NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROTOTYPE SYSTEM FOR DETECTING AND PROCESSING OF IEEE 802.11A SIGNALS

by

Che Seng Goh

March 2004

Thesis Advisor:	Tri T. Ha
Second Reader:	Murali Tummala

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Prototype System for Detecting and Processing of IEEE 802.11a Signals	**5. FUNDING NUMBERS**
6. AUTHOR(S) Che Seng Goh	
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)

As the need to send larger amounts of information increases, the military is looking into viable solutions to push this information throughout the battle space. IEEE 802.11a wireless LAN network presents an attractive high-speed solution by providing data rates up to 54 Mbps. At the same time, wireless LAN introduces increased security risk due to its vulnerability to exploitation of the wireless LAN physical layer.

This research will develop a prototype system using low cost hardware and software solution to detect and process wireless IEEE 802.11a signals. Using the prototype, performance data will be collected to determine whether IEEE 802.11a is a feasible option as a high-speed information network for military use. Additionally, the performance data collected will provide a good basis for predicting the expected performance in an operational scenario and provide valuable information for proper deployment planning.

14. SUBJECT TERMS Wireless Transmission Protocol, IEEE 802.11a, Wireless LAN	**15. NUMBER OF PAGES** 85
	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

THIS PAGE INTENTIONALLY LEFT BLANK

PROTOTYPE SYSTEM FOR DETECTING AND PROCESSING OF IEEE 802.11A SIGNALS

Che Seng Goh
Major, Republic of Singapore Air Force
Bachelor of Engineering (First Class Honors),
Nanyang Technological University, Singapore, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author:	Che Seng Goh
Approved by:	Tri T. Ha Thesis Advisor
	Murali Tummala Second Reader/Co-Advisor
	Dan Boger Chairman, Department of Information Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the need to send larger amounts of information increases, the military is looking into viable solutions to push this information throughout the battle space. IEEE 802.11a wireless LAN network presents an attractive high-speed solution by providing data rates up to 54 Mbps. At the same time, wireless LAN introduces increased security risk due to its vulnerability to exploitation of the wireless LAN physical layer.

This research will develop a prototype system using low cost hardware and software solution to detect and process wireless IEEE 802.11a signals. Using the prototype, performance data will be collected to determine whether IEEE 802.11a is a feasible option as a high-speed information network for military use. Additionally, the performance data collected will provide a good basis for predicting the expected performance in an operational scenario and provide valuable information for proper deployment planning.

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

First and foremost, I would like to thank my wife Priscilla and my three wonderful children Clemence, Celine and Clifford for their unwavering support, love and kind understanding throughout the conduct of this research. The tight two academic quarters spent on this research has been enjoyable but hectic, considering the other subjects that I have taken. Without my family's support, none of this research would be possible.

Next, I would like to thank Nathan Beltz, the Cryptologic Research Lab Manager, who has been very helpful in providing equipment support, information and technical assistance for this research. I am most impressed that, despite the long procurement lead-time and hosts of funding issues, he is still able to get all the required equipment for this research. The only flip side to this is that I have to scramble to finish all the experimentation in my last academic quarter.

I would like to thank Professor Tri Ha, who placed complete trust in my work and provided guidance along the way.

I would also like to thank Professor Murali Tummala, who readily agreed to be my second advisor.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE AND BENEFIT OF THIS RESEARCH

In the past decade, Wireless Local Area Network (WLAN) technology has grown from an obscure and expensive pursuit into a practical and affordable networking technology. Among the many IEEE 802.11 WLAN standards, the 802.11a networks utilizing the Orthogonal Frequency Division Multiplexing (OFDM) technology in the 5-GHz band offer an increasingly attractive option as a high-speed information network for military use, providing up to 54 Mbps of bandwidth.

At the same time, utilizing WLAN in the military introduces increased security risk due to the vulnerability of the WLAN physical layer to exploitation. A number of papers have been published that describe several theoretical vulnerabilities in the security mechanisms provided by the 802.11 standards. Attacks based on these vulnerabilities have been implemented and are freely available on the World Wide Web.

This thesis research will explore commercially available 802.11a compliant hardware and software and attempt to build a low cost prototype that can be used to detect and process 802.11a WLAN signals. The prototype system will be helpful for military use as a detection system to process other 802.11a WLAN signals in the battlefield. Additionally, the system will be a useful tool for security vulnerability assessment of a military WLAN network.

As an added work in this research, the prototype system produced will be used to collect data pertaining to the detection range and effective data rate of the 802.11a WLAN at various ranges.

This thesis will eventually answer the following three questions:

1. What specific commercially available low cost hardware and software solutions can be utilized to detect and process a wireless IEEE 802.11a compliant network signal?

2. What is the detection and processing performance of the prototype hardware and software solution?

3. What is the measured operating range of 802.11a compliant networks, compared to theoretical/advertised operating range?

The end product of this research will be a prototype system, made up of commercially available low cost hardware and software, which can be used to detect and process 802.11a compliant WLAN signals. Additionally, the performance data collected by the prototype system can be used as a basis for predicting expected performance in an operational scenario and provide valuable information for proper deployment planning.

Chapter II of this thesis will outline the various 802.11 WLAN standards, 802.11 architecture and the Orthogonal Frequency Division Multiplexing (OFDM) technique used in the 802.11a standard. The topics covered in this chapter will provide useful background information needed to understand terms and concepts used in this research.

Chapter III of this thesis covers the development of the prototype system. In this chapter, all details leading to the development of the prototype system are presented. These include the selection of both the hardware and the software portion of the system, and the test setup for performance comparison among the various available hardware solutions.

Chapter IV will present the test setup and performance results of the prototype system when it is used to detect and process 802.11a WLAN signals.

Chapter V of this thesis covers the test setup and measurement results pertaining to the 802.11a link performance as detected and processed by the prototype system.

Chapter VI is the final chapter and it covers the conclusions for this thesis and suggests possible future work on this thesis.

B. PREVIOUS RELATED WORK

An earlier prototype system for detecting 802.11b WLAN signals has been developed and tested by Cpt Walter N. Currier Jr. in March 2002 [1]. The 802.11b detection system enjoyed the convenience of interchangeable antennas – because equipment vendors supply PC cards with pigtail interfaces for external antenna. This resulted in more research devoted to the choice of external antenna. With the external antenna, the 802.11b prototype system achieved very good detection ranges. On the other hand, due to the more complicated OFDM technique used in 802.11a, equipment vendors do not supply PC cards with external antennas. The detection range for 802.11a signals is expected to be limited due to this factor.

Another interesting work pertaining to the performance of 802.11a WLAN is that of James C. Chen [2]. In this work, an 802.11a access point and an 802.11b access point were set up at the same location in the office. An 802.11a mobile client and an 802.11b mobile client were then placed at the same distance away from the access points and the range performance data was collected. The study concluded that the 802.11a has similar range compared to the 802.11b in a typical office environment, yet 802.11a has two to five times the data link rate of 802.11b. The results are interesting for this thesis because the link rate data for 802.11a indoors can serve as a basis for comparison with the measured link rate for outdoors.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. IEEE 802.11 INTRODUCTION

Wireless Local Area Network (WLAN) technologies offer a wide range of capabilities and operate in different ways and environments. The common denominator among all of these technologies is that they do not require fixed wire connection, but instead transmit signals to one or more wireless receivers over a wireless channel.

The IEEE initiated the 802.11 project in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area."[3]. In 1997, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications, similar to what was done with the 802.3 Ethernet standards.

The IEEE 802.11 standard specifies the use of both Radio Frequency (RF) spread spectrum and infrared technologies for WLAN. The RF spread spectrum technology is further broken down into two components – frequency hopping spread spectrum (FHSS) and Direct Sequence spread spectrum (DSSS), as shown in Figure 1 below.

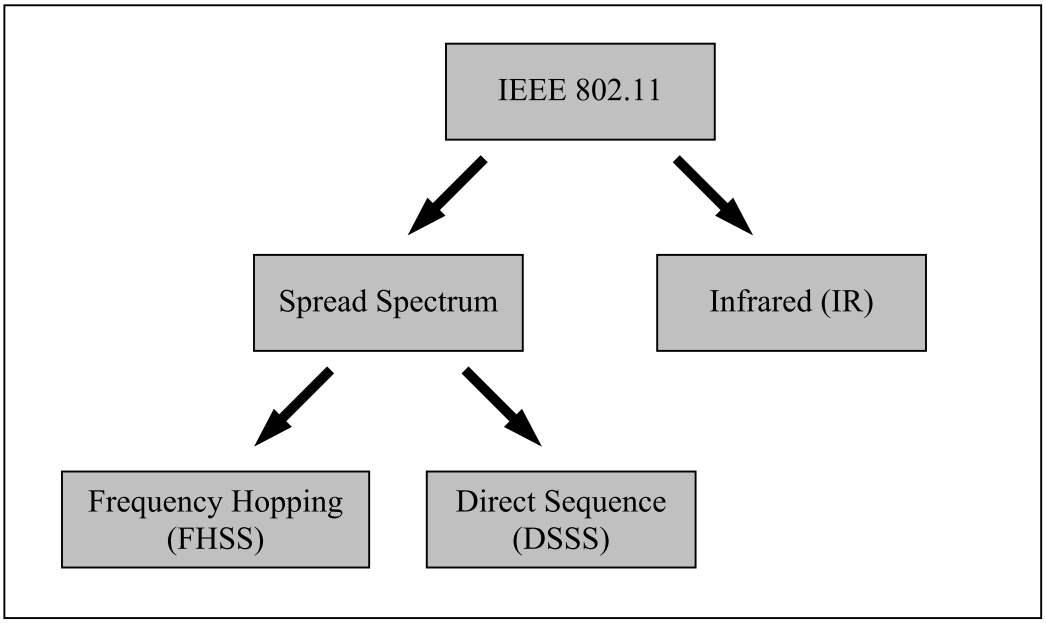

Figure 1. IEEE 802.11 Technologies for WLAN

The 802.11 standard, as specified by the IEEE, covers FHSS, DSSS, and infrared at 1 Mbps and 2 Mbps, although higher speeds are supported with each of these technologies. The following paragraphs list the various standards and drafts of the 802.11 standard.

B. IEEE 802.11 STANDARDS AND DRAFTS

The following brief description of IEEE 802.11 standards and drafts are all based on the original 802.11 standard.

1. 802.11b Standard

802.11b is the first revision of the IEEE 802.11 standard for direct sequence spread spectrum WLAN. The 802.11b standard specifies the use of the 2.4 GHz Federal Communications Commission (FCC) authorized Industrial, Scientific, and Medical (ISM) radio frequency band, as does the original 802.11 standard. The IEEE defines channels for use in this band that operates within the frequencies allotted by the FCC within the United States. The IEEE also defines channels for operation in other countries that work within those countries' frequency allocations.

802.11b only covers DSSS at 11 Mbps and 5.5 Mbps (backward compatible with 802.11 using DSSS at 1 and 2 Mbps). This standard is very popular due to the good throughput, long range and relatively low cost of the components that are compliant with this standard. However, with the decreasing cost of components and higher speed offered by the later 802.11a & 802.11g standards, the 802.11b popularity is gradually eroding.

The only difference between the 5.5 & 11 Mbps (under 802.11b revision) and the 1 & 2 Mbps (in original 802.11) data rates is the modulation techniques and spreading codes used. Instead of barker code with Binary Phase Shift Keying (BPSK) and Quadrature Phase Shift Keying (QPSK) modulation, 802.11b utilizes Complementary Code Keying (CCK) with QPSK modulation.

2. 802.11a Standard

The 802.11a standard is the focus of this thesis. 802.11a is a revision to the IEEE standard that operates in the FCC designated Unlicensed National Information Infrastructure (UNII) 5 GHz band. Most 802.11a products support data rates up to 54

Mbps, although some product vendors advertise data rates of up to 108 Mbps under their proprietary “Turbo” mode [4]. The 802.11a standard specifies the use of UNII bands and the use of Orthogonal Frequency Division Multiplexing (OFDM) technology. This standard consists of four channels of 20 MHz with 5 MHz of separation between channels. There are a total of twelve non-overlapping channels – four channels each for the Lower (5.15 – 5.25 GHz), Middle (5.25 – 5.35 GHz) and Upper (5.725 – 5.825 GHz) bands.

OFDM is the secret behind how the 802.11a is able to get up to a whopping 54 Mbps data rate. OFDM creates eight non-overlapping channels 20 MHz wide across the two lower bands of the 5 GHz UNII band (four channels in each of the two lower bands). Each of these eight channels is subdivided into fifty-two subcarriers, each approximately 300 kHz wide. Each subcarrier is transmitted in parallel with the other fifty-one, meaning all fifty-two subcarriers transmit and receive simultaneously. A receiving station then processes these fifty-two incoming signals, each one representing a fraction of the total data transmitted, and makes up the complete transmission.

To prevent data loss from the large amount of information being transmitted at such high data rates, some means of error correction is required. In this respect, the 802.11a uses Forward Error Correction (FEC). The performance impact due to the inclusion of FEC is fairly negligible due to the high data rate.

The 802.11a standard requires speeds of 6, 12, and 24 Mbps, with a maximum of 54 Mbps. Typical product vendor implementations include data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Data rates higher than 54 Mbps, such as the “turbo” rate of 108 Mbps mentioned earlier use proprietary technology that is not compatible across vendors.

The Wireless Fidelity (Wi-Fi) Alliance has announced that the Wi-Fi certification now also covers interoperable 802.11a products. They have further discussed that Wi-Fi for 802.11a will likely be geared to have 802.11h replace 802.11a in interoperability testing in the near future [5].

Due to the competing use of the UNII 5 GHz bands by both 802.11a and HiperLAN2, the European Telecommunications Standard Institute (ETSI) has not certified 802.11a for usage in Europe yet. In an effort to resolve the problem, two new additions have been proposed for the 802.11a standard: Dynamic Channel Selection (DCS) and Transmit Power Control (TPC). Together, these two solutions allow 802.11a clients to detect the most available channels for use and then use the minimum amount of transmit power that is necessary if any interference is evident. With these additions, 802.11a may be licensed for use in Europe by ETSI as a short-time solution until IEEE ratifies the 802.11h standard.

3. 802.11h Draft

Both 802.11a and 802.11h are nearly identical, except that 802.11h includes TPC and DCS as outlined previously. This should allow 802.11a to be licensed in Europe once IEEE ratifies the final standard.

The Wi-Fi Alliance's Wi-Fi5^{TM} currently covers 802.11a, but not 802.11h. Adding to the confusion, 802.11h is likely to replace 802.11a within the industry and the Wi-Fi5^{TM} brand. The 802.11h standard is backward compatible with 802.11a, but it is likely that 802.11a products produced in the United States will not work with European 802.11h access points.

The HiperLAN2 and 802.11 standards have nearly identical physical layers (PHY) but are very different at the Media Access Control (MAC) level. HiperLAN2 and 802.11 products are thus not interoperable. Technically, 802.11 works as wireless Ethernet, while HiperLAN2 works more like wireless Asynchronous Transfer Mode (ATM).

4. 802.11g Draft

The 802.11g draft uses the ISM 2.4 GHz band, the same one used by 802.11b and 802.11. The fastest rate specified by the 802.11g draft is 54 Mbps, the same as 802.11a. To achieve the same speed as 802.11a, 802.11g specifies the use of two technologies – DSSS at 11 Mbps and below, and OFDM technology at speeds higher than 11 Mbps. OFDM is the same modulation technique used in 802.11a devices, while the use of DSSS modulation and spreading code techniques ensure that 802.11g is backward compatible with 802.11b and 802.11 at 11 Mbps and lower speeds.

The biggest disadvantage of 802.11g is that it is still in the crowded 2.4 GHz ISM band. Equipment that complies with the new 802.11g standard will likely make the situation worse, overcrowding the 2.4 GHz band, which is already flooded by 802.11b products and other wireless devices such as cordless phones. The biggest advantage, however, is that 802.11g is backward compatible with 802.11b products. This backward compatibility could amount to substantial savings to large enterprises that already have large investments in 802.11b products.

5. 802.11i Draft

One of the key concerns of the 802.11 standard is security, specifically the vulnerability of the Wired Equivalent Privacy (WEP) algorithm. 802.11i will provide an alternative to WEP with new encryption methods and authentication procedures. IEEE 802.1x forms a key part of 802.11i along with Extensible Authentication Protocol (EAP) and per-session key distribution.

