium with its own unique encryption key. The TKIP fixes the security problems of WEP protocol in IEEE 802.11b by using RC4 ciphering with an added function such as a 128-

bit encryption key, a 48-bit initialization vector, a new Message Integrity Code (MIC), and Initialization Vector (IV) sequencing rules to provide better protection.

c. The Advanced Encryption Standard Encryption Algorithm

The Advanced Encryption Standard (AES) encryption algorithm is the standard approved by NIST to replace the RC4 encryption of a WEP. It can generate 128, 192, and 256 bit keys for enhanced security. The AES will serve as a replacement for the Data Encryption Standard (DES), which has a key size of 56 bits. In addition, AES can encrypt data much faster than Triple-DES, a DES enhancement that essentially encrypts a message or document three times.

d. Cipher Negotiation

To accommodate a mix of encryption modes in the same WLAN, the 802.11i specification requires that devices advertise their encryption capabilities in AP beacons and station association requests. The AP and station then set the appropriate encryption cipher based on their mutual capabilities and any specific policies that have been set up for the network.

2. Virtual Private Network Wireless Security

A Virtual Private Network (VPN) is a private data network that makes use of the public Internet. It provides secure access to the corporate network for remote users. In the remote user application, the VPN provides a secure tunnel over the insecure network. The three most common VPN communications protocol standards are used with, Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPSec) [Ref. 23].

The VPN technology can also be used for securing the WLAN by using an end-to-end encryption method. The APs are configured for open access with no WEP encryption, but the WLAN is isolated from the wired LAN by the VPN server [Ref 23]. The APs can be connected together via a Virtual LAN (VLAN) or a LAN that is deployed in the Demilitarized Zone (DMZ)[6] and connected to the VPN server as shown

---

6 The Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

in Figure 12. Authentication and full encryption over the wireless network is provided through the VPN servers that also act as firewalls/gateways to the internal private network. Unlike the WEP key and MAC address filtering approaches, the VPN-based solution is scalable to a very large number of users.

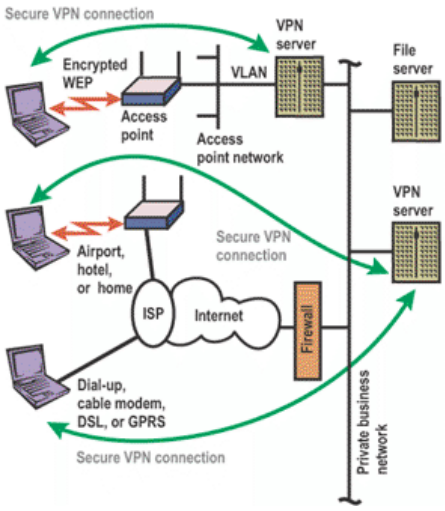

Figure 12. 802.11 VPN Wireless Security (From: Ref 4)

The VPN is preferable for large networks because the administrators do not have to maintain MAC addresses on each AP. The point at which the number of mobile station systems becomes unmanageable varies depending on the organization's ability to administer the network, on its choice of security methods (SSID, WEP, and MAC address filtering), and on its tolerance for risk. If MAC address filtering is used on a wireless network, the fixed upper limit is established by the maximum number of MAC addresses that can be programmed into each AP used in an installation. This upper limit varies, but the practical problem of manually entering and maintaining valid MAC addresses in every AP on a network limits the use of MAC address filtering to smaller networks.

In summary, there is need for future work for the WLAN in SML to enhance the security by applying the VPN or the IEEE 802.11i. In addition, since a new experiment and a new tool that is more sophisticated for breaking the new security standard is probable, previous and new counter measurements and security policies must be reviewed periodically

APPENDIX A. COMMON WIRELESS FREQUENCIES AND APPLICATIONS [REF 2]

EM Band Designation	Frequency Range	Wireless Device/Application
VLF: Very Low Frequency	9 kHz–30 kHz	
LF: Low Frequency	30 kHz–300 kHz	
MF: Medium Frequency	300 kHz–3 MHz	AM radio stations (535 kHz–1 MHz)
HF: High Frequency	3 MHz – 30 MHz	United States Navy fleet communication
VHF: Very High Frequency	30 MHz–300 MHz	FM radio stations VHF television stations 7–13, NTSC Standard (174MHz – 220 MHz) Garage door openers (~40 MHz) Standard cordless telephones (40MHz–50 MHz) Alarm Systems (~40 MHz) Paging Systems (50Mhz–300 MHz)
UHF: Ultra High Frequency	300 MHz–3 GHz	Paging systems (300MHz–500 MHz) 1G Mobile telephones (824MHz–829 MHz) 2G Mobile telephone (800MHz–900 MHz) Global System for Mobile Communication (GSM) Enhanced Data Rates for Global Evolution (EDGE) (800/900/1800/1900 MHz bands) 3G Mobile telephones (international standard) (1,755 MHz– 2200 MHz) Bluetooth devices (2.4 GHz) HomeRF (2.4 GHz) WLAN (2.4 GHz)
SHF: Super High Frequency	3 GHz–30 GHz	Applications in the short range, point-to-point communications including remote control systems, PDAs, etc WLAN (5.8 GHz). Local Multipoint Distribution Services (LMDS), a fixed wireless technology that operates in the 28 GHz band and offers line-of-sight coverage over distances up to 3-5 kilometers.
EHF: Extremely High Frequency	30 GHz–300 GHz	Satellite Communications
IR: Infrared	300 GHz	Remote controls for home audio visual components IR links for peripheral devices PDA and cellular telephone IR links

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. THE IEEE 802.11 B STANDARD

The 802.11b is a RF standard developed by the IEEE for WLANs. Using this standard, businesses and home users can connect their networks with a variety of 802.11b compatible devices, such as desktop computers, laptop computers, PC peripherals, without wires connected to the PC cards, and mini PCI and USB ports. The 802.11b standard is also known as Wireless Fidelity (Wi-Fi)[7] [Ref 25]; its technology is already changing how businesses and home users access the network.

In 1997, the IEEE first 802.11 working group was developed for 1Mbps and 2Mbps data rates [Ref 25]. This Physical (PHY) layer uses a Direct Sequence Spread Spectrum (DSSS) signaling scheme, with modulation methods used for the 1Mbps and 2Mbps data rates being Differential Binary Phase Shift Keying (DBPSK) and Differential Quadrature Phase Shift Keying (DQPSK), respectively. The 802.11b extension was then developed by the working group in 1999 to increase the data rate by using Complementary Code Keying (CCK), which uses a set of 64 eight-bit unique code words [Ref 5]. This extension uses the same bandwidth as the 1Mbps and 2Mbps data rates operating in the 2.4GHz (2.4 to 2.483 GHz) unlicensed RF band. The extension can transmit up to 11Mbps (Megabits per second).

The basic architecture, features, and services of the 802.11b are defined by the original 802.11 standard, which includes only two bottom levels of an OSI reference model, PHY and the Data Link Layer. The Data Link Layer consists of two sublayers, the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer as shown in Figure 13. The 802.11b specification affects only the physical layer, adding a higher data rate and more robust connectivity [Ref 6].

---

[7] Wi-Fi was adopted by the Wireless Ethernet Compatibility Alliance (WECA), which tests and certifies products for compliance and interoperability with the 802.11b standard and gives the Wi-Fi label to those that pass the tests (see Ref 26).