Security is a major weakness of WLANs. The WEP algorithm is well known to the world and its weakness has been widely publicized. Exploitations of the WEP algorithm are also readily available on open literature and the World Wide Web. To make matters worse, equipment vendors often ship their products without setting default security features. The 802.11i specification is part of a set of security features that should address and overcome these security issues. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with Advanced Encryption Standard (AES) and TKIP backward compatibility. The Wi-Fi Alliance has announced that the Wi-Fi certification will support 802.11i.

6. 802.11f Draft

The purpose of the 802.11f draft is the Inter-Access Point Protocol. This protocol provides inter-vendor roaming by allowing access points to communicate in a standard method.

7. 802.11e Draft

The purpose of the 802.11e draft is to enhance the 802.11 MAC by adding Quality of Service (QoS) and other protocol improvements. Security enhancements were moved from this group to 802.11i. Suggested QoS functions are Enhanced Distributed Coordination Function (E-DCF) and Hybrid Coordination Function (HCF). E-DCF is based on priority queues while HCF is based on a central controller. 802.11e also addresses multicast issues such as multicast group management and multicast acknowledgement.

8. Summary of IEEE WLAN Standards

A table summary of the various IEEE WLAN standards is shown below.

	802.11	802.11b	802.11a	802.11g
Standard Approved	July 1997	September 1999	September 1999	November 2002
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Available Bandwidth	83.5 MHz	83.5 MHz	300 MHz	83.5 MHz
Number of Non-Overlapping Channels	3 (Indoor/ Outdoor)	3 (Indoor/ Outdoor)	4 (Indoor) 4 (Indoor/ Outdoor) 4 (Indoor/ Outdoor)	3 (Indoor/ Outdoor)
Data Rates	1, 2 Mbps	5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
Modulation	FHSS, DSSS	DSSS	OFDM	OFDM
Advertised Range	300 feet	300 feet	225 feet	300 feet
Encryption	40-bit RC4	40-bit, 104-bit RC4	40-bit, 104-bit RC4	40-bit, 104-bit RC4

Table 1. Summary of IEEE WLAN Standards

It is worth pointing out that, although various 802.11 standards point to data rates of up to 54 Mbps, the effective data throughput of all standards is usually less than 50% of the maximum rated throughput. This is due to the nature of radio transmissions using half-duplex communications and the need for overheads for coordination, error correction and other management functions. The FEC alone reduces the effective data throughput to 50% if 1/2 rate coding is used. It is also worthwhile to note that advertised ranges are wildly variable and can be affected, often drastically, by all types and manners of obstructions.

C. IEEE 802.11 ARCHITECTURE

1. Authentication and Association

Authentication is the process a station uses to announce its identity to another station. Authentication is the verification that the client is who it claims to be. By IEEE 802.11 standard, the process does not involve a great deal of checking. The client is either simply accepted under open system authentication or challenged using a shared secret key under shared key authentication.

Association is an IEEE 802.11 service that enables the mapping of a wireless station to the wired distribution system via an access point. The process of association is how a wireless client gets connected to the network. When a client is associated, it is connected to the network and able to pass traffic through the access point to which it is associated.

a. Open System Authentication

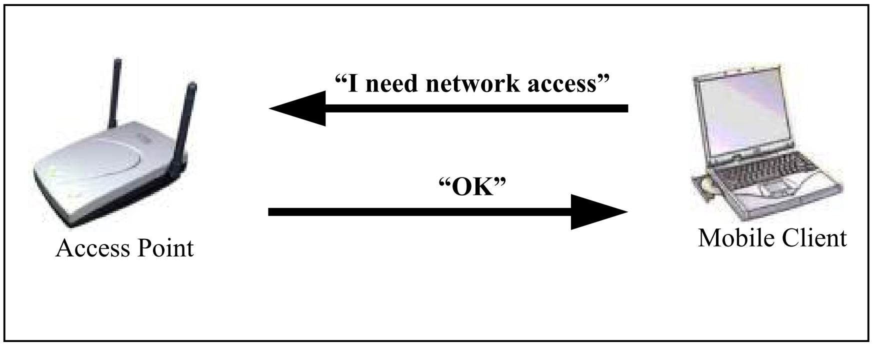

Figure 2. Open System Authentication

Open system authentication is the IEEE 802.11 default authentication method. It consists of a very simple, two step process. First, the station wanting to associate to the network sends an association request frame to the access point. The access point then sends an association response frame alerting the station as to whether it recognizes the identity of the authenticating station. Using this method of authentication, a station can associate with any access point and listen to all data that is sent across that access point – a serious security flaw.

If the WEP algorithm is used with open system authentication, then the client is allowed to associate, but packets being passed between the access point and the station are encrypted. If both the access point and the station do not have the same encryption key, neither will understand anything the other is saying and the received packet is simply dropped.

b. Shared Key Authentication

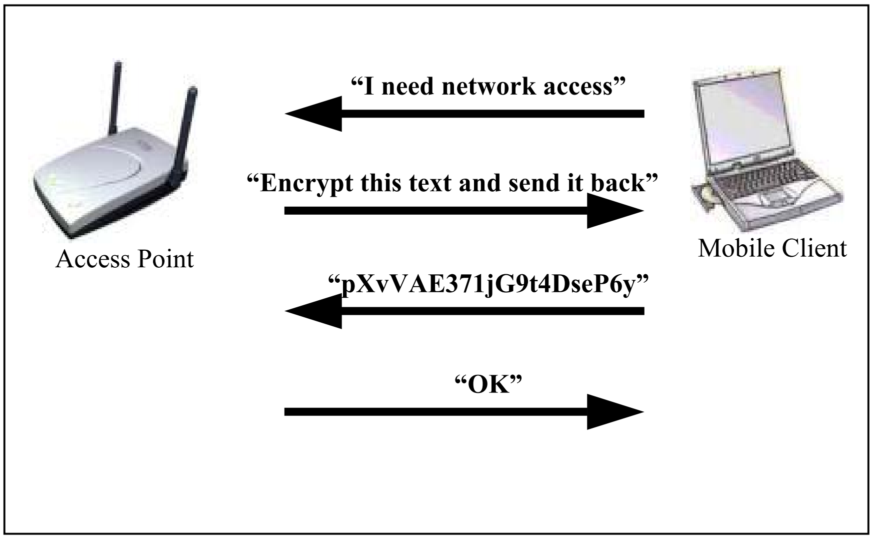

Figure 3. Shared Key Authentication

Shared key authentication is a type of authentication that assumes each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key. The use of shared key authentication requires implementation of the 802.11 WEP algorithm. The WEP key resides in each station's radio card firmware. With shared key authentication, the use of the WEP key is mandatory for authentication and encryption.

The steps to shared key authentication are:

i. The client makes a request to associate by sending an association request frame.

ii. The access point sends a clear text challenge to the client.

iii. The client responds to the access point by sending back the challenge text encrypted using the client's WEP key.

iv. The access point decrypts the challenge text with its own WEP key and compares the decrypted text with the challenge text sent. If they are the same, the access point sends back an association response frame authenticating the client.

Note that because both the challenge text and encrypted response are transmitted into free space, a hacker can collect them readily and then run algorithm to recover the WEP key. This generally means that shared key authentication is not secure. It is generally more secure to use WEP encryption with open system authentication.

2. Service Sets

a. Basic Service Set (BSS)

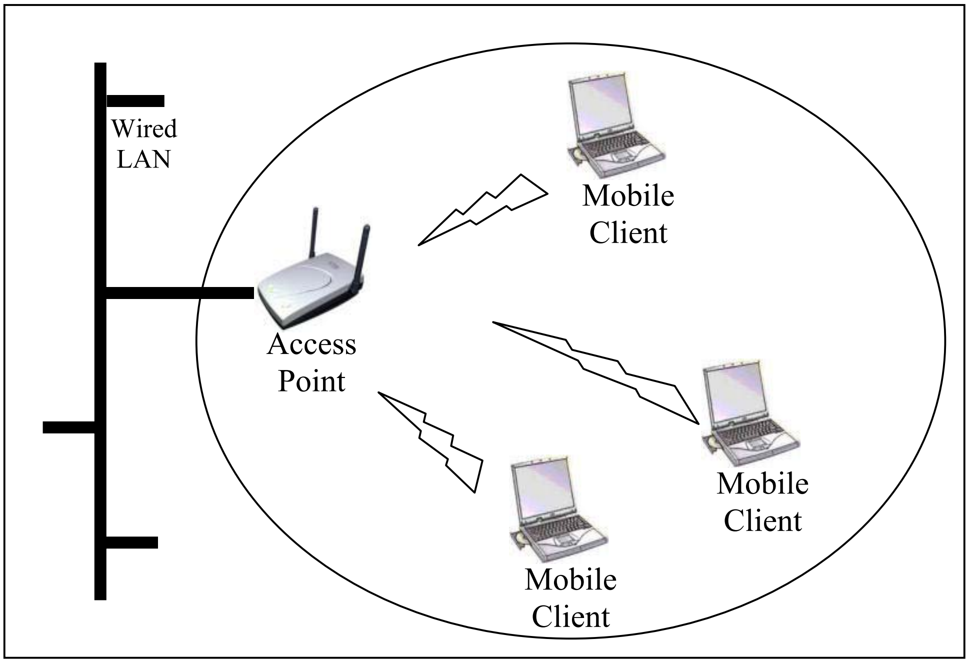

Figure 4. Basic Service Set (BSS)

A BSS is a set of 802.11-compliant stations and an access point that operates as a fully connected wireless network. The use of a BSS is also commonly referred to as an *Infrastructure Mode*. A BSS uses a single cell and a single Service Set Identifier (SSID), the network name. A cell refers to the RF field around an access point. A BSS requires exactly one access point.

When using only one access point, the network is in infrastructure mode by default. In infrastructure mode, when one mobile client sends data to another mobile client, the data must go through the access point. In this mode, the access point acts as the gateway between the WLAN and the wired LAN segment to which the access point is connected.

b. Extended Service Set (ESS)

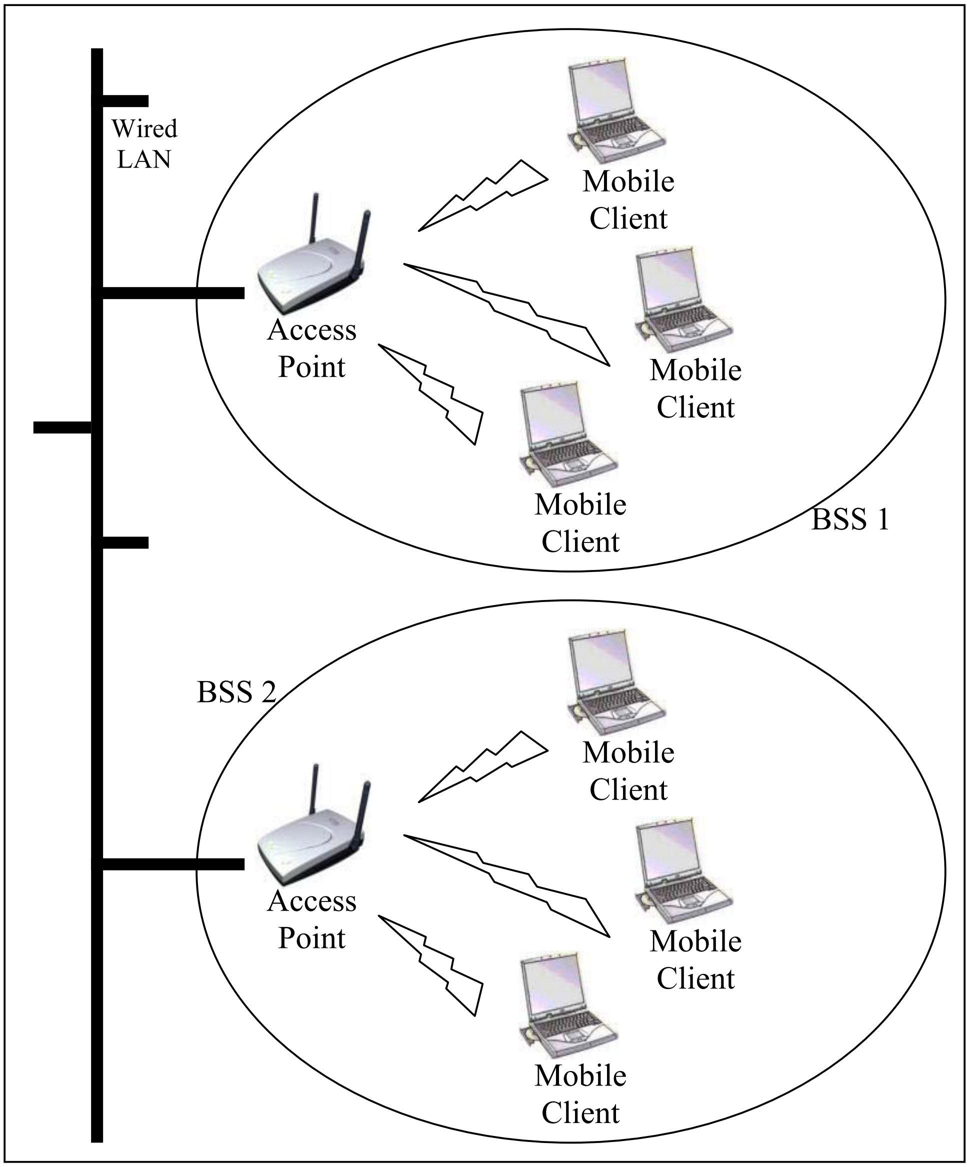

Figure 5. Extended Service Set (ESS)

The IEEE 802.11 standard defines an ESS as a collection of BSS tied together via a common distribution system such as the wired LAN. An ESS, like BSS, is also considered as *Infrastructure Mode*. An ESS must have at least two access points, so that it consists of at least two cells.

The ESS does not have to support roaming, although roaming is allowed and sometimes required based on user needs. Roaming can be seamless or non-seamless depending on how the network is configured and the range of each of the access point. When the cells of the access points overlap, users can roam from one cell to another without losing network connectivity. The IEEE 802.11 standard does not specify that there must be roaming between two or more BSS that form an ESS.

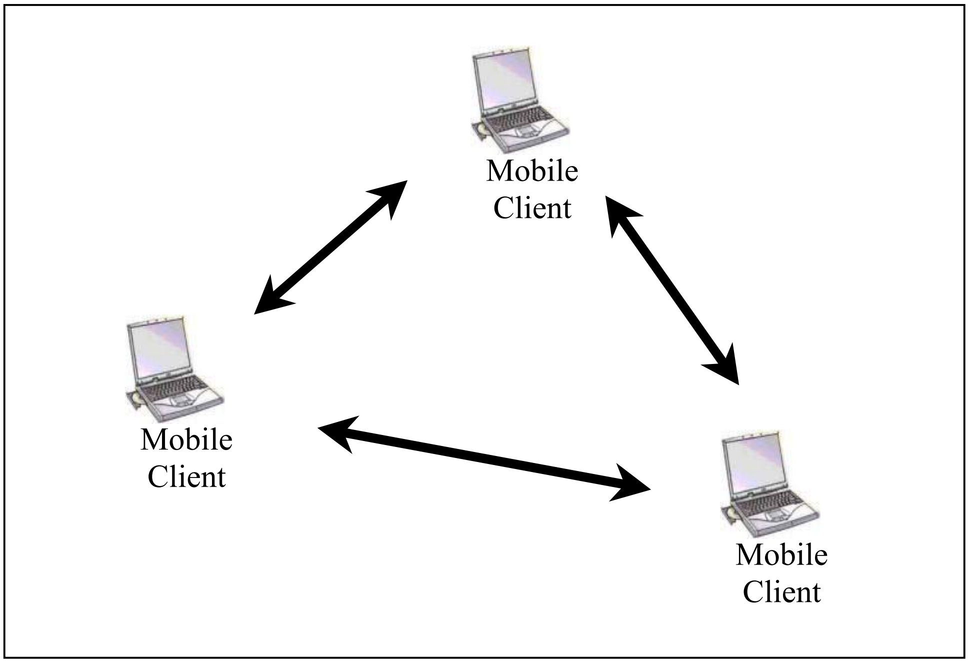

Figure 6. Independent Basic Service Set (IBSS)

c. Independent Basic Service Set (IBSS)

An IBSS is an IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless mobile stations and no access point. This type of network is often referred to as an *ad-hoc* network because it can be constructed quickly without much planning and has no access point with which to connect. Client stations connect directly to each other much like the wired peer-to-peer network. An IBSS has a single cell and one SSID.

In an *ad-hoc* mode, one node (mobile station) must act as a gateway (router) in order to send packets out of the WLAN segment.