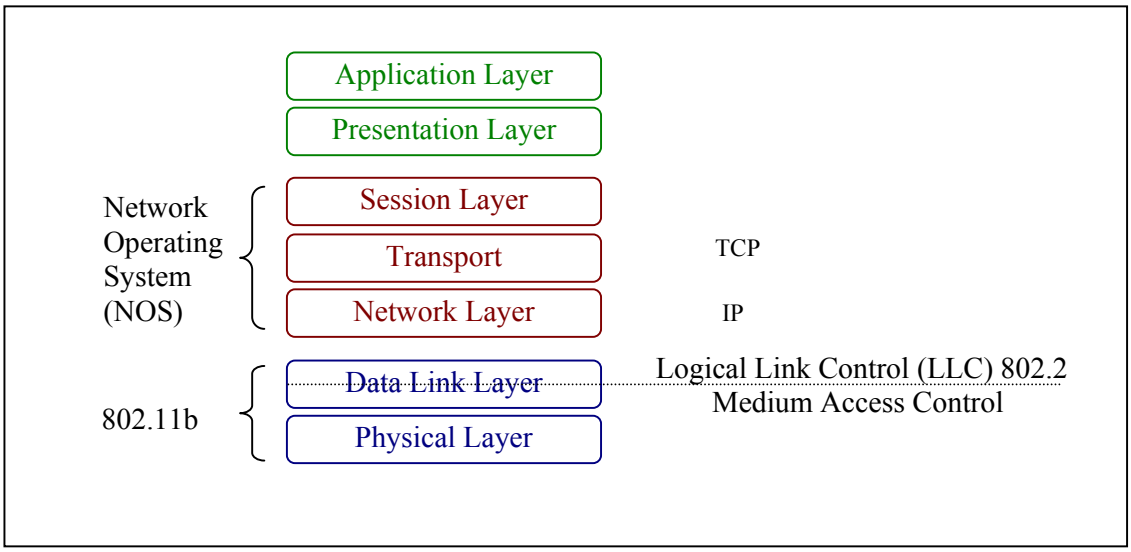

Figure 13. OSI Reference Model (From: Ref 6)

A. OPERATION MODES

The IEEE 802.11b defines two pieces of equipment for a WLAN: first, a wireless station, usually a PC or a laptop with a wireless Network Interface Card (NIC); second, an AP, which acts as a bridge between the wireless stations and the Distribution System (DS) or wired networks [Ref 6]. The WLAN has two operating modes: the Infrastructure mode and the Ad Hoc mode, as shown in Figure 14.

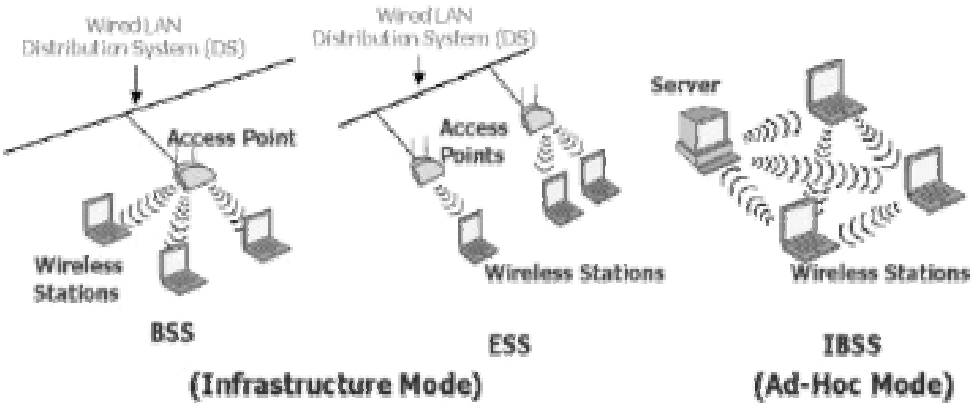

Figure 14. Infrastructure Mode and Ad Hoc Mode (From: Ref 27)

1. Infrastructure Mode

In the infrastructure mode, at least one wireless AP and one mobile station exist. The mobile station uses the AP to access the network. This mode includes a basic service set and an extended service set.

a. Basis Service Set

The Basis Service Set (BSS) is a single AP that supports one or multiple wireless stations. An AP provides a local bridge function for the BSS. All wireless stations communicate with the AP but do not communicate directly with wired networks. All frames are relayed between mobile stations by the AP.

b. Extended Service Set

The Extended Service Set (ESS) is a set of two or more APs that are connected to the same wired network. The APs communicate among themselves, forwarding traffic from one BSS to another to facilitate movement of wireless stations between BSSs [Ref 28]. In addition, the ESS is a single logical network segment (also known as a subnet), which is identified by its Service Set Identifier (SSID). If the available physical areas of APs are in an ESS overlap, a wireless station can roam or move from one location (with an AP) to another (with a different AP), while maintaining Network layer connectivity.

2. Ad Hoc Mode

In the Ad Hoc mode, also known as a peer-to-peer mode, wireless stations communicate directly with each other from an Independent Basic Service Set (IBSS) [Ref 6]. The mode is a set of 802.11 wireless stations which communicate directly with one another without using the AP or wired connection. However, every station may not be able to communicate with all stations due to range limitations. Therefore, all stations need to be within the range of each other to communicate directly (without the use of an AP).

B. THE IEEE 802.11B PHYSICAL LAYER

The 802.11 Physical (PHY) layer is the interface between the MAC layer and the wireless media where frames are transmitted and received. The layer is split into two parts, the Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent (PMD) sublayer [Ref 5]. The PLCP presents a common interface for the MAC

sub layer to write to and provides carrier sense and Clear Channel Assessment (CCA). The PMD provides a clear channel assessment mechanism, transmission, and a reception mechanism. It also provides the wireless encoding.

The PHY provides three functions. First, the PHY provides an interface to exchange frames with the upper MAC layer for transmission and reception of data. Second, the PHY uses signal carrier and spread spectrum modulation to transmit data frames over the media. Third, the PHY provides a carrier sense indication back to the MAC to verify activity on the media [Ref 28].

1. Transmission Methods

The IEEE 802.11b defines 11 Mbps and 5.5 Mbps data rates (in addition to the 1 and 2Mbps rates) utilizing an extension to DSSS called High Rate DSSS (HR/DSSS). It also defines a rate shifting technique in which 11 Mbps networks may transmit at lower speeds, such as 5.5 Mbps, 2 Mbps, and 1 Mps under noisy conditions or to inter-operate with legacy 802.11 PHY layers [Ref 28]. If the wireless station moves back within the range of a higher-speed transmission, the connection will automatically speed up again. Table 1 summarizes the key details in DSSS.

Traditionally, IEEE 802.11 uses either a Frequency-Hopping Spread Spectrum (FHSS) or DSSS technology. Both are good solutions for transmission data rates of 1 to 2 Mbps. However, IEEE 802.11b cannot use FHSS in the United States for higher speeds without violating FCC regulations that restricts subchannel bandwidth to 1 MHz. These regulations force FHSS systems to spread their usage across the entire 2.4 GHz band, meaning they must hop often, which leads to a high amount of hopping overhead [Ref 6]. In contrast, the direct sequence signaling technique divides the 2.4 GHz band into fourteen 22-MHz channels [Ref 6]. Adjacent channels overlap one another partially, with three of the 14 being completely non-overlapping as shown in Figure 15.