3. Beacons

Beacons (short for "beacon management frame") are short frames of data sent from an access point to mobile clients for the purpose of:

- Time synchronization between the clients and the access point
- Passing channel selection information
- Informing clients of supported transmission rates
- Informing clients of DSSS and FHSS parameter sets
- Informing clients of capacity information and supported rates
- Sending the Traffic Indication Map

a. Time Synchronization

For certain features such as power saving mode, the access point and all clients must be time synchronized. When an access point sends a frame, the frame is time-stamped. When the mobile client receives the frame, it reads the time-stamp and updates its clock so that the mobile client and the access point stay synchronized. This process allows any mobile client that is in a power saving mode to wake up at a specified interval to receive beacons.

b. Channel Information, Parameter Sets and Supported Rates

For FHSS systems, the beacons will contain information about the frequency hopping sequence, current transmission frequency, and dwell time. Beacons transmitted using DSSS will contain the channel that is being used. Since there are many speeds of operation for WLANs, the beacons must pass transmission rate capability information. For an 802.11a access point, its beacons will announce support for 6, 9, 12, 18, 24, 36, 48 and 56 Mbps. This lets the mobile clients know at what speed they can connect with the access point.

4. Power Management Modes

Power Saving Poll (PSP) mode, part of the 802.11 standard, allows the client to go to sleep instead of staying on all the time. This feature allows mobile clients to conserve battery life, and keep client devices cooler for longer component life.

It is important to keep in perspective that when the mobile client goes to sleep, they do so in milliseconds, that is, the mobile clients actually turns off and on several times a second. The PSP process relies on the time synchronization mechanism mentioned earlier to get the mobile clients to wake up at the correct interval.

5. Dynamic Rate Shifting

Dynamic Rate Shifting (DRS) is the mechanism that allows data rates to be automatically adjusted for noisy conditions or increased distance between the transmitter and receiver. All 802.11a devices will transmit at lower speeds such as 48, 36, 24, 18, 12, 9 and 6 Mbps as noise increases or separation distance between the access point and mobile client increases. The reverse will also happen – when noise reduces or separation distance decrease, the data rate increases. Data rate selection decision is based primarily on the signal strength of the access point. DRS may also be referred to as Adaptive Rate Selection or Automatic Rate Selection (ARS).

D. 802.11A WLAN CONCEPTS

1. Multipath

Multipath is the effect whereby signals transmitted follow several propagation paths to the receiver. As a result, multiple copies of the transmitted signal arrive at the receiver, each with a different attenuation and time delay. All these combine and produce spatial, frequency and time variations of the signal at the receiver, a characteristic known as fading. Fading produces signal distortion and Inter-Symbol Interference (ISI), and limits the maximum data rate.

The solutions to combat fading and ISI include lowering the data rate and the use of equalizers. Lowering data rate is not desired and equalization usually requires complex processors. There are however more practical multipath resolution methods – the use of space diversity and frequency diversity using OFDM.

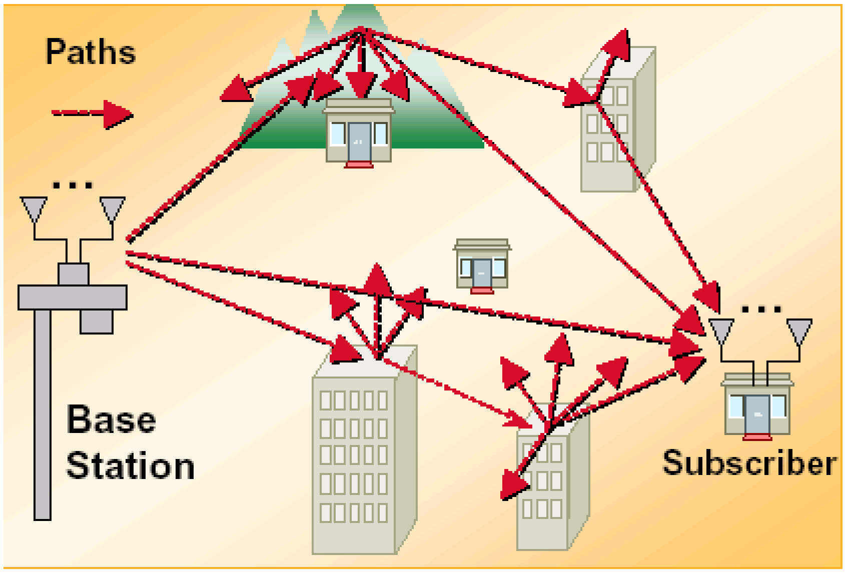

Figure 7. Multipath Illustration (from Ref [18])

2. Antenna Diversity (Space Diversity)

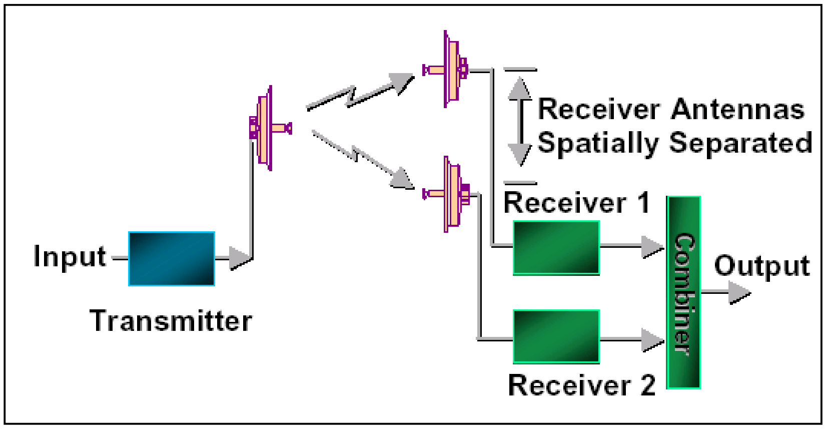

Figure 8. Antenna Diversity (from Ref [18])

Space or antenna diversity is the use of two or more antennas in order to compensate for the negative effects of multipath. The received signals are then combined so that the resultant signal will have a higher signal-to-noise ratio. Note however that the space diversity method does not allow for higher data rate.

Incidentally, the need for space diversity for 802.11a applications resulted in equipment vendors supplying PC cards for mobile clients with integrated, non-removable space diversity antenna.

3. OFDM (Frequency Diversity)

OFDM is the technique to code high-speed data stream as multiple low-rate streams, that is, to transmit the data stream over multiple channels (frequencies) in parallel at lower rates that will not be adversely affected by fading.

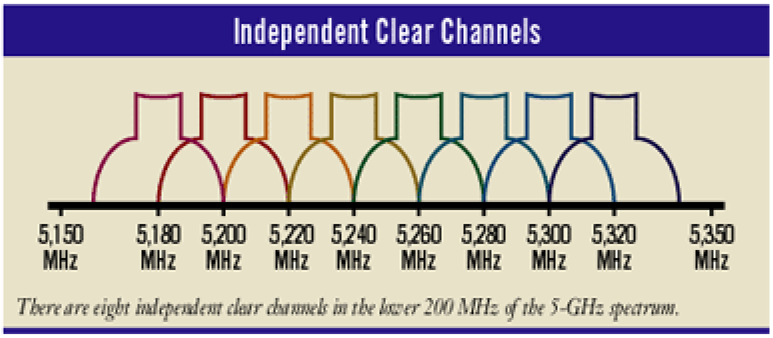
Independent Clear Channels
5,150 MHz
5,180 MHz
5,200 MHz
5,220 MHz
5,240 MHz
5,260 MHz
5,280 MHz
5,300 MHz
5,320 MHz
5,350 MHz
There are eight independent clear channels in the lower 200 MHz of the 5-GHz spectrum.

Figure 9. Eight Independent Clear Channels in lower 5-GHz Band (from Ref [19])

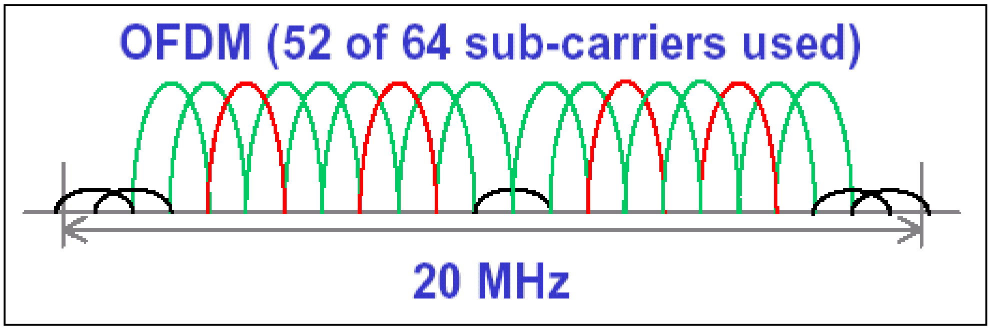

Figure 10. OFDM Subcarriers In Each Channel (from Ref [20])

As described earlier, 802.11a is assigned with eight independent clear channels of 20 MHz each in the band 5.15 – 5.35 GHz. The 20 MHz channel is further sub-divided into 64 sub-channels or subcarriers. The 64 subcarriers are used as follows:

a. 12 zero subcarriers (unused) on the sides and the center (shown in black in Figure 10). The zero subcarriers on the sides provide the guard bands and those at the center provide DC offset or carrier leak rejection.

b. 48 data subcarriers as the frequency diversity channels for data (shown as green in Figure 10).

c. 4 pilot subcarriers for synchronization and tracking (shown as red in Figure 10).

Each subcarrier can be encoded independently of the others. The data encoding can be either BPSK, QPSK, 16-QAM or 64-QAM, providing 1, 2, 4 or 6 bits per symbol respectively. For increased robustness, convolutional coding is used at rates of 1/2, 2/3 or 3/4.

With the sampling rate of 250,000 symbols per second, the overall data rates that can be achieved using OFDM are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The lowest rate results from the combination of BPSK and 1/2 rate convolutional coding, giving the minimum data rate of (48 subcarriers * 1 bit/symbol * 1/2 rate * 250,000 symbols/s) = 6 Mbps. Similarly, the highest rate is achieved by using 64-QAM with 3/4 rate convolutional coding, giving the maximum data rate of (48 subcarriers * 6 bit/symbol * 3/4 rate * 250,000 symbols/s) = 54 Mbps.

E. APPLICABLE FORMULAE

This portion of Chapter II covers all applicable formulas use in the thesis.

1. Free-Space Path Loss

As the transmitted RF signal traverses the atmosphere, its power level decreases at a rate inversely proportional to the distance traveled and proportional to the wavelength of the signal. To account only for the effect of diminishing voltage as the signal propagates, the following free-space path loss formula is used:

$$L_O = \left(\frac{4\pi d}{\lambda}\right)^2 \tag{2.1}$$

where λ is the wavelength of the signal.

d is the distance in meters between the transmitter and receiver.

The wavelength λ of the signal can be calculated from

$$\lambda = \frac{c}{f} \tag{2.2}$$

where c is the speed of light in meters per second.

f is the frequency of the signal in hertz.

Note that equation (2.1) does not account for absorption or dispersion by the atmosphere, which are not severe at the 5 GHz band for 802.11a. A logarithmic version of the free-space path loss equation in (2.1) may be derived by taking (10 log) of both sides of the equation to eliminate the need for division:

$$10\log L_O = 10\log\left(\frac{4\pi d}{\lambda}\right)^2 = 20\log\left(4\pi\right) + 20\log d - 20\log\lambda \qquad (2.3)$$

Using equation (2.2) to eliminate λ,

$$L_{O(dB)} = 20\log\left(\frac{4\pi}{c}\right) + 20\log d + 20\log f$$

$$L_{O(dB)} = -147.6 + 20\log d_{(m)} + 20\log f_{(Hz)} \qquad (2.4)$$

For the purpose of this thesis, where the expected distance between the access point and mobile client is in feet, and the frequency is around 5 GHz, it is more convenient to express equation (2.4) for distance in feet and frequency in GHz. Thus, the final version of the logarithmic formula is

$$L_{O(dB)} = 22.1 + 20\log d_{(ft)} + 20\log f_{(GHz)} \qquad (2.4)$$

where $d_{(ft)}$ is the distance in feet between the transmitter and receiver.

$f_{(GHz)}$ is the frequency of the signal expressed in GHz.

2. Distance Determination Using Location Coordinates

In this thesis, distance between the transmitter and receiver is provided by a GPS receiver in navigation mode. However, the GPS receiver is also able to provide the coordinates for each location. The distance between two locations can therefore be derived from the location coordinates using geometrical calculations.

As a start, the earth is assumed to be a perfect sphere (to simplify calculations) although it is a tad wider than it is tall, giving it a slight bulge at the equator. Earth's shape is usually described as an ellipsoid or more properly, geoid (earth-like).

Next, the circumference of the earth at the equator is assumed to be 24,901.55 miles [7] or about 21,638.86 nautical miles, making it about 69.2 miles (60 nautical miles) for each degree of longitude and latitude at the equator.

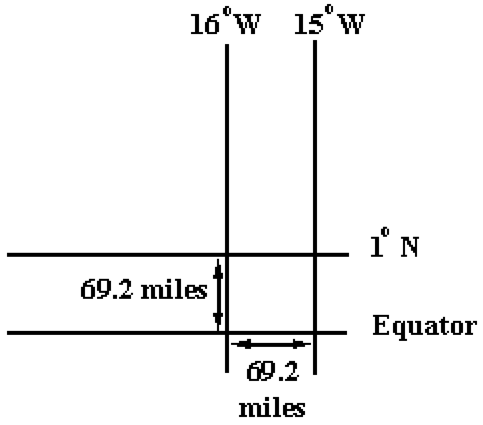

Figure 11. Latitude and Longitude Distance at Equator (from Ref [7])

For the United States, the distance for each degree of latitude can be assumed to be 69.2 miles.

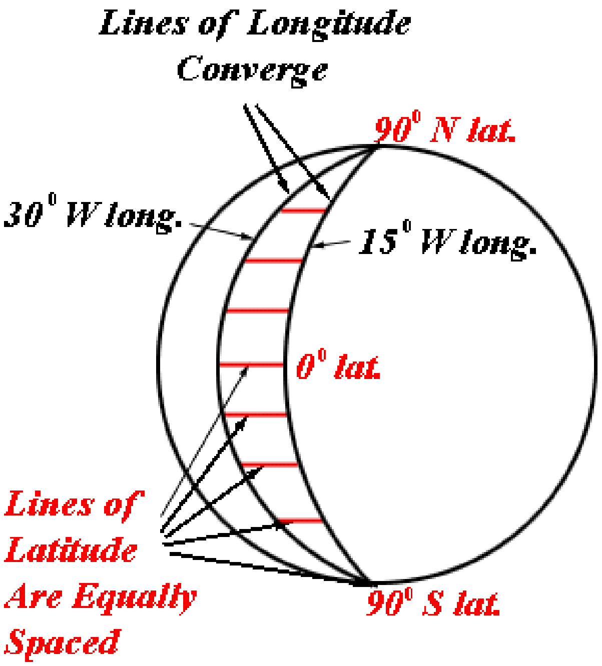
Lines of Longitude Converge
90° N lat.
30° W long.
15° W long.
0° lat.
Lines of Latitude Are Equally Spaced
90° S lat.

Figure 12. Variances of Latitude and Longitude (from Ref [7])

However, unlike the lines of latitude that remains equally spaced, the lines of longitude get closer and closer together towards the poles of the earth. For example, at the equator, the distance between $15°W$ and $30°W$ longitude is quite a lot. But as the two longitude lines move towards the poles, the distance between them shrinks down to zero to meet at the poles. To account for this 'shorter' distance between longitudes at latitudes other than the equator, the distance can be approximated by

$$1^\circ\, \mathit{longitude} = \cos\left(\mathit{latitude}\right)\times\left(69.2\right)\, \mathit{miles} \tag{2.5}$$

For the area around the Naval Postgraduate School in Monterey, California the latitude is around $36^\circ 35'$. This means that the geometrical distances applicable are

$$1^\circ\, \mathit{latitude} = 69.2\, \mathit{miles} \tag{2.6}$$

$$1^\circ\, \mathit{longitude} = \cos\left(36^\circ 35'\right)\times\left(69.2\right) = 55.6\, \mathit{miles} \tag{2.7}$$

To calculate the distance between two GPS coordinates, the difference in both the latitude and longitude coordinates are first determined. The difference in latitude is then multiplied by 69.2 while the longitude difference is multiplied by 55.6. The square root of the squares of these values is finally calculated to derive at the separation distance.

$$\mathit{Separation} = \sqrt{\left(\Delta \mathit{latitude}\times 69.2\right)^2 + \left(\Delta \mathit{longitude}\times 55.6\right)^2}\ \mathit{miles} \tag{2.8}$$

To convert to feet, the result is simply multiplied by 5,280 (1 mile = 5,280 feet).

$$\mathit{Separation} = \sqrt{\left(\Delta \mathit{latitude}\times 69.2\right)^2 + \left(\Delta \mathit{longitude}\times 55.6\right)^2}\ \times 5{,}280\, \mathit{feet} \tag{2.9}$$

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROTOTYPE DEVELOPMENT

A. REQUIREMENT REVIEW

The main requirement of the prototype system is to detect and process 802.11a compliant WLAN signals for tasks such as detecting other WLAN networks and assessing the vulnerability of one's own WLAN network. The following are desired characteristics for the prototype system:

1. Use of commercially available low cost hardware and software.
2. Capture, decode and display 802.11a traffic and information in real-time.
3. High sensitivity to capture 802.11a signals from long ranges.
4. Highly portable for mobility.
5. Good processing power and large storage capacity for captured data.

B. SOFTWARE SELECTION

The only software that is required for the prototype system is a suitable *protocol analyzer* to capture the desired 802.11a WLAN signals.

A protocol analyzer is a network management tool that captures traffic on a network for the purpose of ensuring that the network is functioning as expected. Protocol analyzers are usually regarded as testing and planning tools – it is not required unless there is network to maintain, or troubleshoot. This is generally true for wired networks such as the Ethernet.

However, for WLAN, things are different. Because the WLAN physical medium is the electromagnetic spectrum – which exists everywhere and respects few boundaries – WLAN protocol analyzers have been used increasingly for reasons other than a maintenance and troubleshooting tool. Simple protocol analyzers that can be downloaded free from the Internet have been used for 'war driving' by hackers to canvass a region by car to locate unsecured access points [6]. To deal with the threat of such intruders, both casual and professional, more complex protocol analyzers have been marketed to detect and track down rogue access points, and for security vulnerability assessments.

1. Available WLAN Analyzers

As stated earlier, there are many protocol analyzers available for capturing WLAN signals. Some are plain simple implementations – a Wi-Fi equipped laptop running Windows XP or Mac OS X can automatically log on to any open wireless network available. On the other end, there are full-fledge Wi-Fi protocol analyzers that not only capture and decode 802.11a packets at the MAC layer, they are able to understand IP and filter packets by address.

Both Andy Dorman [8] and Tom Henderson [9] have done some impressive work comparing and surveying available WLAN protocol analyzers. Both their works cover 802.11b and 802.11a analyzers. For the purpose of this thesis, an 802.11a WLAN protocol analyzer is required. Based on these works, software-based Wi-Fi protocol analyzers suitable for a laptop-based prototype system are listed. Note that laptop-based analyzers are selected as opposed to PDA-based (Personal Digital Assistant) or Handheld-based system simply because of available screen size for simultaneous display of important information for real-time analyses.

Program	Vendor	Platforms	802.11 Type	NIC Required	Layers
AirMagnet Laptop	AirMagnet www.airmagnet.com	Win 98, NT 4, 2000, XP	b and a	Supplied PC or CF+ Card	2-4
AiroPeek NX	WildPackets www.wildpackets.com	Win 2000, XP	b or a	Any Intersil- or Atheros-based	2-7
LANFielder	Wireless Valley Communications www.wirelessvalley.com	Win 98, NT 4, 2000, XP	b, a or FH	Cisco Aironet	2,3
Observer	Network Instruments www.networkinstruments.com	Win 98, NT 4, 2000, XP	b or a	Cisco Aironet, Proxim Skyline	2-7
Sniffer Wireless	Network Associates www.sniffer.com	Win 98, NT 4, 2000, XP	b or a	Proxim, Cisco, Symbol, Agere	2-7

Table 2. Software-based Wi-Fi Protocol Analyzers for Laptops (After Ref [8])

Of all the available Wi-Fi protocol analyzers, only the AiroPeek NX and Sniffer Wireless have the ability to perform analysis for OSI (Open System Interconnect) layers 2 to 7, and the flexibility to use commercially available 802.11a-compliant Network Interface Cards (NIC).

It is interesting to note that the software candidates for the prototype system coincide with the selected protocol analyzers in a prior thesis by Walter N. Currier Jr. [1]. In the thesis, he has evaluated earlier versions of these two protocol analyzers, the Sniffer Pro 4.6 and the AiroPeek 1.1012. Based on the evaluation, AiroPeek 1.1012 had been recommended over the Sniffer Pro 4.6 based on its "sufficient capture capabilities, significant cost savings, and easy-to-use filtering capability" [1].

In terms of cost, as of December 2003, Sniffer Wireless costs $8,162 for a yearly subscription license [10] while the AiroPeek NX costs $2,500 for a 12-month license and maintenance contract [11]. The AiroPeek NX is therefore still the selected protocol analyzer for the prototype system.

C. HARDWARE SELECTION

Based on the desired characteristics, the prototype system will need to be a laptop-based system, running WLAN detection, decoding and analyzing software, with an 802.11a hardware card as the receiver. The following section describes the selection of the hardware components of the prototype system.

1. Laptop Selection

The primary considerations for laptop selection are processing power and storage capacity. In addition, in order to capture, decode and display 802.11a traffic and information in real-time, it is necessary that the laptop has a large screen with at least 1600 x 1200 pixel resolution for displaying as much information as possible simultaneously.

For this thesis, an existing laptop platform, the Dell Latitude C840, with configurations listed in Table 3 is used.

In the context of low-cost, however, the most cost-effective solution is usually the recommended configuration packages offered by laptop manufacturers such as Dell, Gateway and HP. Customizations can then be done to arrive at the desired configuration.

System Configuration	
Computer Processor	Intel Pentium 4 Mobile 1.8 GHz
Operating System	Windows XP Professional
Display	UXGA 15", 1600 x 1200 pixels
Installed RAM	512 MB
Hard-disk Capacity	20 GB
Secondary Storage	CD Read/Write Drive

Table 3. Dell Latitude C840 Configuration

2. Available Hardware for 802.11a Reception

At the onset of the thesis, only the Linksys WPC54A 802.11a PC card is available for experimentation. Subsequently, two more 802.11a compliant cards, the Proxim ORiNOCO GOLD 11a/b/g ComboCard (8480-WD) and Cisco AiroNet AIR-CB20A 802.11a Client Adaptor are purchased and made available for experimentation. The following paragraphs provide descriptions for the three available 802.11a cards for this thesis.

a. Linksys WPC54A PC Card

Figure 13. Linksys Instant Wireless PC Card (from Ref [12])

The WPC54A PC Card from Linksys is an 802.11a PCMCIA Card that is developed for Small Office/Home Office (SOHO) applications, that is, mainly for home use. The WPC54A, like all other 802.11a cards, has a fixed (integrated) antenna that is not removable. Based on the specifications [12], the WPC54A has a new higher-powered antenna that provides greater ranges and Linksys claims that the WPC54A has increased sensitivity that helps filter out interference and “noise” to keep the 802.11a signal clear. Linksys also claim that the WPC54A incorporated improved error correction in its chipset to keep it “operating at higher transmission rates for longer distances” [12]. The WPC54A is capable of up to 152-Bit WEP Security.

The WPC54A card operates on 8 non-overlapping channels (channel 36, 40, 44, 48, 52, 56, 60 and 64) in the Lower and Middle UNII bands. The Lower UNII band (5.15 – 5.25 GHz) is designated for indoor use only, while the Middle UNII band (5.25 – 5.35 GHz) is designated for both indoor and outdoor use. If used in conjunction with Linksys 802.11a access point WAP54A, the WPC54A is able to provide up to 72 Mbps (more than the 802.11a specified maximum of 54 Mbps) under its proprietary “turbo” mode. The exact receive sensitivity of the WPC54A, which is a critical specification for the prototype system, is not available from the specifications. Neither is the transmit power of the WPC54A available from specifications.

The WPC54A also has a feature known as Integrated Hardware Power Management that varies its transmit power to conserve the battery life of the laptop. For the purpose of this thesis, the transmit power is always set to the maximum for all experimentations.

b. Proxim ORiNOCO GOLD 11a/b/g ComboCard Gold

Figure 14. ORiNOCO 11a/b/g ComboCard Gold (from Ref [13])

The ORiNOCO 11a/b/g ComboCard is Proxim's solution to allow the convenience of secure connections to 802.11b, 802.11a and 802.11g networks from a single card. The ORiNOCO ComboCard, like the WPC54A, has a fixed (integrated) antenna that is not removable. However, unlike WPC54A, the 802.11a portion of the ORiNOCO ComboCard (Gold version) is operable on all the 12 non-overlapping channels (channel 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157 and 161) in the entire UNII band (5.15 – 5.35 GHz, 5.725 – 5.85 GHz). When used in conjunction with a Proxim access point, the ORiNOCO ComboCard is able to deliver up to 108 Mbps under Proxim's proprietary "2X" mode. The ORiNOCO ComboCard (Gold version) is also capable of up to 152-Bit WEP Security.

Based on the specifications [13], the ORiNOCO ComboCard (Gold version) has a transmit power of 60 mW (equivalent to +17.8 dBm) in 802.11a mode. Its receive sensitivity, a critical consideration for the prototype system, is not stated.

The ORiNOCO ComboCard (Gold version) also has a transmitter power control feature, which is disabled in experimentations in this research – the transmit power is always set to the maximum.

c. Cisco AiroNet AIR-CB20A Client Adapter

Figure 15. Cisco AiroNet AIR-CB20A Client Adapter (from Ref [14])

The Cisco Aironet AIR-CB20A 5 GHz 54 Mbps WLAN client adapter is an 802.11a-compliant CardBus adapter that operates in the Lower and Middle UNII bands (5.15 – 5.35 GHz), on channels 36, 40, 44, 48, 52, 56, 60 and 64. It has a maximum data rate of 54 Mbps. Like all other 802.11a cards, it incorporates an integrated, non-removable antenna. According to the specifications [14], the integrated patch antenna has a gain of 5 dBi.

Based on Cisco's datasheet, the AiroNet AIR-CB20A has an advanced signal processing feature that helps to manage the multipath propagation often found in office environments and an intelligent filtering process that addresses ambient noise and interference that can decrease network performance [14]. The AiroNet AIR-CB20A also has a variable transmit power setting (20 mW, 10 mW and 5 mW) that is set to maximum for this thesis. Coupled with the integrated 5 dBi gain patch antenna, the Effective Isotropically Radiated Power (EIRP) from the AiroNet AIR-CB20A is +18 dBm.

Cisco has very detailed receiver sensitivity for the AiroNet AIR-CB20A, and is presented in Table 4.

Receive Sensitivity (typical)	
Data Rate	Sensitivity
6 Mbps	-85 dBm
9 Mbps	-84 dBm
12 Mbps	-82 dBm
18 Mbps	-80 dBm
24 Mbps	-77 dBm
36 Mbps	-73 dBm
48 Mbps	-69 dBm
54 Mbps	-68 dBm

Table 4. Cisco AiroNet AIR-CB20A Sensitivity (After Ref [14])

3. Sensitivity Measurements (LOS)

While the receiver sensitivities for the Cisco AIR-CB20A is available, those of ORiNOCO ComboCard and Linksys WPC54A are not. An equitable comparison methodology is thus required to determine which of the 3 available 802.11a-compliant card is best suited for the prototype system.

a. Test Set-up

Figure 16. Linksys WAP55AG Access Point (from Ref [17])

To test the receive performances, the Linksys WAP55AG access point is used as a source of 802.11a packets for collection by the 3 802.11a-compliant cards. The WAP55AG is a Dual-Band Wireless A+G Access Point that contains two separate radio transceivers, supporting 802.11a in the 5 GHz band at 54 Mbps, and 802.11g in the 2.4 GHz at 54 Mbps. Based on specifications, the transmitted power of the WAP55AG in 802.11a bands is +16 dBm (equivalent to 40 mW).

In this measurement, the WAP55AG Access Point is set up to continuously transmit beacons at the rate of one per 100 ms (or 10 beacons per second). The beacon frames, which are 67 bytes in length, are transmitted at 6 Mbps on channel 52. Channel 52 is arbitrarily chosen because it is the first channel in the middle UNII band for outdoor use. Also, based on equation (2.4), the free-space propagation loss is not affected much even if another channel within the band is selected.

The access point is set for open authentication with no WEP encryption. All three 802.11a-compliant cards are then used with the AiroPeek NX software in the prototype system to capture the beacon frames from the WAP55AG. The prototype system is stationed at various distances away from the location of the WAP55AG, and at least 500 packets of the beacon signal are captured for each measurement.

To determine the exact location of each of the measurement points, the Garmin *e*trex handheld GPS receiver is used. The GPS has an accuracy of 19 feet, and using the navigation function, distances at 100 feet intervals are marked out along the line-of-sight (LOS) path from the access point position. As an added assurance, the location coordinates of the measurement points displayed by the GPS device are recorded. A view of the measurement environment is shown in Figure 17.

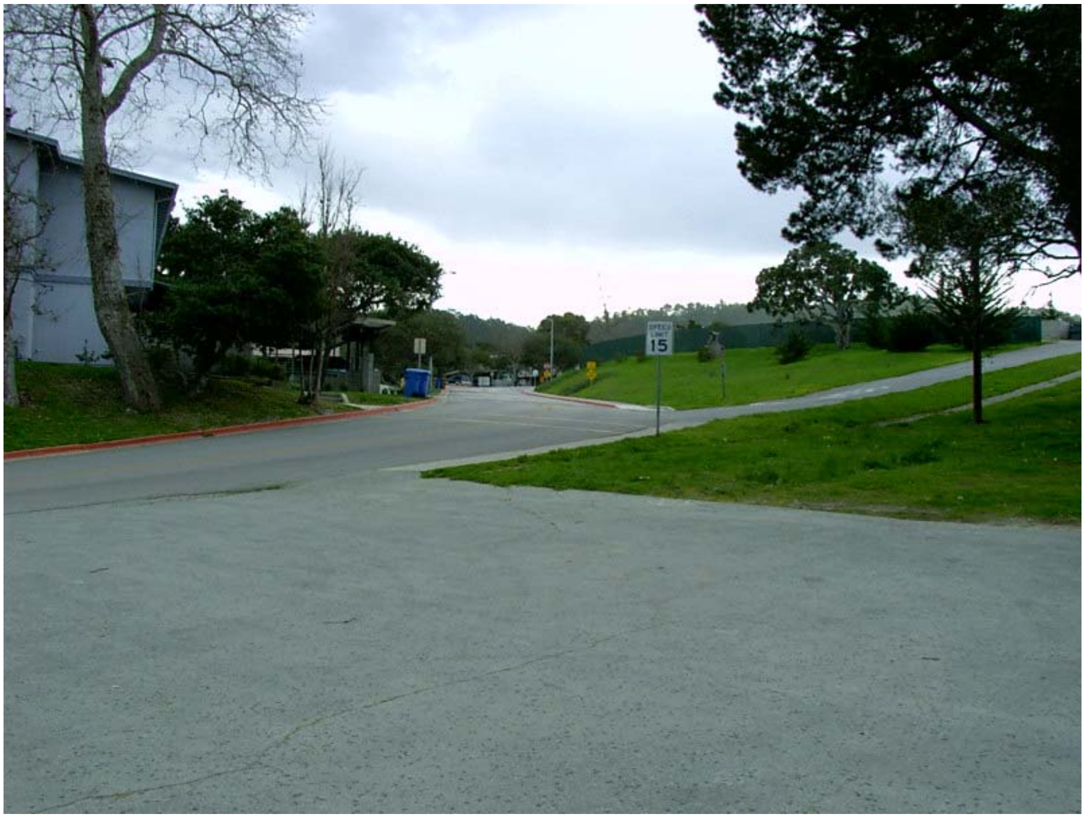

Figure 17. LOS Measurement Environment

The location coordinates provided by the GPS receiver is listed in Table 5, along with the exact separation distance calculated using equation (2.9) developed earlier. The calculations showed that the accuracy of the GPS receiver is within tolerance.

At each location, about 500 packets of beacons are captured for each measurement. To account for variations in measurement, 3 sets of measurements are performed for each of the 802.11a card. For all the measurements, packet filtering is used so that the 802.11a card captures only beacons from the Linksys access point.