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

Table 2. IEEE 802.11b Data Rate Specifications (From Ref: 27)

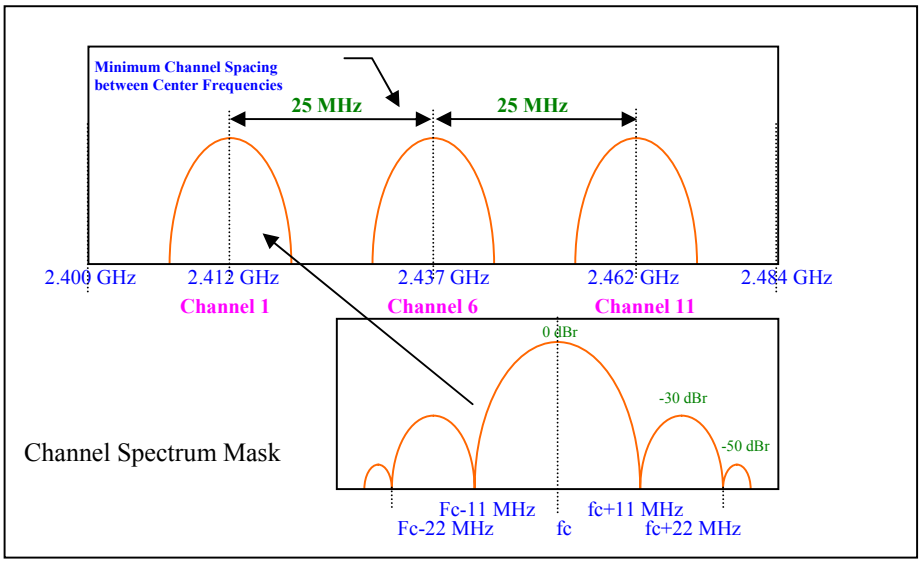

Figure 15. Channel Shape and Channel Spacing (From: Ref 27)

2. The PLCP

An additional protocol layer has been introduced to enable access to the different PHYs for the MAC. This layer called Physical Layer Convergence Protocol (PLCP) is defined differently for each transmission method. Basically, the PLCP for the DSSS mode of 802.11b adds a preamble and a header to the PLCP Service Data Unit (PSDU) coming from the MAC layer [Ref 29].

The PLCP has two formats: a long and a short preamble (see Figure 16 and Figure 17). All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's

throughput when transmitting special data, such as voice, Voice-over IP (VoIP) and streaming video. The format of PLCP consists of two parts, the PLCP Preamble and the PLCP Header.

a. The PLCP Preamble

The PLCP Preamble consisting of a Synchronization (SYNC) and a Start Frame Delimiter (SFD) field and will be transmitted with 1 Mbps Barker spreading[9] [Ref 29].

(1) The SYNC field consists of 128 bits for a long preamble and 56 bits for a short preamble. The field aids the receiver in synchronizing to the signal.

(2) The SFD field consists of 16 bits that help the receiver determine the correct frame start timing. The short preamble format uses a time inverted variant of the long preamble SFD.

b. The PLCP Header

The PLCP Header contains 48 bits of information helping the receiver to demodulate the PSDU. Its content is the same for both the long and short format. The long header is transmitted with 1 Mbps DBPSK, the short one with 2 Mbps DQPSK, both with Barker spreading.

The transmission duration of the short PLCP preamble and header format is just half the time of the long format. Devices soley compatible with the original 802.11 DSSS mode will not be able to produce or decode the short format. The following PSDU can be transmitted on any of the four available data rates with Barker spreading, CCK or PBCC. The long preamble and header format can be combined with any PDSU data rate; whereas, the short format is restricted to 2, 5.5, and 11 Mbps. A complete transmission frame consisting of PLCP preamble, header and PSDU is called a PLCP Protocol Data Unit (PPDU).

(1) The Signal or Data rate (DR) field consists of 8 bits to indicate how fast the data will be transmitted (1, 2, 5.5 or 11 Mbps).

(2) The Service field consists of 8 bits, which is reserved for future use.

---

[8] The original 802.11 DSSS standard specifies an 11-bit chipping called a Barker sequence to encode all data sent over the air. Each 11-chip sequence represents a single data bit (1 or 0), and is converted to a waveform, called a symbol, which can be sent over the air.

[9] Barker spreading is the method of modulation in the DSSS PHY layer with 11-bit Barker word, which is applied to a modulo-2 adder (Ex-Or function) together with each of the information bits in the PPDU. The PPDU is clocked at the information rate, 1 Mbps, for example, and the 11-Barker word at 11 Mbps (the chipping block). The output of the module-2 adder results in a signal with a data rate that is 10x higher than the information rate. At the receiver, the DSSS signal is convolved with the 11-bit Barker word and correlated. The correlation operation recovers the PPDU information bits at the transmitted information rate and the undesired interfering in-band signals are spread out-of-band. The spreading and despreading of a narrowband to a wideband signal is commonly referred to as processing gain and is measured in decibels (dB). Processing gain is the ratio of the DSSS signal rate to the PPDU information rate.

(3) The Length field consists of 16 bits, which indicates the length of the ensuing Medium Access Control sublayer's Protocol Data Unit (MAC PDU).

(4) The Cyclic Redundancy Code (CRC) field consists of 16 bits, which is used for error detecting.

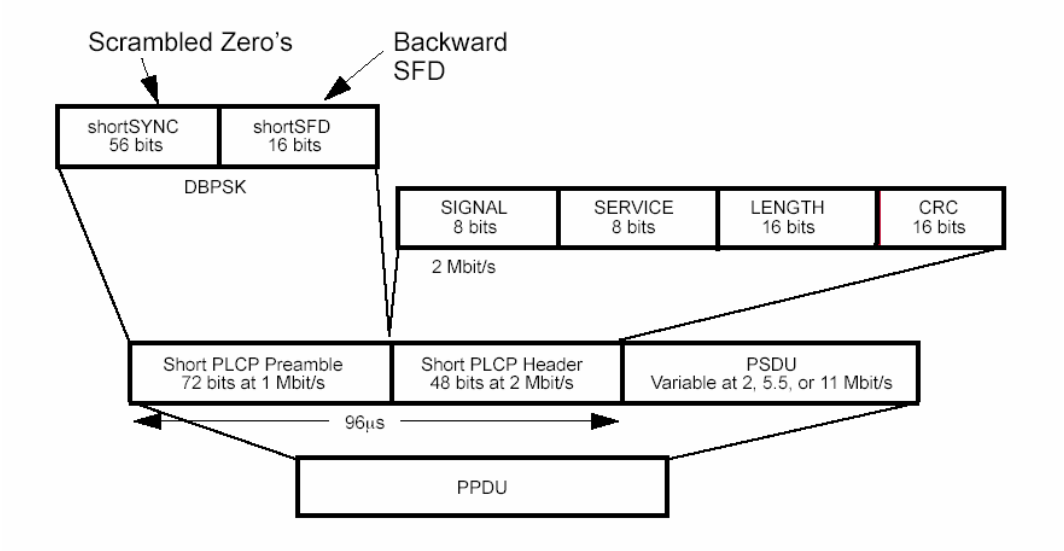

Figure 16. Short PLCP PPDU format (From: Ref 29)

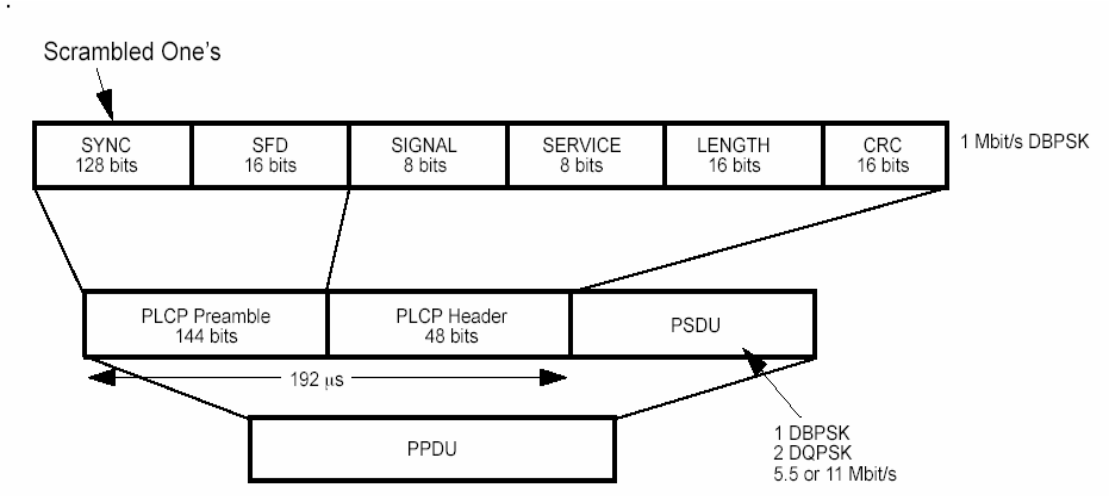

Figure 17. Long PLCP PPDU format (From: Ref 29)

C. THE IEEE 802.11B MEDIUM ACCESS CONTROL SUBLAYER

The MAC sublayer of the IEEE 802.11b serves as the interface between the physical layer and the host device. It is responsible for channel allocation procedures, Protocol Data Unit (PDU) addressing, frame formatting, error checking, fragmentation and reassembly [Ref 30].

This sublayer supports both Infrastructure and Ad Hoc operation modes. Two robustness features in the IEEE 802.11b MAC sublayer are Cyclic Redundancy Check (CRC) and Packet Fragmentation [Ref 27]. Each packet has a CRC calculated and attached to ensure that the data are not corrupted in transit. Packet Fragmentation will send large packets in small pieces when sent over the air. This has two advantages. The first advantage is to reduce the need for retransmission because the probability of a packet becoming corrupted increases with the packet size. The second advantage is where a packet becomes corrupted, the node needs to retransmit only one small fragment; therefore, it is faster.

The transmission medium can operate in the contention mode exclusively, requiring all stations to contend for access to the channel for each packet transmitted. The medium can also alternate between the contention mode, known as the Contention Period (CP), and a Contention-Free Period (CFP). During the CFP, the medium usage is controlled (or mediated) by the AP, thereby eliminating the need for stations to contend for channel access.

1. Inter Frame Spaces (IFS) and Frame Types

Priority access to the medium is controlled through the use of Inter Frame Space (IFS) intervals. This system allows every station access to the medium at the correct moment when sending a frame, but it does not allow one station to transmit data with preference over others. The standard defines four different IFS intervals [Ref 30]. Figure 18 shows the relationships between difference timings.

a. Short Inter Frame Space (SIFS)

The SIFS is used to separate transmissions belonging to a single dialog (e.g. Fragment-ACK). It is the minimum time Interframe (IF). With SIFS there is at least one station to transmit at a given time, hence having priority over all other stations. This value is fixed per PHY and is calculated in such a way that the transmitting station will

be able to switch back to the receive mode and be capable of decoding the incoming packet. For the 802.11 PHY, this value is set to 28 microseconds, which is the period between the completion of packet transmission and the start of the ACK frame. (The minimum IFS)

b. Point Coordination IFS

The Point Coordination IFS (PIFS) is used by the AP (or Point Coordinator, as it is called in this case), to gain access to the medium before any other station. This value is equal to SIFS plus a Slot Time

c. Distributed IFS

The Distributed IFS (DIFS) is the Inter Frame Space used for a station willing to start a new transmission. It is calculated as PIFS plus one slot time.

d. Extended IFS

The Extended IFS (EIFS) is the longest IFS used by a station receiving a packet that it could not understand. It is needed to prevent the station from colliding with a future packet belonging to the current dialog.

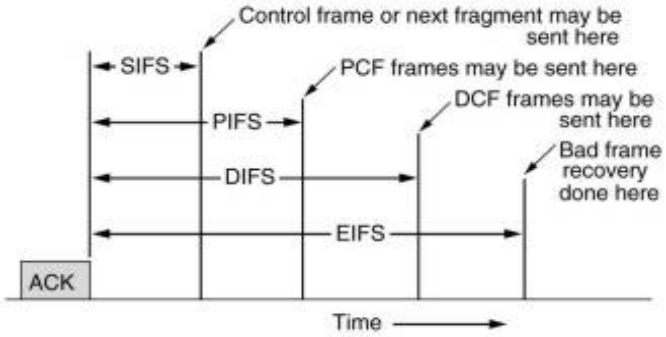

Figure 18. Interframe Space Relation (From: Ref 31)

2. The Basic Access Method

The IEEE 802.11 MAC sublayer provides fairly controlled access to the shared Wireless Medium (WM) through two different access methods [Ref 32]. These are the Distributed Coordination Function (DCF), using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), and the Point Coordination Function (PCF), providing contention-free frame transfers.

a. Distributed Coordination Function (DCF)

The basic access method of the 802.11b standard is a Distributed Coordination Function (DCF) [Ref 28] that allows for automatic medium sharing through the use of a CSMA/CA algorithm (see Figure 19). These are medium access timings for different frame types: the random backoff procedure, frame transfer procedures, acknowledgement procedures, and Request To Send (RTS) and Clear To Send (CTS) procedures. The backoff procedure is used for collision avoidance, where each station waits for a backoff time (a random time interval in units of slot times) before each frame transmission. Moreover, a priority level for access to the channel is provided through the use of IFS, as discussed earlier; however, it does not allow one station to transmit data with preference over others [Ref 32]. For example, before each transmission, a station has to wait a time equal to DIFS to not disturb other ongoing transmissions, which might be only separated by a time equal to SIFS.

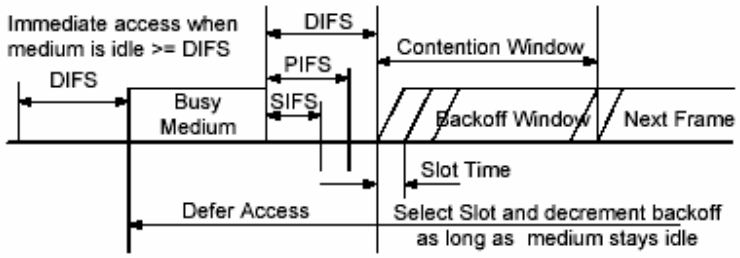

Figure 19. 802.11 Collision Avoidance Mechanism (From: Ref 31)

In addition, all traffic uses immediate positive Acknowledgement (ACK frame), where retransmission is scheduled by the sender if no ACK is received. In this case, a Stop-and-Wait Automatic Repeat Request (ARQ) error control mechanism will take over [Ref 33]. A Carrier sense is performed both through physical and virtual mechanisms. The virtual carrier sense mechanism is based on frames (e.g., RTS/CTS, Beacon Frames) that convey information about how long the medium will be busy. This mechanism is called a Network Allocation Vector (NAV).

b. Point Coordination Function (PCF)

Point Coordination Function (PCF) is an extension to DCF, which is an optional access method [Ref 30]. The PCF is integrated with the DCF, with both

operating simultaneously. The PCF using PIFS instead of DIFS enables transmission of time-sensitive information. The PCF supports Quality of Service (QoS), which guarantees certain characteristics during transmission for certain communication requirements (high priority traffic to access the medium at constancy interval, higher throughput and to maximize the utilization of available bandwidth) [Ref 34]. An AP is necessary for PCF, which can assign the broadcasting rights by means of a channel reservation to the mobile stations. This procedure is called polling. With PCF, a Point Coordinator (PC), within the AP, controls which stations can transmit during any given period of time.

The PC begins a period of operation called the Contention-Free Period (CFP), during which the PCF is operating. This period is called contention free because access to the medium is completely controlled by the PC and the DCF is prevented from gaining access to the medium [Ref 34].

The PC resides in the AP and schedules a CFP (within a time period), which it announces by sending a beacon frame after the SIFS. This indicates a higher priority than the ordinary contention frames. When a station receives the poll from the AP, the medium is reserved for the duration of its transfer up to the length of CFP. When the data transfer completes or the reserved time finishes, the AP waits for PIFS seconds and polls another station. The PCF continues until the CFP interval is up, then the system operates in the DCF mode. If the AP finds the medium idle, it waits for a PIFS period of time and then transmits a beacon frame with a polling frame following SIFS seconds after it. The PCF further maintains a list of stations that have requested to be polled during the CFP and polls them. For example, the point coordinator may first poll station A; during a specific period of time station A can transmit data frames allowing no other station to send. The point coordinator will then poll the next station and continue down the polling list while permitting stations to have a chance to send data.