Location	Coordinates	Distance from equation (2.9)
Access Point	N 36°34'53.7" W121°52'34.8"	-
100 feet	N 36°34'52.8" W121°52'34.5"	94.6
200 feet	N 36°34'51.8" W121°52'34.2"	198.9
300 feet	N 36°34'50.9" W121°52'33.7"	298.0
400 feet	N 36°34'50.0" W121°52'33.2"	397.5
500 feet	N 36°34'49.1" W121°52'32.9"	491.9
600 feet	N 36°34'48.2" W121°52'32.6"	586.3
700 feet	N 36°34'47.4" W121°52'32.0"	679.0

Table 5. Location Coordinates of LOS Measurement Points

b. Expected Results

The expected signal strength at various distances can be predicted from equation (2.4) derived in Chapter II. As mentioned earlier, the access point WAP55AG is transmitting at a power of +16 dBm. Substituting the frequency of 5.26 GHz and the various distances into equation (2.4), the expected signal strength assuming an LOS path with no multipath effects are tabulated in Table 6.

A point to note is that, although the measurement environment does provide direct LOS path between the access point and the prototype system, there will still be multipath effects. Table 6 is therefore used only as a preliminary gauge of the expected signal strength at the various measurement points. Actual measurement is expected to deviate from these values. Also, both the 600 and 700 feet measurement points are located within an area that is flanked by buildings on both sides. The expected signal strength at these points is therefore expected to suffer more losses due to multipath.

Location	Expected Signal Strength
100 feet	-60.5 dBm
200 feet	-66.5 dBm
300 feet	-70.1 dBm
400 feet	-72.6 dBm
500 feet	-74.5 dBm
600 feet	-76.1 dBm
700 feet	-77.4 dBm

Table 6. Expected Signal Strength at Various Distances

c. *Measurement Results and Analyses*

For each capture, the average signal strength as detected by the 802.11a card under test, the number of packets captured and the number of packets captured in error are recorded.

Distance	Test Number	Average Signal	Number of Packets	Number of Error Packets
100 feet	Capture 1	69% / -52 dBm	507	0
	Capture 2	70% / -52 dBm	507	0
	Capture 3	70% / -52 dBm	506	0
200 feet	Capture 1	50% / -65 dBm	507	0
	Capture 2	50% / -65 dBm	504	0
	Capture 3	51% / -64 dBm	503	0
300 feet	Capture 1	38% / -72 dBm	504	0
	Capture 2	39% / -72 dBm	504	0
	Capture 3	40% / -71 dBm	503	0
400 feet	Capture 1	48% / -66 dBm	502	0
	Capture 2	50% / -65 dBm	505	0
	Capture 3	49% / -66 dBm	505	0
500 feet	Capture 1	46% / -67 dBm	503	0
	Capture 2	47% / -67 dBm	503	0
	Capture 3	45% / -68 dBm	504	0
600 feet	Capture 1	42% / -79 dBm	519	0
	Capture 2	32% / -75 dBm	636	0
	Capture 3	34% / -75 dBm	512	0
700 feet	Capture 1	12% / -87 dBm	507	28
	Capture 2	13% / -87 dBm	508	6
	Capture 3	12% / -87 dBm	508	33

Table 7. Measurement Results for Linksys WPC54A

The measurement results for Linksys WPC54A are tabulated in Table 7. From the measurement, it is observed that the signal strength reported by the Linksys WPC54A suffered a sudden drop at both the 200 and 300 feet point. This is likely due to multipath effects pointed out earlier. Comparing the signal strength reported by the Linksys WPC54A against the expected values in Table 6, it is noted that the values reported by the WPC54A is slightly higher in most cases except at the 300, 600 and 700 feet measurement points.

From the capture files, it is also observed that packet errors start to occur severely at signal strengths of about -86 dBm.

Distance	Test Number	Average Signal	Number of Packets	Number of Error Packets
100 feet	Capture 1	51% / -59 dBm	502	0
	Capture 2	48% / -61 dBm	502	0
	Capture 3	53% / -58 dBm	502	0
200 feet	Capture 1	29% / -72 dBm	502	0
	Capture 2	28% / -75 dBm	502	0
	Capture 3	27% / -76 dBm	502	0
300 feet	Capture 1	37% / -69 dBm	502	0
	Capture 2	42% / -65 dBm	502	0
	Capture 3	34% / -71 dBm	502	0
400 feet	Capture 1	32% / -72 dBm	502	0
	Capture 2	34% / -71 dBm	502	0
	Capture 3	31% / -73 dBm	501	0
500 feet	Capture 1	32% / -72 dBm	502	0
	Capture 2	32% / -72 dBm	502	0
	Capture 3	34% / -71 dBm	502	0
600 feet	Capture 1	26% / -77 dBm	502	0
	Capture 2	28% / -75 dBm	502	0
	Capture 3	29% / -72 dBm	502	0
700 feet	Capture 1	10% / -88 dBm	501	4
	Capture 2	12% / -86 dBm	508	6
	Capture 3	13% / -85 dBm	507	8

Table 8. Measurement Results for ORiNOCO ComboCard

The measurement results for the ORiNOCO ComboCard are tabulated in Table 8. Similar results due to the multipath effects at the 200 feet point are observed. Comparing the signal strength reported by the ORiNOCO ComboCard against the expected values in Table 6, it is noted that the values are very close. Deviations at the 200 and 700 feet points are expected.

From the capture files, it is also observed that packet errors start to occur at signal strengths of about -85 dBm. The packet errors, however, are not as severe as the case for Linksys WPC54A.

Distance	Test Number	Average Signal	Number of Packets	Number of Error Packets
100 feet	Capture 1	36% / -20 dBm	505	0
	Capture 2	34% / -20 dBm	507	0
	Capture 3	42% / -20 dBm	504	0
200 feet	Capture 1	23% / -45 dBm	501	0
	Capture 2	20% / -55 dBm	503	0
	Capture 3	21% / -55 dBm	506	0
300 feet	Capture 1	18% / -60 dBm	506	0
	Capture 2	18% / -60 dBm	506	0
	Capture 3	17% / -60 dBm	505	0
400 feet	Capture 1	25% / -40 dBm	506	0
	Capture 2	20% / -55 dBm	505	0
	Capture 3	23% / -45 dBm	507	0
500 feet	Capture 1	14% / -70 dBm	507	2
	Capture 2	13% / -70 dBm	507	7
	Capture 3	15% / -65 dBm	506	1
600 feet	Capture 1	17% / -60 dBm	519	8
	Capture 2	15% / -65 dBm	508	4
	Capture 3	16% / -65 dBm	509	0
700 feet	Capture 1	12% / -75 dBm	510	36
	Capture 2	11% / -75 dBm	508	11
	Capture 3	11% / -75 dBm	508	14

Table 9. Measurement Results for Cisco AIR-CB20A

The measurement results for the Cisco AIR-CB20A are tabulated in Table 9. Similar results due to the multipath effects at the 200 and 300 feet points are observed.

When the signal strengths reported by Cisco is compared with the expected values in Table 6, it is noted that the Cisco values are grossly misrepresented, especially at the nearer distances of 100 and 200 feet. Incidentally, this observation is consistent with those in the thesis by Walter N. Currier Jr. [1].

From the capture files, it is also observed that packet errors start to occur as early as the 500 feet point. This corresponds to signal strengths of about -74.5 dBm based on Table 6, or about -65 dBm as reported by the Cisco AIR-CB20A. The packet error also becomes more severe at 700 feet.

Based on the three sets of results, a combined table for performance comparison is presented in Table 10. The signal strength is averaged for the three captures and the packet error rate (PER) is computed.

Distance (feet)	Linksys		ORiNOCO		Cisco		Theoretical {eqn (2.4)} (dBm)
	Signal (dBm)	PER	Signal (dBm)	PER	Signal (dBm)	PER	
100	-52	0	-58	0	-20	0	-60.5
200	-64	0	-72	0	-45	0	-66.5
300	-71	0	-69	0	-60	0	-70.1
400	-66	0	-71	0	-45	0	-72.6
500	-67	0	-72	0	-70	0.006	-74.5
600	-73	0	-75	0	-65	0.008	-76.1
700	-87	0.044	-86	0.012	-75	0.040	-77.4

Table 10. Combined Measurement Results

From the combined results, it is quite obvious that the ORiNOCO ComboCard performs better than both the Cisco AIR-CB20A and the Linksys WPC54A. The signal strength measurement of the ORiNOCO is the closest to the theoretical values, and the PER is the lowest among the three under severe multipath environment at the 700 feet measurement point.

4. Sensitivity Measurements (Non-LOS)

To further validate the result that suggests that the ORiNOCO ComboCard is the best 802.11 card, a simple measurement for non-LOS measurement is carried out.

a. Test Set-up

The same Linksys WAP55AG access point is set up in the microwave laboratory in Spanagel Hall of the Naval Postgraduate School. The access point is set up such that the access point over-looks an area with trees and flanked by two buildings. The measurement environment is shown in Figure 18.

Three locations are arbitrarily chosen, and the location coordinates and distance with respect to the access point is tabulated in Table 11.

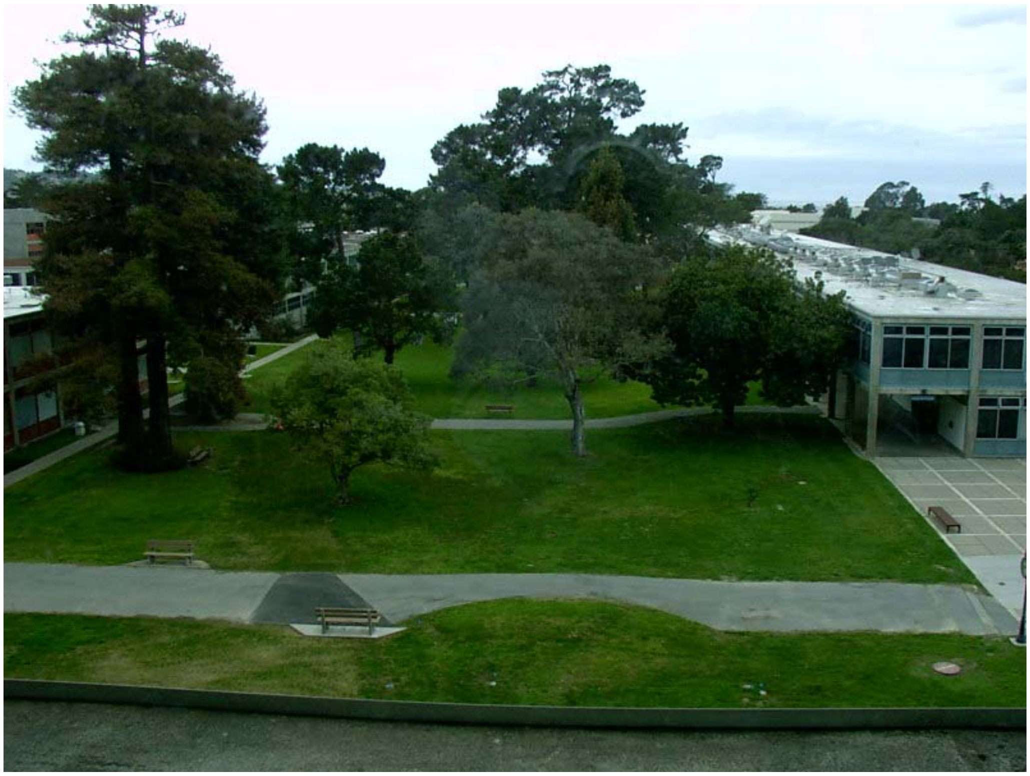

Figure 18. Non-LOS Measurement Environment

AP Location	System Location	Distance (from GPS)	Distance eqn (2.9)	Remarks
N 36°35'42.1" W121°52'29.7"	N 36°35'42.8" W121°52'31.0"	150 feet	127.6	Under trees
N 36°35'42.1" W121°52'29.7"	N 36°35'43.5" W121°52'32.7"	300 feet	282.9	LOS blocked by trees
N 36°35'42.1" W121°52'29.7"	N 36°35'46.1" W121°52'34.6"	600 feet	569.6	LOS blocked by trees

Table 11. Non-LOS Measurement Points

b. Non-LOS Measurement Results and Analyses

Distance (feet)	Linksys		ORiNOCO		Cisco		Theoretical {eqn (2.4)} (dBm)
	Signal (dBm)	PER	Signal (dBm)	PER	Signal (dBm)	PER	
150	-72	0	-75	0	-60	0	-64.0
300	-87	0.138	-86	0	-80	0.122	-70.1
600	-89	0.172	-89	0.044	No signal		-76.1

Table 12. Non-LOS Measurement Results

The measurement results in Table 12 validated those obtained in the earlier measurement for LOS situations. The ORiNOCO ComboCard performs best in both cases, providing the lowest PER.

An interesting relation from the Non-LOS measurement results is also observed. If the ORiNOCO signal strength measurement results are used as the closest match to the actual signal strength, it seems to indicate that the WLAN signal suffer about 10 dB of loss when propagating through the trees.

5. 802.11a Receiver Selection

Based on all the measurement data, the best-suited 802.11a card for the prototype detection system is the ORiNOCO 11a/b/g ComboCard (Gold version).

There is also an added advantage of using the ORiNOCO ComboCard for the prototype system. While both the Linksys WPC54A and the Cisco AiroNet AIR-CB20A cards can detect signals only in the Lower and Middle UNII bands, the ORiNOCO is able to detect signals in the Upper UNII band (5.725 – 5.825 GHz) too. In fact, because the ORiNOCO is an 11a/b/g –compliant card, the resulting prototype system is able to detect signals from 802.11b- and 802.11g-compliant networks too.

Based on procurement cost, the Linksys WPC54A, ORiNOCO ComboCard and Cisco AIR-CB20A cost $129, $150 and $180 respectively. Although the ORiNOCO ComboCard is not the cheapest, the incremental cost is insignificant compared to the advantages offered.

D. PROTOTYPE SYSTEM SUMMARY

The first question of this thesis can now be answered. The commercially available low cost hardware and software solution to detect and process a wireless IEEE 802.11a compliant network signal will consist of the following components:

1. Laptop Computer running on Windows XP Professional, with at least 512 MB RAM, 60 GB hard-disk and 15-inch display of 1600 by 1200 pixels. A Dell Latitude C840 system similar to that used in the thesis is expected to cost no more than $2,000.

2. Proxim ORiNOCO 11a/b/g ComboCard GOLD 8480-WD, at the cost of $150.

3. AiroPeek NX protocol analyzer software, at the cost of $2,500.

In all, the prototype system will cost about $4,650 and the system is shown in Figure 19.

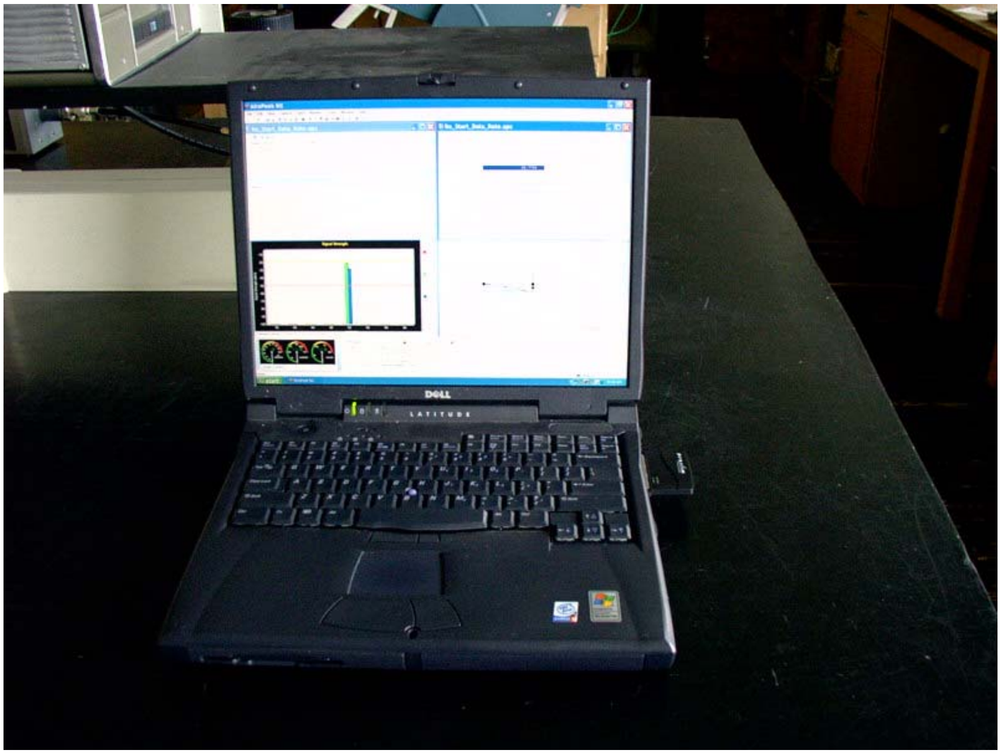

Figure 19. Prototype System for 802.11a Detection

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERFORMANCE TEST AND RESULTS

Having answered the first question, this portion is devoted to answering the second question of the thesis: what is the detection and processing performance of the prototype hardware and software solution?