Thus, PCF is a contention-free protocol and enables stations to transmit data frames synchronously with regular time delays between data frame transmissions. This makes it possible to more effectively support information flows, such as video and control mechanisms that have more demanding synchronization requirements [Ref 5].

Timing mechanisms within the 802.11b protocol ensure that stations on the WLAN alternate between the use of DCF and PCF. As a result, the WLAN can support both asynchronous and synchronous information flows. For a period of time, stations will fend for themselves by using CSMA. For the following time period, the stations will wait for a poll from the point coordinator before sending data frames.

3. The IEEE 802.11b MAC Frame

A MAC frame or a MAC Protocol Data Unit (MPDU) encapsulate the higher layer protocol data or contain MAC management messages [Ref 29]. The 802.11b specification also details frame format structure. This structure is designed to support DCF and PCF operation. The frame format consists of a MAC header and a frame body. The frame body contains the MAC Service Data Unit (MSDU) from the higher layer protocols, and it has a maximum length of 2,048 bytes [Ref 23]. The frame structure also includes a MAC header, which contains information on the frame type, destination addresses, and the length of the data payload [Ref 5].

a. The IEEE 802.11b MAC Frame Format

The exact format of the MAC frame differs somewhat for the various MAC protocols in use. In general, all of the MAC frames have a format similar to that of Figure 20. This general format is used for all data and control frames, but not all fields are used in all contexts. The fields of this frame are as follows [Ref 28].

- **Frame control:** This field consists of 2 bits, which indicates the type of frame and provides control information. It carries control information being sent from station to station.
- **Duration/connection ID**: This field consists of 16 bits with each frame containing information that identifies the duration of the next frame transmission. Whenever the contents of this field are less than the value 32768, the duration value is used to update the Network Allocation Vector (NAV)

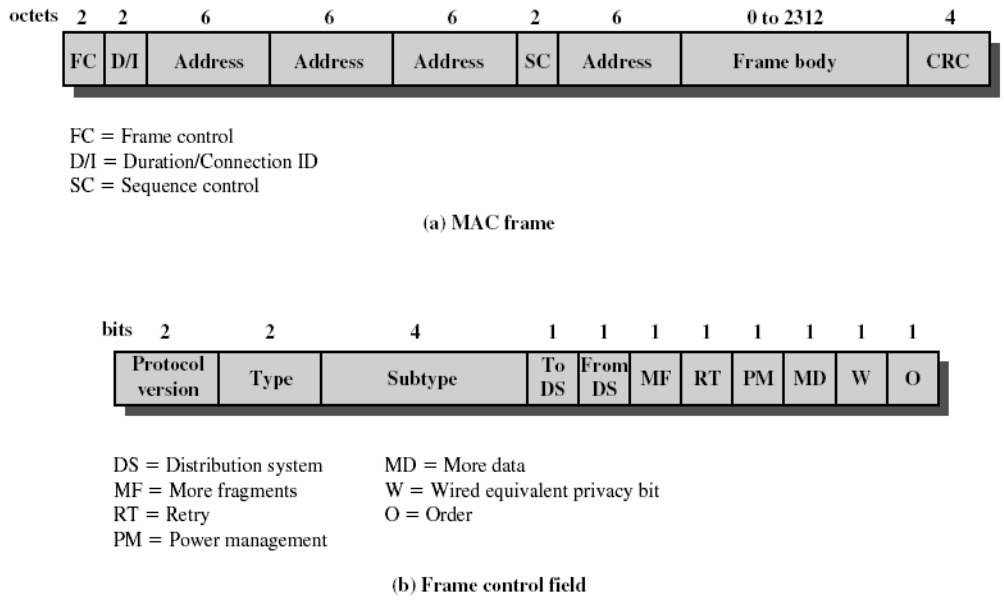

Figure 20. The MAC Frame and Control Field (From: Ref 31)

- **Addresses:** This field consists of 48 bits with four different address fields in the MAC frame format. Address-1 is the recipient address. If To Distribution System (ToDS) is set, it is the AP Address; if it is not set, this is the end-station address. Address-2 is the transmitter address. If From Distributing System (FromDS) is set, this is the AP Address. If it is not set, this is the station address. Address-3 is in most cases the remaining, missing address. On a frame with FromDS set to 1 Address-3 is the original Source Address, if the FromDS is set, then Address-3 is the destination Address. Address-4 is used in special cases when a Wireless Distribution System is used and when the frame is being transmitted from one AP to another. Both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.
- **Sequence control:** This field contains 16 bits. It consists of two sub fields: Sequence Number (12 bits) used for fragmentation and reassembly, and the Fragment Number (4 bits) used to number frames sent between a given transmitter and receiver.
- **Frame body:** This field is a variable length field containing MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- **Frame check sequence:** This field contains 32 bits with a CRC. It is calculated over all the fields of the MAC header and the Frame Body field.

b. Frame Control

The Frame Control field itself is divided into subfields as shown in Figure 20. They are as follows Figure 20 shows the 802.11 frame format. This general format is used for all data and control frames, but not all fields are used in all contexts. The fields are as follows [Ref 34]:

- **Protocol version:** This field consists of 2 bits indicating the version of the IEEE 802.11 standard. Currently the version of the standard value is fixed as 0.
- **Type:** This field consists of 6 bits identifying the frame as control, management, or data.
- **Subtype:** This field consists of 6 bits defining the type of the Frame. Table 3 details in valid Type and Subtype Combination.
- **To DS:** This bit is set to 1 when the frame is sent to the Distribution System (DS). This includes cases when the destination station is in the same BSS, and the AP is to relay the frame.
- **From DS:** This bit is set to 1 when the frame is coming from the Distribution System (DS).
- **More fragments:** This bit is set to 1 when more fragments belong to the same frame following the current fragment.
- **Retry:** This bit is set to 1 if this is a retransmission of a previous frame. This will be used by the receiver station to recognize duplicate transmissions of frames that may occur when an Acknowledgment packet is lost.
- **Power management:** This bit is set to 1 if the transmitting station is in a sleep mode. It indicates the power management mode that the station will be in after the transmission of the frame. This is used by stations that are changing state either from Power Save to Active or vice versa.
- **More data:** This bit is set to 1 when more frames are buffered to this station. Each block of data may be sent as one frame or a group of fragments in multiple frames
- **WEP:** This bit is set to 1 when the frame body is encrypted with Wired Equivalent Protocol (WEP), which is used in the exchange of encryption keys for secure data exchange

- **Order:** This bit is set to 1 in any data frame sent using the strictly ordered service class, which tells the receiving station that frames must be processed in order. Next, the various MAC frame types are discussed.

c. The IEEE 802.11 MAC Frame Format Types

Three main types of MAC frames are used in the MAC layer: data, control and management. Data frames are used for data transmission. Control Frames are used to control access to the medium (e.g., RTS, CTS, and ACK). Management Frames are transmitted in the same manner as data frames to exchange management information; however, they are not forwarded to upper layers (e.g., beacon frames). Each frame type is subdivided into different subtypes according to their specific function.

Within the frame structure is a series of control frames. Overall, the IEEE 802.11b supports six types of control frames: RTS, CTS, AC, PS-Poll, CF-End, and CF+End+ACK.

(1) Control Frame Subtypes assist in the reliable delivery of data frames between stations. There are six control frame subtypes [Ref 34]:

- **Request To Send (RTS):** This is the first frame in the four-way frame exchange. It is optional and reduces frame collisions present when hidden stations have associations with the same AP. A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame.
- **Clear To Send (CTS):** This is the second frame in the four-way exchange. A station responds to a RTS with a CTS frame, providing clearance for the requesting station to send a data frame. This frame is sent by the destination station to the source station to permit sending a data frame. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for the required time of the requesting station to send its frame. This minimizes collisions among hidden stations, which can result in higher throughput if implemented properly.
- **Acknowledgment:** This provides an acknowledgment from the destination to the source. After receiving a data frame, the receiving station utilizes an error checking process to detect the presence of errors. The receiving station sends an ACK frame to the sending station if no errors are found. If the sending station does not receive an ACK after a period of time, the sending station retransmits the frame to the receiver.

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1100	Deauthentication
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-ACK
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-ACK + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-ACK (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-ACK + CF-Poll (no data)

Table 3. Type and Subtype of the Frame Control Field (From: Ref 28)

- **Power Save-Poll (PS-Poll):** This frame is used when the station wakes up, and sends this frame to the AP requesting the AP to sends the buffered data when the station is in active mode.
- **Contention-Free (CF)-end:** The purpose of this frame is to announce the end of a CFP that is part of the point coordination function.
- **CF-end _ CF-Ack:** The purpose of this frame is to acknowledge the CF-end. This frame ends the CFP and releases stations from the restrictions associated with that period.

(2) Data Frames Subtypes are used for data transmission which carries packets from higher layers, such as web pages, printer control data, etc., within the body of the frame. The eight data frame subtypes are organized into two groups. The first four subtypes define frames that carry upper-level data from the source station to the destination station. The four data-carrying frames and four subtypes which do not carry user data [Ref 34]:

- **Data:** This is the simplest data frame, which is variable in length (29-2346 bytes). It may be used in both a contention period and a CFP.
- **Data _ CF-Ack:** This frame is only sent during a CFP. In addition to carrying data, this frame acknowledges previously received data. The ACK is for a previously received data frame, which may not be associated with the address of the destination of the current frame.
- **Data _ CF-Poll:** This frame is used only by a point coordinator when delivering data to a mobile station during a CFP, to deliver data to a mobile station. It is also used to simultaneously request the mobile station to send a data frame that it may have buffered when the current reception was completed.
- **Data _ CF-Ack _ CF-Poll:** This frame combines the functions of the Data _ CF-Ack and Data _ CF-Poll into a single frame, which is used by the PC during the CFP.
- **Null Function (no data):** This data frame subtype, without data, is only used to exchange information for the power saving function. The mobile station sends this frame to the AP to carry a Power Management Bit in the Frame Control field, which indicates that the mobile station is changing to a low-power operating state.
- **CF-ACK (no data):** A mobile station uses this to acknowledge the PC during a CFP. The ACK is more efficient since this frame is 29 bytes long. If the PC receives a Data + CF-ACK frame from a station, the PC can send a Data + CF-Poll + CF-ACK frame to a different station, where the CF-ACK portion of the frame acknowledges receipt of the previous data frame. The ability to combine polling and acknowledgement frames with data frames, transmitted between stations and the PC, has been designed to improve efficiency.

- **CF-Poll (no data):** The PC uses this to request a mobile station to send a pending data frame during the CFP.
- **CF-ACK+CF-Poll (no data):** This is used by the PC to combine CF-ACK and CF-Poll.

(3) Management Frames Subtype is used to manage communications between stations and APs. It enables a station to establish and maintain communication. The following subtypes include [Ref 34]:

- **Association request:** The mobile station requests an association with a BSS for the success or failure of a request to the AP. If the AP accepts the request, it returns an association response with a status field value of successful. The Station must then ACK the successful association response for the Station to be associated with the AP. There are two information elements in the association request: the Service Set Identifier (SSID) and the supported rates.
- **Association response:** This frame is sent by an AP to indicate whether it is accepting a mobile station for association. If the AP accepts the mobile station, the frame includes information regarding the association, such as an association ID and supported data rates. If the outcome of the association is positive, the mobile station can utilize the AP to communicate with other mobile stations in the network and systems on the distribution (e.g., Ethernet) side of the AP.
- **Reassociation request:** This frame is sent by a mobile station when it roams away from the currently associated AP to find another AP having a stronger beacon signal. The mobile station uses reassociation rather than association so that the new AP knows to negotiate with the old AP to forward data frames.
- **Reassociation response:** This frame is sent by the AP to indicate whether it is accepting a reassociation request. Similar to the association process, the frame includes information regarding the reassociation, such as the association ID and supported data rates.
- **Probe request:** This frame is sent by the mobile station to obtain information from another station or AP. It contains SSID and the supported rates. In the Infrastructure BSS, the AP will always respond to probe requests. In IBSS, the mobile station that sent the latest beacon will respond.

- **Probe response:** This frame is sent by the mobile station to respond with a probe response frame containing capability information, supported data rates, etc.
- **Beacon:** This frame is periodically sent by the AP to allow mobile stations to locate and identify a BSS. The AP announces its presence and relay information, such as timestamp, SSID, and other parameters related to the AP and the mobile stations that are within range. The mobile stations continually scan all 802.11 radio channels and listens to beacons as the basis for choosing the best AP for association.
- **Announcement traffic indication message:** This frame is sent by a mobile station to alert other mobile stations, which were possibly in a low power mode, that this station has frames buffered and waiting to be delivered to the station addressed in this frame.
- **Dissociation:** This frame is used by the mobile station to terminate an association; either the AP or the mobile station may disassociate.
- **Authentication:** This frame is used to conduct a multiple exchange to authenticate one station with another. The mobile station must send system authentication (the default) of itself before it is permitted to send data. The mobile station sends only one authentication frame; the AP responds with an authentication frame indicating acceptance or rejection. With the optional shared key authentication, the mobile station sends an initial authentication frame. The AP then responds with an authentication frame containing challenge text. The mobile station must send an encrypted version of the challenge text by using its WEP key in an authentication frame back to the AP. The AP ensures that the mobile station has the correct WEP key by observing whether the challenge text recovered after decryption is the same that was sent previously.
- **Deauthentication:** This frame is sent by the mobile station to another mobile station or AP to announce that it is terminating secure communications.

D. THE IEEE 802.11B SECURITY BASIC METHOD

Security mechanisms in 802.11b networks should be equivalent to existing mechanisms in wired LANs. However, the WLANs have a much larger area to protect because the WLANs transmit signals over a much larger area than those for wired media. Wired networks are located in buildings, which are already secured from unauthorized physical access. A user must gain physical access to the building to gain access to the network. On the other hand, a WLAN, which is configured incorrectly, may be accessed

from any location within the range of the WLAN. Currently in the 802.11b standard three basic methods exist to secure access to an AP [Ref 35].

1. Service Set Identifier (SSID)

A service set identifier (SSID) is a sequence of characters that uniquely name a WLAN. The system manager enters identifier code into the setup of all APs and mobile stations that will participate in the network to declare a network as open or closed. The SSID will be unique within a Basic Service Set (BSS) or Extended Service Set (ESS). This SSID must be known by the Network Interface Controller in order to associate with the AP and thus proceed with data transmission on the network [Ref 36]. If the SSID does not match the one stored in the AP, the station cannot establish a connection to the WLAN.

Most APs will broadcast the SSID to all wireless devices by default from the vendor within the wireless network. This enables a station to determine which networks allow mobile station access without a specific SSID [Ref 25]. Although this makes it easy to get a wireless network running, it offers no security. Therefore, this feature should be disabled because it may assist an intruder in gaining access to a private network. The administrator of an AP can disable the broadcast mechanism, but, generally, SSIDs are easily shared.

When installing a WLAN, changing the default SSID and selecting unique ID is recommend. By default, the SSID is broadcasted, allowing users to easily identify a nearby AP. For added security, this broadcast function can be disabled. However, this may introduce additional configuration issues for users and network support personnel.