A. PERFORMANCE TEST SETUP

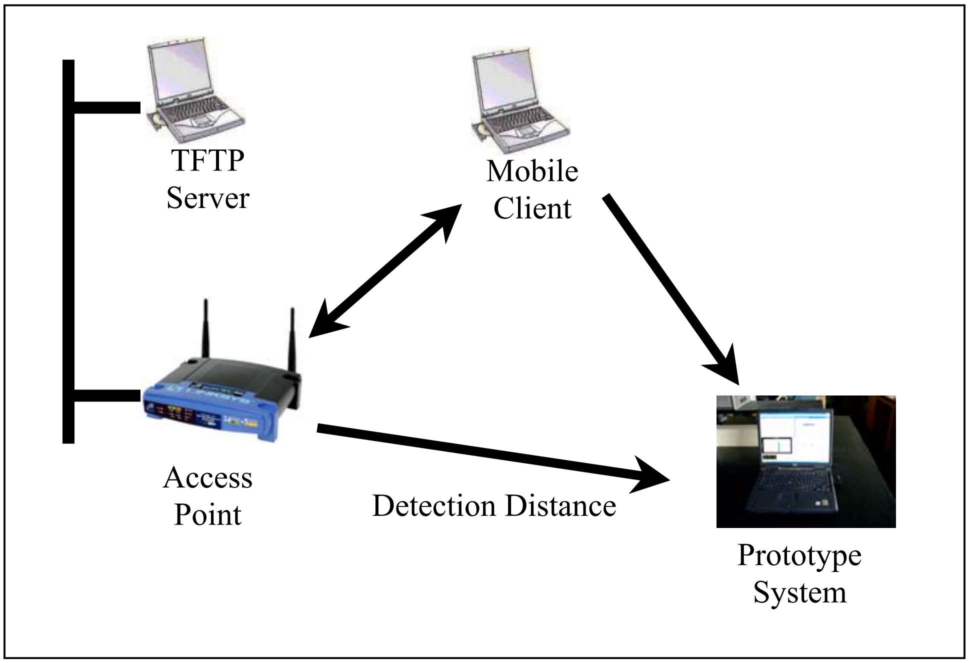

Figure 20. Performance Test Setup

The performance test setup is shown in Figure 20. In this test, three different sets of available equipment are used, namely the Linksys system, the ORiNOCO system and the Cisco system. Both the ORiNOCO and the Cisco system are commonly used for commercial/industrial WLAN networks, while the Linksys system is mainly used for home-based WLAN.

To test the performance of the prototype system built in Chapter III, the access point is connected by Ethernet to a laptop that serves as a TFTP (Trivial File Transfer Protocol) Server, running the SolarWinds TFTP Server software supplied by ORiNOCO. The wireless mobile client is connected to the TFTP Server through the wireless network in infrastructure mode, using open authentication without WEP encryption. Data is then moved between the mobile client and the TFTP Server through the 802.11a network.

The performance of the prototype system under LOS environment is evaluated using two different data packet sizes. This is done to determine whether the performance is dependent upon packet size. Small data packets of 96 bytes are generated using continuous PING from the mobile client to the TFTP Server while larger data packets of 580 bytes are generated by transferring large data files (of about 20 Mbytes each) from the TFTP Server to the mobile client using TFTP. For the measurements, the prototype system is placed at distances of 300 feet, 500 feet, 600 feet and 700 feet from the access point to capture the transmitted PING and TFTP packets. The measurement environment for LOS is the same as that used in Chapter III, as shown on Figure 17.

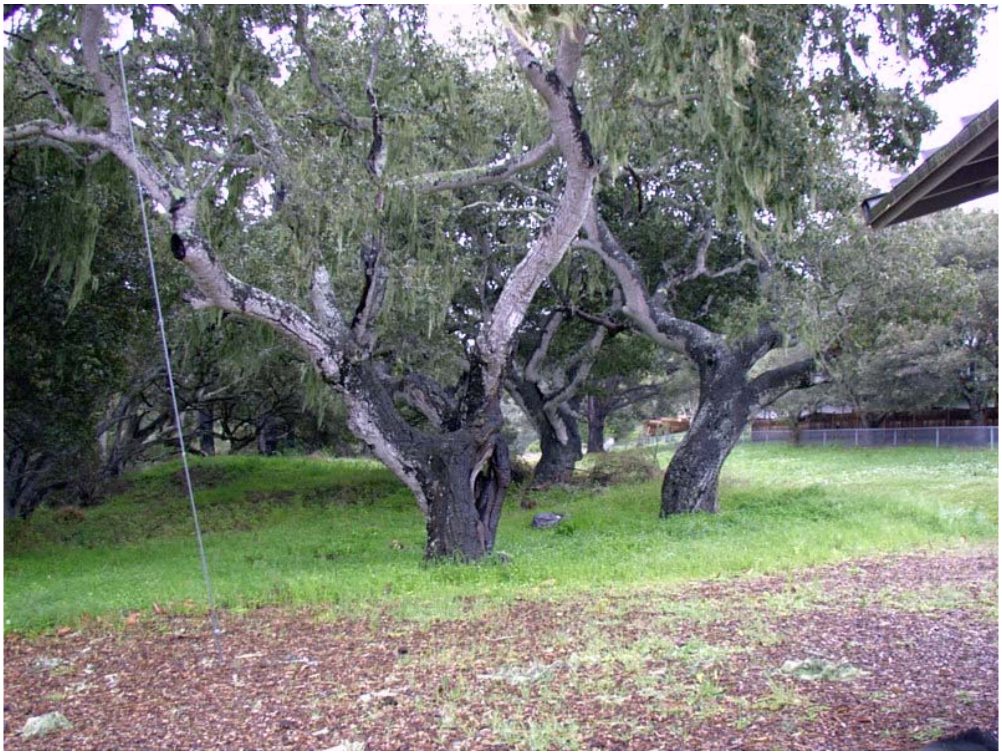

Figure 21. Wooded Area Measurement Environment

AP Location	System Location	Distance (from GPS)	Calculated from eqn (2.9)
N 36°34'52.8" W121°52'34.8"	N 36°34'53.4" W121°52'33.4"	100 feet	118.2 feet
	N 36°34'52.7" W121°52'32.5"	200 feet	213.3 feet
	N 36°34'52.0" W121°52'31.6"	300 feet	312.8 feet
	N 36°34'51.3" W121°52'31.0"	400 feet	394.2 feet

Table 13. Wooded Area Measurement Points

The performance of the prototype system under non-LOS environment is evaluated using TFTP packets, in the wooded area shown on Figure 21. This is done to simulate situations where the prototype system could be hidden within a wooded area to capture 802.11a WLAN traffic. The measurements would reveal the effect of foliage on the performance of the prototype system. For this measurement, shorter distances of 100, 200, 300 and 400 feet are used and the measurement points are listed in Table 13.

Based on the data captured in Chapter III, the prototype system is able to capture 802.11a beacons without errors up to 600 feet (LOS) and 300 feet (non-LOS). Beyond these distances, packet errors occurred. However, because the beacons are transmitted at the lowest data rate of 6 Mbps (using BPSK and 1/2 rate convolutional coding), they are relatively easier to detect without errors. For higher data rates where more complex modulations such as QPSK, 16-QAM and 64-QAM are used, packet errors are expected to increase since these modulations are more susceptible to noise and interference. The data link rate of the 802.11a network becomes another important variable in the performance assessment – the capturing range is expected to be shorter and packet error rate is expected to be higher for higher data link rates.

B. RESULTS AND ANALYSIS

1. Linksys System

The Linksys WAP55AG access point is paired up with the WPC54A card in the mobile client so that there will not be any incompatibility issues between the access point and the client adaptor. As mentioned earlier, the transmit power of the WAP55AG is 40 mW or +16 dBm. The expected signal strength at various distances, as shown in Table 6, is still applicable.

The LOS measurement results for PING packets are shown in Table 14 while the results for TFTP packets are shown in Table 15. For both the smaller PING packets and the larger TFTP packets, the results showed that the majority of the packets are transmitted at 18 and 24 Mbps data rate. The data link rate is purely a function of the link condition between the access point and the mobile client. The results showed that the number of packets received in error increased with increasing distance, and that error packets were captured as early as at 300 feet. Another observation is that packets at higher data rates are missed (cannot be detected) at larger distances, especially at 700 feet.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-68	37	0	220	460	287	73	0	0	11 (0.010)
500	-73	27	0	130	324	272	60	0	0	12 (0.015)
600	-76	45	0	137	352	246	48	0	0	35 (0.042)
700	-86	1	0	7	2	0	0	0	0	2 (0.200)

Table 14. LOS Capture Performance on Linksys (PING Packets)

Distance (feet)	Average Signal (dBm)	Number of Packets (at various data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-66	19	0	116	333	446	359	33	0	30 (0.023)
500	-67	30	0	180	320	345	72	0	0	29 (0.031)
600	-70	44	0	165	321	269	66	0	0	55 (0.064)
700	-84	17	0	62	127	63	6	0	0	171 (0.621)

Table 15. LOS Capture Performance on Linksys (TFTP Packets)

Recall that the beacons are 67 bytes in length, and the PING packets are comparatively similar in size at 96 bytes in length. There is therefore some merit to compare the derived PER in Table 14 with those obtained earlier in Table 8. The comparison suggested that the PER performance of the prototype system depends on the data rate of the packets being captured – the number of packets captured in error increases with increased data rate of the packets.

To determine the effect of packet size on the performance of the prototype system, the derived PER in Table 14 are compared with those in Table 15. The results revealed that the PER performance of the prototype system also depends on the size of the packets captured – more errors are expected for capturing data packets that are larger in size.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
100	-65	0	0	0	19	123	224	131	0	32 (0.064)
200	-70	3	0	31	40	91	268	180	0	96 (0.157)
300	-79	1	0	12	19	48	8	0	0	38 (0.432)
400	-82	3	0	28	14	51	15	0	0	58 (0.523)

Table 16. Non-LOS Capture Performance on Linksys (TFTP Packets)

Table 16 shows the measurement results for TFTP packets under the non-LOS environment where the prototype system is hidden within a wooded area. Both the access point and the mobile client have not been moved. The data link condition is therefore similar to the LOS setup.

From the measurement results, it is observed that the foliage significantly increase the number of packets captured in error, in addition to the increased attenuation of the signals. As in the LOS case, it is also noted that more packets at higher data rates are missed at longer ranges.

If the average signal strength received is used as a reference, comparison of the PER in Table 16 with those in Table 15 suggested that the wooded area introduced interference and noise that caused more packets to be received in error.

2. ORiNOCO System

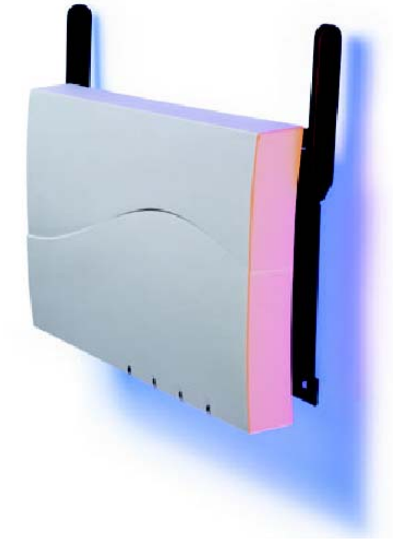

Figure 22. ORiNOCO AP2000 with 802.11a Upgrade Kit (from Ref [15])

The ORiNOCO system consists of the AP2000 access point installed with the 802.11a upgrade kit, operating with ORiNOCO ComboCard GOLD in the mobile client. The AP2000 is shown in Figure 22. Based on the AP2000 datasheet [15], the maximum transmit power available from the 802.11a radio is +17 dBm, while the receiving sensitivity ranges from -85 dBm at 6 Mbps to -65 dBm at 54 Mbps. The antenna supplied with the 802.11a radio has a gain of 5 dBi. This provides the AP2000 with an effective transmit power of +22 dBm or 158 mW.

The LOS measurement results for PING packets are shown in Table 17. Due to the much higher effective transmit power of the AP2000, the results showed that the packets captured are transmitted at higher data rates of between 24 and 54 Mbps, compared to the Linksys system. When combined and compared, the data in Table 17, Table 14 and Table 8 validated the earlier suggestion that the PER performance of the prototype system deteriorates with increased data rate.

The LOS measurement results for TFTP packets are shown in Table 18. Compared to the PING packets, the TFTP packets are transmitted at higher data rates of between 36 Mbps and 54 Mbps. The results also validated the suggestion that the PER performance of the prototype system deteriorates as the size of the captured data increases.

In exact agreement with previous observations, for both the PING and TFTP cases, packets at higher data rates are missed (cannot be detected), especially at 700 feet. The sudden drop in number of 54 Mbps packets captured is expected as the signal strength at 700 feet averaged at only -75 dBm. Assuming that the ORiNOCO ComboCard used in the prototype system has similar sensitivity as the AP2000, then the 54 Mbps signals are below the sensitivity of the prototype system.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-68	0	0	0	2	390	4	44	128	30 (0.053)
500	-69	0	0	6	2	443	26	35	102	72 (0.117)
600	-71	0	0	6	2	240	24	21	48	51 (0.149)
700	-81	0	0	2	1	218	25	4	60	137 (0.442)

Table 17. LOS Capture Performance on ORiNOCO (PING Packets)

Distance (feet)	Average Signal (dBm)	Number of Packets (at various data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-66	0	0	0	0	0	157	5528	1356	419 (0.060)
500	-70	0	0	0	0	0	20	4228	4171	1070 (0.127)
600	-72	0	0	0	0	0	5	2775	1887	694 (0.157)
700	-75	0	0	0	0	1	26	846	44	515 (0.562)

Table 18. LOS Capture Performance on ORiNOCO (TFTP Packets)

Table 19 shows the measurement results for TFTP packets under the non-LOS environment where the prototype system is hidden within a wooded area. Both the access point and the mobile client have not been moved. The data link condition is this similar to the LOS setup.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
100	-67	0	0	0	0	0	4	1317	1837	329 (0.104)
200	-69	0	0	0	0	0	6	2115	2717	1353 (0.280)
300	-72	0	0	0	0	1	549	1686	412	1536 (0.580)
400	-76	0	0	0	1	0	398	545	17	601 (0.625)

Table 19. Non-LOS Capture Performance on ORiNOCO (TFTP Packets)

As expected, the wooded area attenuated the signals significantly. The results also suggested that the number of packets captured in error increases with increase in data rate when the data in Table 16 is taken into consideration.

3. Cisco System

Figure 23. Cisco AP1200 with 802.11a Radio Kit (from Ref [16])

The Cisco system consists of the AP1200 access point installed with the 802.11a upgrade kit, operating with the Cisco AiroNet AIR-CB20A Client Adaptor in the mobile client. The AP1200 is shown in Figure 23. Based on the datasheet [16], the maximum transmit power from the AP1200 is +16 dBm, while the receiving sensitivity ranges from -85 dBm at 6 Mbps to -68 dBm at 54 Mbps. The patch antenna shown, when used in the upright position as an omni-directional antenna, has a gain of +2 dBi. This provides the AP1200 with an effective transmit power of +18 dBm or 63 mW.

The LOS measurement results for PING packets are shown in Table 20 while the results for TFTP packets are shown in Table 21. The data rate for PING packets are between 36 Mbps and 54 Mbps, while the TFTP data rates are between 12 Mbps and 36 Mbps. Again, the results suggested that the PER increases with increase in the data rate of the captured packets. The same phenomenon of missing data packets at high data rates is also observed. In this case, the average signal at 700 feet is at -81 dBm. Therefore, it is not surprising that packets at 48 Mbps are also not detected.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-73	0	1	0	1	12	197	374	556	48 (0.042)
500	-74	0	1	2	5	34	224	398	562	153 (0.125)
600	-76	0	0	1	1	14	159	313	476	148 (0.154)
700	-81	0	0	0	0	3	14	0	0	8 (0.471)

Table 20. LOS Capture Performance on Cisco (PING Packets)

Distance (feet)	Average Signal (dBm)	Number of Packets (at various data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
300	-74	0	483	784	187	410	705	0	1	0 (0.000)
500	-75	0	0	137	637	490	1031	0	0	104 (0.045)
600	-76	0	0	0	2	1064	3615	0	0	1077 (0.230)
700	-80	0	0	6	71	2021	1642	0	0	1890 (0.505)

Table 21. LOS Capture Performance on Cisco (TFTP Packets)

Table 22 shows the measurement results for TFTP packets under the non-LOS environment. The prototype system is similarly hidden within a wooded area, and both the access point and the mobile client have not been moved. The data link condition is this similar to the LOS condition for TFTP packets.