2. Media Access Control (MAC) Address Filtering

The access list contains the media access control (MAC) address of the stations authorized to access the network through an AP. A mobile station can be identified by the unique MAC address of its 802.11b network card. A MAC address is a unique hardware number assigned to the network card, which is a permanent 48-bit MAC address written into the hardware (no two network devices have the same MAC address) [Ref 37]. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the mobile stations allowed to access the AP. Each AP must have a list of authorized mobile station MAC addresses in its Access Control List

(ACL)[10]. As a rusult, the AP will grant access to any computer that is using a NIC whose MAC address is on the list. If the mobile station's MAC address is not included in this list, the mobile station is not allowed to associate with the AP. Filtering the MAC address is time consuming because the list of mobile station MAC addresses must be manually inputted in each AP. Since the MAC address list must be kept up-to-date it is, therefore, better suited for a small network.

The MAC address filtering provides good security. However, since the MAC address is sent in clear text in the data link layer header, it can be obtained by network monitoring. At the same time the MAC address of an attacker's wireless network card can be altered to correspond to it (known as MAC address spoofing). Since MAC addresses can be spoofed, the MAC address filtering is not regarded as a strong authentication method.

3. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the standard mechanism for security in 802.11b that provides an equivalent level of privacy to the wired LAN by encrypting the transmitted data. In addition, WEP is based on the symmetric key encryption[11] algorithm Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG) [Ref. 36]. This algorithm provides protection against eavesdropping and physical security attributes comparable to a wired network. The mechanism of WEP provides a secured WLAN data streams between mobile stations and APs, with confidentiality achieved by encrypting the data sent between wireless nodes. To do this, WEP relies on a shared secret key between WLAN devices (mobile station device with interface card) and an AP. The key encrypts data before any transmission and deciphers it at the other end.

In WEP encryption, weaknesses that make WEP vulnerable to attacks are due to problems with key management. No defined mechanism changes the WEP key, either per

---

[10] ACL (Access Control List) is used in some WLAN APs to control mobile station access. The ACL is usually based on the mobile's wireless Ethernet MAC address which is unique in each mobile station. The ACL is a database used to store MAC addresses that can access the WLAN. If the mobile station's MAC address is not listed in the ACL, a user's access will be denied

[11] An encryption system which the sender and receiver use a single key to encrypt and to decrypt data. Symmetric-key cryptography is sometimes called secret-key cryptography.

authentication or at periodic intervals, over the duration of an authenticated connection. All APs and mobile stations use the same manually configured WEP key for multiple connections and authentications. This makes it difficult to change the WEP key regularly, which increases the security risk from an intruder. Moreover, in 2001, WEP encryption was proven to be vulnerable to attack because the keys are easily deciphered in its weak encryption code [Ref 25]. Scripting tools, such as WEPCrack and AirSnort, were created to take advantage of the weaknesses in the RC4 algorithm. These tools were used to attack a network and discover the WEP key.

The combination of a lack of both adequate authentication methods and key management for encryption of wireless data has led the IEEE to adopt a new method for securing a WLAN.

GLOSSARY

ACL	Access Control List
APs	Access Points
ACK	Acknowledgement
AES	Advanced Encryption Standard
AMPS	Advanced Mobile Phone System
ARQ	Automatic Repeat Request
BSS	Basic Service Set
CSMA/CD	Carrier Sense Multiple Access Collision Detect
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CDPD	Cellular Digital Packet Data
CCA	Clear Channel Assessment
CTS	Clear To Send
CDMA	Code Division Multiple Access
CCK	Complementary Code Keying
C.I.A.	Confidentiality, Integrity, and Availability
CP	Contention Period
CF	Contention-Free
CFP	Contention-Free Period
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DR	Data Rate
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
DCF	Distributed Coordination Function
DIFS	Distributed Inter Frame Spaces
DS	Distribution System
DNS	Domain Name Server
DFS	Dynamic Frequency Selection
EM	Electromagnetic
EIFS	Extended Inter Frame Spaces
ESS	Extended Service Set
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FHSS	Frequency-Hopping Spread Spectrum
FromDS	From Distributing System

GHz	Gigahertz
EDGE	Global Evolution
GPS	Global Positioning System
GSM	Global System for Mobile
HR/DSSS	High Rate Direct Sequence Spread Spectrum
IBSS	Independent Basic Service Set
IR	Infrared
IV	Initialization Vector
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter Frame Spaces
ICAT	Internet Categorization of Attack Toolkit
IPSec	Internet Protocol Security
ISM	Industrial, Scientific and Medical
KHz	Kilohertz
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LMDS	Local Multipoint Distribution Services
LLC	Logical Link Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
Mbps	Megabits per second
MAC	Media Access Control
MIC	Message Integrity Code
GSM	Global System for Mobile Communications
mW	milli Watt
UNII	Unlicensed National Information Infrastructure
NIST	National Institute of Standards and Technology
NAV	Network Allocation Vector
NICs	Network Interface Cards
OSI	Open Systems Interconnect
OFDM	Orthogonal Frequency-Division Multiplexing
PBCC	Packet Binary Convolutional Coding
PCF	Point Coordination Function
PDAs	Personal Digital Assistants
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PPDU	PLCP Protocol Data Unit
PSDU	PLCP Service Data Unit
PIFS	Point Coordination Inter Frame Spaces
PC	Point Coordinator
PPTP	Point-to-Point Tunneling Protocol

PS-Poll	Power Save-Poll
PDU	Protocol Data Unit
QPSK	Quadrature Phase Shift Keying
QOS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RTS	Request To Send
RF	Radio Frequency
RC4 PRNG	Ron's Code 4 Pseudo Random Number Generator
RTS/CTS	Request To Send/Clear To Send
SSID	Service Set Identifier
SIFS	Short Inter Frame Space
SNMP	Simple Network management protocol
SML	Software Metrics Lab
SFD	Start Frame Delimiter
SYNC	Synchronization
TKIP	Temporal Key Integrity Protocol
TGi	IEEE Taskgroup I
TDMA	Time Division Multiple Access
ToDS	To Distribution System
TCP\IP	Transmission Control Protocol/Internet Protocol
TPC	Transmission Power Control
TLS	Transport Layer Security
VLAN	Virtual LAN
VPN	Virtual Private Network
VoIP	Voice-over IP
Wi-Fi	Wireless Fidelity
WEP	Wired Equivalent Privacy
WAP	Wireless Application Protocol
WM	Wireless Medium
WWAN	Wireless Wide Area Network
WLAN	Wireless Local Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Lasse Seppänen, "Wireless Local Area Network (WLAN) IEEE 802.11", whitepaper, 2002, Available online, [http://trade.hamk.fi/~lseppane/courses/ wlan/doc/Material.pdf.], February 2002.

[2] Tom Karygiannis, Les Owens, National Institute of Standards and Technology, Administration, U.S. Department of Commerce. "DRAFT Wireless Network Security 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld Devices 802.11, Bluetooth and Handheld" NIST Special Publication 800-48, November 2002

[3] Florida State University, "FSU Official Wireless Security Document", 2003, Available online, [http://www.acns.fsu.edu/network/wireless_security.shtml# _Toc26601403], February 2003.

[4] Russell Dean Vines, "Wireless Security Essentials", Wiley Publishing, Inc, 2002.

[5] Plamen Nedeltchev, "Wireless Local Area Networks and the 802.11 Standard", whitepaper, March 2001, Available online, [http://www.cisco.com/warp/public/ 84/packet/jul01/pdfs/whitepaper.pdf.], March 2003.

[6] 3COM, "IEEE 802.11b Wireless LANs", whitepaper, 2002, Available online [http://www.3com.com/other/pdfs/infra/corpinfo/en_US/50307201.pdf.], March 2003.

[7] Dr. Norman F. Schneidewind, "IS3502 Computer Networks: WAN/LAN, Wireless Networks", course notes, Naval Postgraduate School, 2002.

[8] Public Safety Wireless Network Program, "Wireless Data Networking Standards Support Report: 802.11 Wireless Networking Standard", whitepaper, October 2002, Available online [http://www.pswn.gov/admin/librarydocs11/Wireless_data _networking_standards_802_11.pdf], March 2003.

[9] Polytechnic University, Roye Oake, Teresa Broxton, Eric Blaise, and James Whiting, "Wireless Local Area Network", whitepaper, December 1999, Available online, [http://www.ite.poly.edu/mg/mg790/790Fall99/WirelessLAN_B2B_ TIM2001.PDF.], April 2003.

[10] British Education Communication and Technology Agency (Becta), "Wireless Local Area Networks (WLAN)", whitepaper, October 2002, Available online, [www.ictadvice.org.uk/downloads/ wirelesslan_technical.doc.], April 2003.

[11] Chye Bin Tay, "Wireless LAN Extension", M.Sc. Thesis, Naval Postgraduate School, March 2003.

[12] Jim Graves, "Wireless LAN Threats and Mitigations", whitepaper, December 2002, Available online, [http://www.ins.com/downloads/whitepapers/ins_white_ paper_wireless_lan_threats_1202.pdf], April 2003.

[13] Dale Gardner, “Wireless Insecurities, Control mobile computing vulnerabilities before they get control of you”, whitepaper, January 2002, Available online, [http://www.infosecuritymag.com/2002/jan/cover.shtml], April 2003.

[14] Air Defense, “Wireless LAN security-What Hackers Know That You Don’t”, whitepaper, January 2003, Available online, [http://www.airdefense.net/ eNewsletters/hackersfeature.shtm], June 2003.

[15] Proxim, Wireless Network, “ORiNOCO Range Extender Antenna”, whitepaper, June 2003, Available online, [http://www.farallon.com/products/all/Orinoco /client/rea/], June 2003.

[16] J. D. Morrison, “IEEE 802.11 Wireless Local Area Network Security Through Location Authentication”, M.Sc. Thesis, Naval Postgraduate School, September 2003.

[17] Karri Huhtanen, “Security problems and solutions in WLAN access zones”, whitepaper, May 2001, Available online, [http://erwin.ton.tut.fi/kh/interests/ security/security-problems-and-solutions-in-wlan-access-zones.pdf], June 2003.

[18] Wireless Integrated Network, Florida State University, “FSU Official Wireless Security Document”, whitepaper, May 2003, Available online, [http://www.acns.fsu.edu/network/wireless_security_pdf.shtml], June 2003.

[19] Bob Brewin, “FSU Worldwide ‘war drive’ expose insecure wirless LANs”, whitepaper, September 2002, Available online, [http://www.computerworld.com /mobiletopics/mobile/story /0,10801,74103,00.html], June 2003.

[20] Western Division Naval Facilities Engineering Command, “Master Plan Naval Postgraduate School, Monterey, CA, September 1983.

[21] AirDefense Inc, “Wireless LAN policies for security and management”, whitepaper, 2003, Available online, [http://www.airdefense.net/company/ whitepaper/policies.pdf], July 2003.

[22] Security in the Government Sector, “Chapter 9: Control of Access to Information Systems”, whitepaper, Jul 2002, Available online, [http://www.security .govt.nz/sigs/html/chapter9.html], July 2003.

[23] Dell “Wireless Security in 802.11 (Wi-Fi®) Networks”, whitepaper, January 2003, Available online, [http://www.dell.com/downloads/global/vectors/wireless_ security.pdf], July 2003.

[24] Atheros Communication “Building Secure Wireless Networks, How Atheros Defines Wireless Network Security Today and In The Future”, whitepaper, 2003, Available online, [http://www.atheros.com/pt/atheros_security_whitepaper.pdf], July 2003.

[25] Scott Anderson, Carolina Gomez, Jerry MacLean, Erin O'Grady, "Securing Wi-Fi's Future SECURING WI-FI'S FUTURE: The Need for a Public-Private Partnership to Secure 802.11b Networks", whitepaper, Georgetown University, Washington, DC, 2002, Available online, [www.georgetown.edu/users/gem8/Securing%20Wi-Fi's%20Future.pdf.], April 2003.

[26] William Stallings "IEEE 802.11: Moving Closer to Practical Wireless LANs", whitepaper, June 2001, Available online, [http://www.csie.ncnu.edu.tw/~ccyang/WirelessNetwork/Papers/802.11/802.11Intro-1.pdf], April 2003.

[27] Kanoksri Sarinnapakorn , " High Rate Wireless Local Area Networks", March 2001, Available online, [http://alpha.fdu.edu/~kanoksri/IEEE80211b.html.], April 2003.

[28] Ergen ergen, "IEEE 802.11 Tutorial", University of California Berkeley, whitepaper, June 2002, Available online, [http://esoumoy.free.fr/telecom/tutorial/ieee-tutorial.pdf.], May 2003.

[29] Rohde&Schwarz, "Generating Signals for Wireless LANs, Part I: IEEE 802.11b", White paper, December 2001, Available online, [http://www.eetchina.com/ARTICLES/2002OCT/A/2002OCT28_RFT_NTES_HBM_AN01.PDF], May 2003.

[30] Jeevan Chittamuru, Arunachalam Ramanathan & Manoj Sinha, "Simulation of Point Coordination Function for IEEE 802.11 Wireless LAN using Glomosim", University of Massachusetts, Amherst, whitepaper, June 2002, Available online, [http://www-unix.ecs.umass.edu/~aramanat/CN/report697_new.doc.], May 2003.

[31] Cleveland State University, "IEEE 802.11 Wireless LAN Standard", whitepaper, June 2002, Available online, [http://academic.csuohio.edu/yuc/mobile03/0128-stallings.pdf.], May 2003.

[32] Javier del Prado and Sunghyun Choi, "Experimental Study on Co-existence of 802.11b with Alien Devices", Philips Research Briarcliff, whitepaper, 2001, Available online, [http://mwnl.snu.ac.kr/~schoi/publication/Conferences/01-VTC-T34_3.PDF.], May 2003.

[33] Michael Fainberg, "A Performance Analysis of The IEEE 802.11b Local Area Network in The Presence of Bluetooth Personal Area Network ", M.Sc. Thesis, Polytechnic University, June 2001, Available online, [http://eeweb.poly.edu/dgoodman/fainberg.pdf], May 2003.

[34] Prado and Sunghyun Choi, Dongyan Chen, Sachin Garg, Martin Kappes and Kishor S. Trivedi, "Supporting VBR VoIP Traffic in IEEE 802.11 WLAN in PCF Mode ", Duke University, whitepaper, 2001, Available online, [http://www.ee.duke.edu/~dc/publications/wlan-opnet.pdf.], April 2003.

[35] Javier del Prado and Sunghyun Choi, “Experimental Study on Co-existence of 802.11b with Alien Devices”, Philips Research Briarcliff, whitepaper, 2001, Available online, [http://mwnl.snu.ac.kr/~schoi/publication/Conferences/01-VTC-T34_3.PDF.], April 2003.

[36] Toshiba, “Rising popularity of WLANs (Wireless Local Area Network) also raises security concerns”, whitepaper, September 2002, Available online, [http://uk.computers.toshiba-europe.com/cgi-bin/ToshibaCSG/download_ whitepaper.jsp?z=36&service=UK& WHITEPAPER_ID=0000000fdd_123], April 2003.

[37] Toshiba, “Low security is better than no security at all”, whitepaper, 2003, Available online, [http://uk.computers.toshiba-europe.com/cgi- bin/ToshibaCSG/ download_whitepaper.jsp? WHITEPAPER_ID=0000000fdf_123], April 2003.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan C. Boger
   Chair, IS Department
   Naval Postgraduate School
   Monterey, California

4. Professor Norman Schneidewind
   Naval Postgraduate School
   Monterey, California

5. Professor Douglas Brinkley
   Naval Postgraduate School
   Monterey, California

6. Captain Thoetsak Jaiaree
   Ministry of Defense, Thailand