Distance (feet)	Average Signal (dBm)	Number of Packets (at the data rates in Mbps)								Number of error packets (PER)
		6	9	12	18	24	36	48	54	
100	-71	0	6	23	203	1932	2010	0	0	219 (0.052)
200	-75	0	0	0	0	1949	2211	0	0	236 (0.056)
300	-80	0	0	0	180	825	290	0	0	514 (0.397)
400	-81	0	0	0	2	561	136	0	0	549 (0.785)

Table 22. Non-LOS Capture Performance on Cisco (TFTP Packets)

The results for this measurement are consistent with previous observations. The performance of the prototype system is badly affected by the interference present in the wooded area.

C. PROTOTYPE PERFORMANCE SUMMARY

All the measurement results suggested that the performance of the prototype system depends very much on the characteristics of the 802.11a signal to be captured.

The data collected for PING packets can be summarized in Table 23. The data points pointed to higher PER for larger distance and higher data rates.

A more useful presentation of the data from Table 23 is shown in Figure 24. Although there are only a few data points for each capturing distance, the graph provides some means to estimate the performance of the prototype system when used to capture small data packets. The graph showed that the capturing distance of the prototype system is limited to about 600 feet.

Distance (feet)	System	Average Data Rate (Mbps)	PER	Average Signal Level
300 feet	Linksys	19.2	0.010	-68 dBm
	ORiNOCO	32.7	0.053	-68 dBm
	Cisco	48.5	0.042	-73 dBm
500 feet	Linksys	20.0	0.015	-73 dBm
	ORiNOCO	30.7	0.117	-69 dBm
	Cisco	47.7	0.125	-74 dBm
600 feet	Linksys	19.2	0.042	-76 dBm
	ORiNOCO	30.3	0.149	-71 dBm
	Cisco	48.6	0.154	-76 dBm
700 feet	Linksys	12.6	0.200	-86 dBm
	ORiNOCO	31.0	0.442	-81 dBm
	Cisco	33.9	0.471	-81 dBm

Table 23. Summary of LOS Capture Performance (PING Packets)

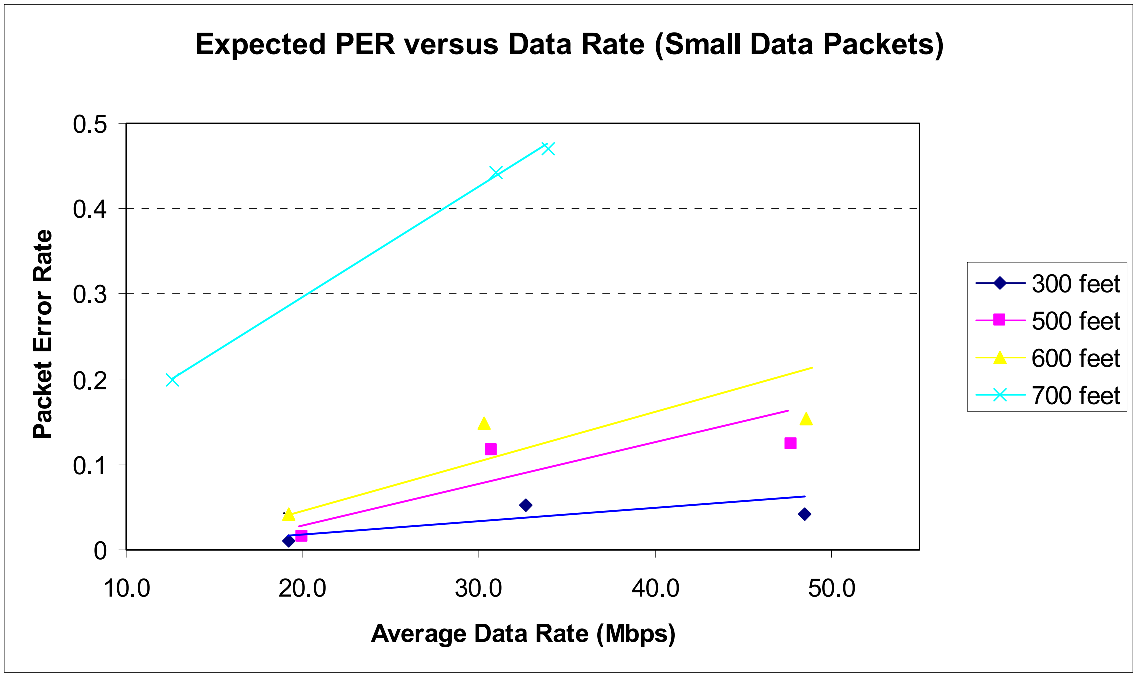

Figure 24. Graph of Expected PER versus Data Rate (Small Data Packets)

Similarly, the data collected for the larger TFTP packets can be summarized in Table 24. The graph for estimating the performance of the prototype system when used to capture large data packets is presented in Figure 25. Again, the results suggest that the prototype system is able to capture signals with tolerable errors up to 600 feet.

Distance (feet)	System	Average Data Rate (Mbps)	PER	Average Signal Level
300 feet	Linksys	25.0	0.023	-66 dBm
	ORiNOCO	48.9	0.060	-65 dBm
	Cisco	20.4	0.000	-74 dBm
500 feet	Linksys	20.0	0.031	-67 dBm
	ORiNOCO	50.9	0.127	-70 dBm
	Cisco	27.0	0.045	-75 dBm
600 feet	Linksys	19.5	0.064	-70 dBm
	ORiNOCO	50.4	0.157	-72 dBm
	Cisco	33.3	0.230	-76 dBm
700 feet	Linksys	17.7	0.621	-84 dBm
	ORiNOCO	47.9	0.562	-75 dBm
	Cisco	29.1	0.505	-80 dBm

Table 24. Summary of LOS Capture Performance (TFTP Packets)

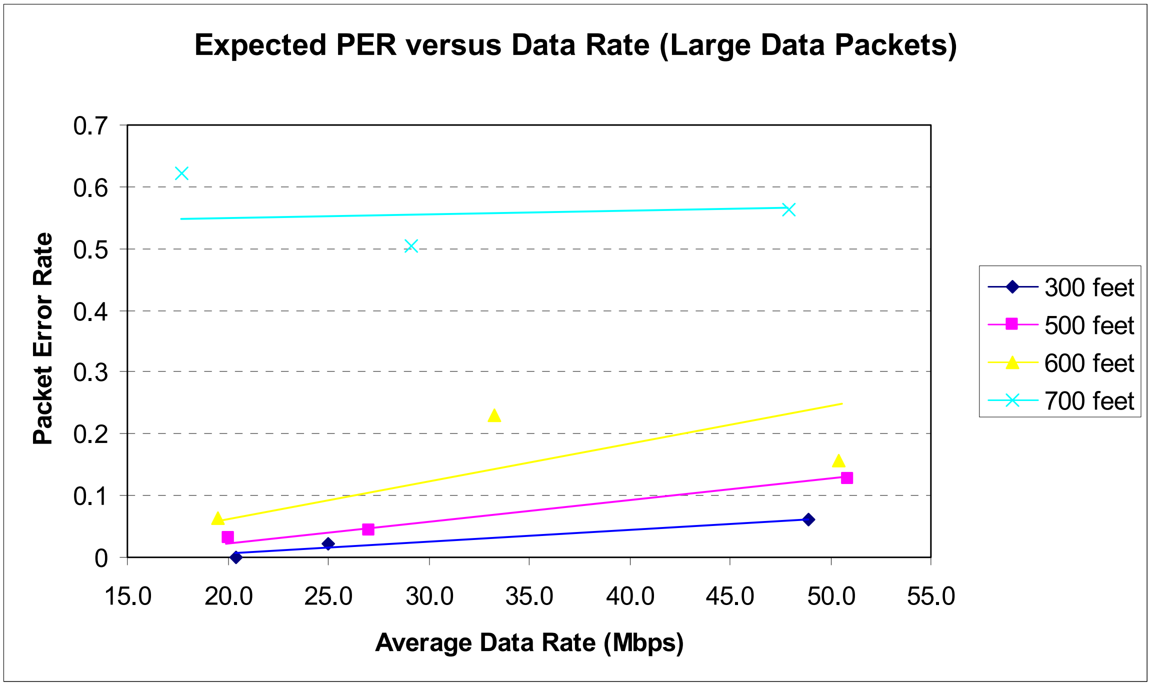

Figure 25. Graph of Expected PER versus Data Rate (Large Data Packets)

For the non-LOS wooded area, the performance of the prototype system is summarized in Table 25. The graph for estimating the performance of the prototype system when used in a wooded area to capture 802.11a signals is presented in Figure 26.

Distance (feet)	System	Average Data Rate (Mbps)	PER	Average Signal Level
100 feet	Linksys	35.5	0.064	-65 dBm
	ORiNOCO	51.5	0.104	-67 dBm
	Cisco	29.4	0.052	-71 dBm
200 feet	Linksys	35.2	0.157	-70 dBm
	ORiNOCO	51.4	0.280	-69 dBm
	Cisco	30.4	0.056	-75 dBm
300 feet	Linksys	22.0	0.432	-79 dBm
	ORiNOCO	46.4	0.580	-72 dBm
	Cisco	25.9	0.397	-80 dBm
400 feet	Linksys	21.4	0.523	-82 dBm
	ORiNOCO	43.1	0.625	-76 dBm
	Cisco	26.3	0.785	-81 dBm

Table 25. Summary of Non-LOS Capture Performance

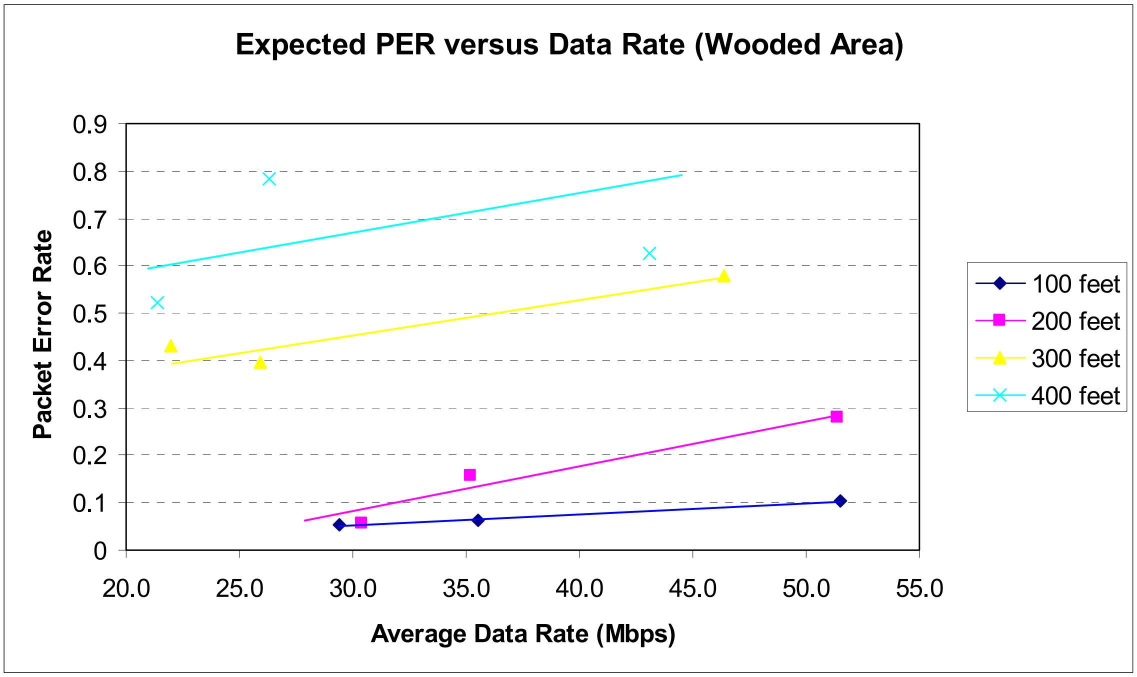

Figure 26. Graph of Expected PER versus Data Rate (Wooded Area)

The results for the wooded area pointed to the same phenomena that the PER increases as the data rate of the captured packets increases. Based on the graph, the effective capturing distance of the prototype is about 200 feet.

V. 802.11A LINK PERFORMANCE

This chapter is dedicated to answering the final question of this thesis: what is the measured operating range of 802.11a compliant networks compared to theoretical/advertised operating range? Three 802.11a systems are used outdoors and the prototype system is used to capture and determine the data link rate achieved by the 802.11a WLAN network at various ranges. The actual performance is then compared with theoretical/advertised ranges.

A. PERFORMANCE TEST SETUP

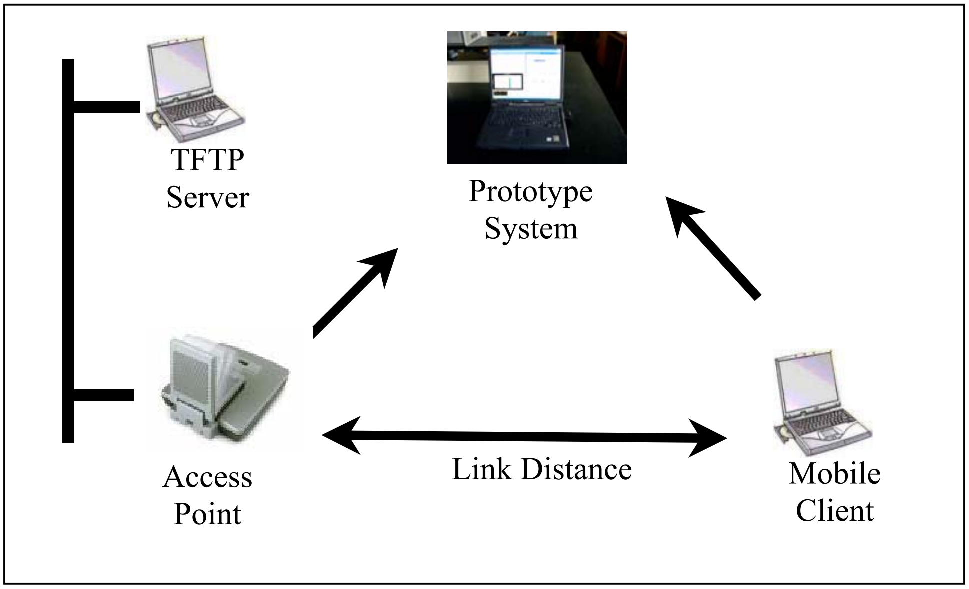

Figure 27. Link Performance Test Setup

The test setup to measure data link rate is shown in Figure 27. In this test, the same three sets of available equipment from Linksys, ORiNOCO and Cisco are used. The access point is similarly connected by Ethernet to a laptop that serves as a TFTP Server. The wireless mobile client is connected to the TFTP Server through the wireless network in infrastructure mode, using open authentication without WEP encryption. TFTP transfer of a large data file is used to generate traffic in the 802.11a network.

The LOS measurement environment in this test is as depicted in Figure 17. The locations of the access point and the measurement points (at 100 feet interval) where the mobile client is placed are the same as those listed in Table 5. The prototype system is stationed in the vicinity of the mobile client to capture the TFTP packets that are transferred between the access point and the mobile client.

B. RESULTS

1. Linksys System

The measurement results for Linksys are tabulated in Table 26. The number of retry packets is the number of packets that have been re-transmitted from the access point by request from the mobile client.

Distance (feet)	Number of Packets (at the data rates in Mbps)								Number of retry packets
	6	9	12	18	24	36	48	54	
100	0	0	0	9	108	436	3316	6623	1333
200	0	0	0	16	210	813	3474	2695	527
300	1	0	11	13	239	2205	1957	1354	1381
400	0	0	2	12	484	3625	2402	376	1602
500	14	0	201	771	2757	2674	104	0	2359
600	20	0	277	1035	3104	2639	126	0	2793
700	184	0	806	1860	2350	2079	0	0	3182

Table 26. Achieved Data Link Rate at Various Distances (Linksys)

As expected, the data link rate gradually decreases from 54 Mbps as the distance between the access point and the mobile client increases. In general, the number of retry packets also increases as the distance is increased. The anomaly at 100 feet is due to the frequent rate switching between 48 Mbps and 54 Mbps.

2. ORiNOCO System

Distance (feet)	Number of Packets (at the data rates in Mbps)								Number of retry packets
	6	9	12	18	24	36	48	54	
100	0	0	0	0	11	411	1936	4009	213
200	0	2	0	0	172	3002	323	3252	191
300	0	0	130	265	622	3240	774	3317	676
400	0	0	0	515	2476	2462	3977	0	895
500	322	41	854	2962	1121	3096	0	0	1412
600	594	461	1812	2691	1702	1174	0	0	1792
700	3581	744	1283	3623	30	0	0	0	2614

Table 27. Achieved Data Link Rate at Various Distances (ORiNOCO)

The results for ORiNOCO are listed in Table 27. Similarly, the data rate is observed to change or shift downwards as the distance increases. The anomaly in the number of retry packets at 100 feet is also observed here.

3. Cisco System

The measurement results for Cisco are tabulated in Table 28.

Distance (feet)	Number of Packets (at the data rates in Mbps)								Number of retry packets
	6	9	12	18	24	36	48	54	
100	0	0	0	7	488	2551	3189	2325	2703
200	8	3	11	15	627	3737	3417	1155	3374
300	0	0	1	18	1968	3747	1038	169	1807
400	1463	874	899	2341	2053	344	9	19	2747
500	3452	1325	1227	1459	812	14	13	24	3006
600	3995	673	1938	2048	26	6	6	12	3743
700	No Signal - Link cannot be established								

Table 28. Achieved Data Link Rate at Various Distances (Cisco)

As with the previous two cases, the data link rate of the 802.11a traffic decreases as the distance increases. However, anomalies in the number of retry packets are observed at both 100 feet and 200 feet. These anomalies are due to data rate adaptation.

Another anomaly recorded is that the Cisco system was not able to achieve a link at the 700 feet point. This could be explained by looking at the specifications of both the Cisco AP1200 access point [16] and the Cisco AiroNet AIR-CB20A Client Adaptor [14].

The AP1200 802.11a radio has a transmit power of 40 mW or +16 dBm. The 802.11a radio has an omni-directional patch antenna with +2 dBi of gain, giving the AP1200 an EIRP of +18 dBm. The AP1200 also has receiver sensitivity ranging from -68 dBm at 54 Mbps to -85 dBm at 6 Mbps, similar to the sensitivity of the Client Adaptor listed in Table 4. The Client Adaptor, on the other hand, has a transmit power of 20 mW or +13 dBm and an integrated patch antenna with +5 dBi of gain. This provides the Client Adaptor with an EIRP of +18 dBm.

From the results in Chapter III where Linksys WAP55AG was used, the signal strength detected at 700 feet by the Cisco Client Adaptor was about -87 dBm (see Table 7). Since the WAP55AG was transmitting at +16 dBm, or about 2 dBm lower than the AP1200, the signal arriving at the Client Adaptor would be about -85 dBm. This is at the sensitivity level for 6 Mbps reception. Apparently, the signals are not good enough for a link to be established.

C. SUMMARY OF 802.11A LINK PERFORMANCE

The data link rate achieved by the three 802.11a systems are averaged and summarized in Table 29. The downshift in data link rate as the distance is increased can be clearly observed.

Distance (feet)	Average Data Link Rate (Mbps)		
	Linksys	ORiNOCO	Cisco
100	51.0	51.0	44.7
200	48.1	44.9	42.0
300	43.7	42.4	34.8
400	40.3	36.9	16.6
500	28.2	24.3	11.5
600	27.4	19.1	10.6
700	24.1	11.8	No Link

Table 29. Summarized 802.11a Data Link Rate (Outdoor)

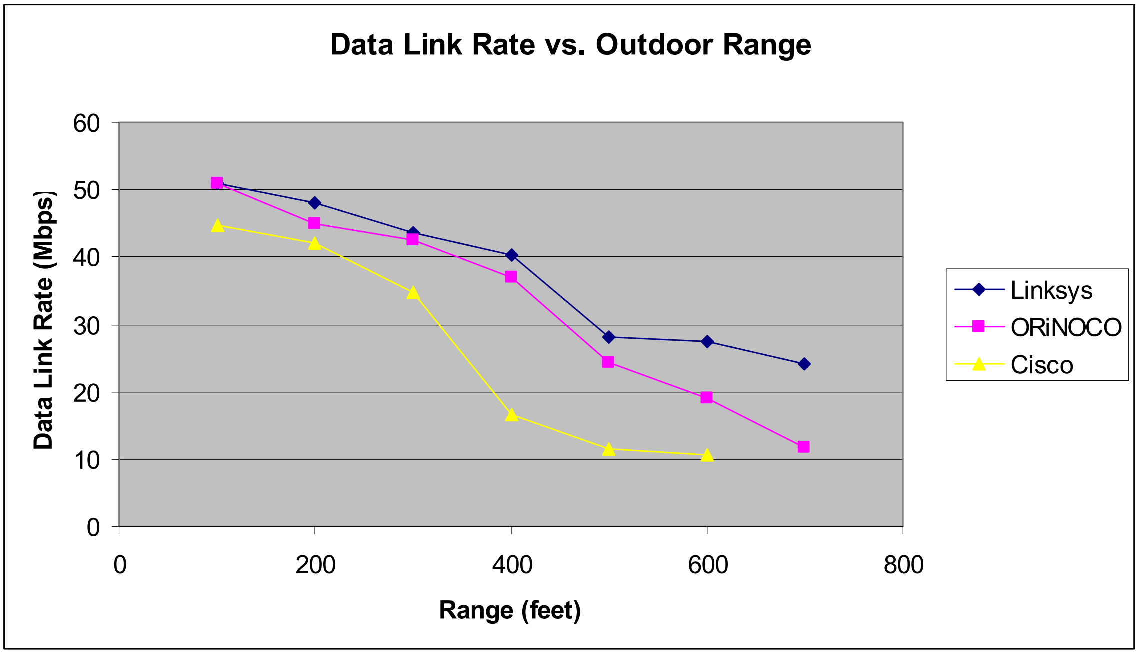

Figure 28. Outdoor Data Link Rate of 802.11a

The graphical presentation of the summarized data in Table 29 is shown in Figure 28. It showed that the 802.11a network could have an operational range of up to 700 feet at a data link rate of up to 24 Mbps.

When compared to the indoor data link rate presented in Figure 29. the data link rate achievable outdoor is two times higher at 100 feet and almost four times higher at 200 feet. This is expected, as the multipath effects indoors are more severe.

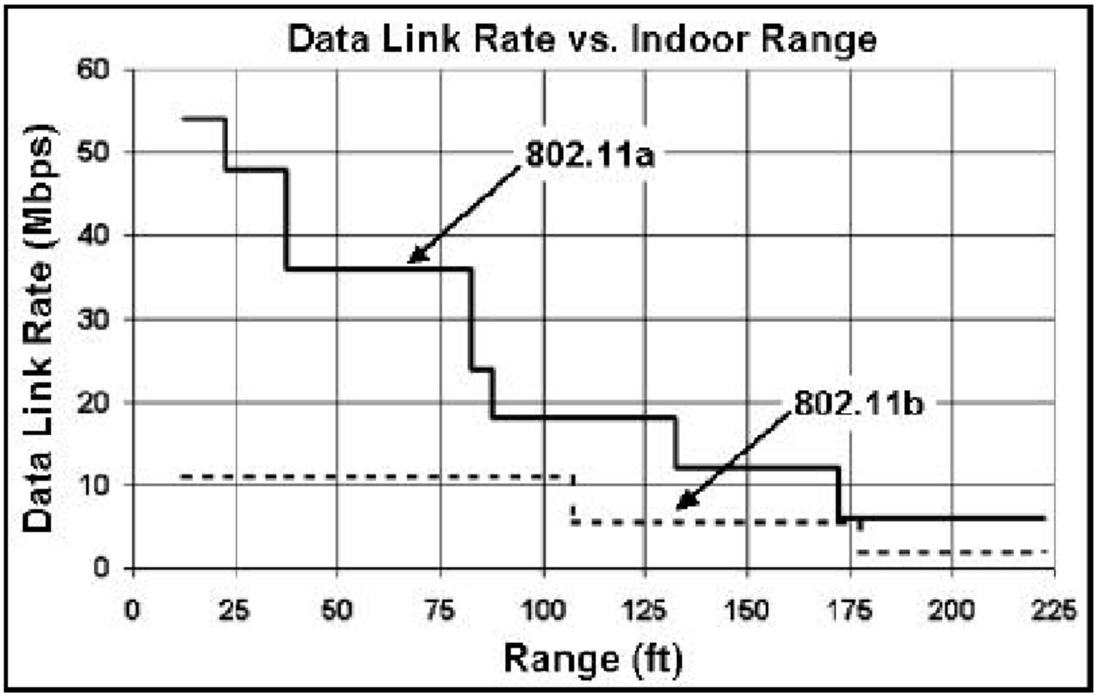

Figure 29. Indoor Data Link Rate of 802.11a (From Ref [2])

The advertised 802.11a data link performance from Cisco [14] is used next for comparison with the measured results. Table 30 shows the advertised outdoor range for the Cisco AiroNet AIR-CB20A when used with the Cisco AP1200 using an omni-directional antenna with +5 dBi gain.

Data Link Rate	Outdoor Range
54 Mbps	100 feet
18 Mbps	600 feet
6 Mbps	1000 feet

Table 30. Cisco AiroNet AIR-CB20A Outdoor Range (After Ref [14])

Comparing the data from Cisco system, the range fell short at all data rates. This could be due two reasons. Firstly, the gain of the antenna used in the measurements is lower by 3 dB. This would reduce the operating range of the 802.11a link. Secondly, severe multipath effects experienced in the measurement may not have been taken into consideration in the advertised outdoor range.

VI. CONCLUSION AND FUTURE WORK

A. CONCLUSIONS

The main purpose of this research was to develop a prototype system, using commercially available low cost hardware and software solutions, to detect and process 802.11a-compliant WLAN signals. To achieve that, answers to the following three questions posed at the beginning were sought after:

1. What specific commercially available low cost hardware and software solutions can be utilized to detect and process a wireless IEEE 802.11a compliant network signal?

2. What is the detection and processing performance of the prototype hardware and software solution?

3. What is the measured operating range of 802.11a compliant networks compared to theoretical/advertised operating range?

To answer the first question, Chapter III reviewed the requirement for the prototype system, and then set out to select both the software and hardware required. Software selection was achieved through literature research, while extensive measurements were performed on available hardware to select the most suitable 802.11a receiver for the system. The resulting prototype system is described at the end of Chapter III and cost a total of $4,650.

The second question was answered by using the developed prototype system to capture and process 802.11a WLAN signals from three available sets of network, namely Linksys, ORiNOCO and Cisco. The performance of the prototype system was then evaluated using the captured data.

Based on the performance results, the prototype system is useful for security vulnerability assessment of a friendly military WLAN network. However, the system may be of limited use to detect and process other 802.11a WLAN signal due to the limited range of about 600 feet. The operable range is even shorter if the system is used in a wooded area.

However, the detection range of the prototype system needs to be referenced to the achievable data link rates of an 802.11a network. If the 802.11a network is used for high-speed data exchange at rates of 48 Mbps and 54 Mbps, the achievable range is no more than 200 feet. Based on the performance data, the system is able to detect and process these data at a range of 600 feet – three times the network operating range.

Moreover, the range limitation is purely due to the limited sensitivity of the commercial 802.11a receiver card that is supplied with integrated antenna. If a suitable specialized 802.11a receiver card incorporating an external amplifier and antenna can be used, the resulting system would be able to capture 802.11a signals at extended ranges.

The final question deals with the operating range of the 802.11a-compliant network so as to assess whether the 802.11a network is suitable for operational use. To answer this question, the prototype system is again used as an independent detection and processing system to capture the data link rate achieved by three different 802.11a networks at various ranges. The measurement results concluded that the 802.11a network is able to provide up to 24 Mbps of data rate for distances up to 700 feet.

While the range of the 802.11a network seemed limited when compared to those of 802.11b, the achieved data rate is several times higher than the maximum of 11 Mbps offered by 802.11b networks. The higher data rate of the 802.11a network would therefore be very useful in operations, where high-speed wireless data exchange is required within a small operational area of up to 600 feet radius.

B. FUTURE WORK

1. Specialized 802.11a Receiver Card

As concluded earlier, the detection range of the prototype system is severely limited by the sensitivity of the commercial 802.11a receiver cards used. The detection range can be extended significantly if a specialized 802.11a receiver card incorporating an external high-gain antenna and an appropriate amplifier are used. Work on developing such a specialized 802.11a receiver card could be carried out as an extension to this thesis.

2. Measurement of Actual Signal Strength Using YellowJacket

Throughout the conduct of this research, the YellowJacket WLAN analyzer capable of accurately measuring the strength of the 802.11a signals is not available. A simple free-space path loss model is used to predict the expected signal strength at various distances from the access point. This could be carried out as an extension to this thesis.

3. Ability to Capture Proprietary Modes

It would be an interesting extension to this research to check whether the prototype system is able to capture, decode and analyze 802.11a traffic operating in the proprietary modes such as the "Turbo" mode from Linksys and the "2X" mode from Proxim. If the current prototype system is not able to do that, modifications to either the hardware or the software of the system can be explored to enable such capabilities.

4. Effect of WEP Encryption on 802.11a Performance

In this thesis, all tests are performed using infrastructure mode with open authentication, and without WEP encryption. It would be interesting to investigate the effect of WEP encryption on the performance of the 802.11a network.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Walter N. Currier Jr., *Prototype System For Detecting and Processing IEEE 80211b Signals*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2002.

2. James C. Chen, *Measured Performance of 5-GHz 802.11a Wireless LAN Systems*, Atheros Communications, Inc., 27 August 2001.

3. LAN MAN Standards Committee of the IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* ANSI/IEEE Std 802.11, 1999 Edition.

4. Netgear**, "**802.11a/b/g Dual Band PC Card" **[**http://www.netgear.com/products/details/WAG511.asp**],** 18 December 2003.

5. Itworld.com, "Too Many Standards Spoil Wireless LAN Soup" [http://wireless.itworld.com/4276/IDG020102wirelesslan/page_1.html], 2 January 2002.

6. LXE Inc., *Keep The Bad Guys Out of Your 802.11 Wireless Network*, May 2003

7. Geography Newsletter, "What is the circumference of the earth?", [http://geography.about.com/library/faq/blqzcircumference.htm], 2 December 2003.

8. Andy Dorman, *Wireless LAN Analyzers: The Ultimate Hacking Tools?*, Network Magazine, 5 March 2003.

9. Tom Henderson, *WLAN Analyzers*, Network World, 14 April 2003.

10. Wireless, "Eighteen Products for Building, Managing, and Securing WLANs", [http://www.infoworld.com/article/03/12/19/50FERevwire_1.html], 19 December 2003.

11. Wildpackets Inc., "AiroPeek NX Special Maintenance Owner Pricing", [http://www.wildpackets.com/products/airopeek_nx/pricing_maint], 17 December 2003.

12. Linksys, "WPC-54A - Instant Wireless™ PC Card" [http://www.linksys.com/products/product.asp?prid=430&grid=22], 8 January 2004.

13. Proxim, "ORiNOCO 11a/b/g ComboCard" [http://www.proxim.com/products/wifi/client/abgcard], 8 January 2004.

14. Cisco Inc., “Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapter” [http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a00800c61ea.html], 8 January 2004.

15. Proxim, “ORiNOCO AP-2000 11a Kit” [http://www.proxim.com/learn/library/datasheets/AP2000_11a_kit.pdf], 8 January 2004

16. Cisco Inc., “Cisco Aironet 1200 Series Access Point” [http://www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html], 8 January 2004.

17. Linksys, “Dual-Band Wireless A + G Access Point” [http://www.linksys.com/products/product.asp?prid=538&scid=35], 8 January 2004.

18. Greg DesBrisay, “Basics of Orthogonal Frequency Division Multiplexing”, [http://www.wca.org/Year2000/gregdesbrisay.pdf], 8 January 2004.

19. Joel Conover, “802.11a: Making Space for Speed”, [http://www.networkcomputing.com/1201/1201ws1.html], 8 January 2004.

20. Jeffrey M. Gilbert, “802.11a Wireless Networks: Principles and Performance”, [http://www.ewh.ieee.org/r6/scv/comsoc/0205.pdf], 8 January 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Chairman, Code IS
   Department of Information Science
   Naval Postgraduate School
   Monterey, CA

4. Professor Tri T. Ha, Code EC/Ha
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

5. Professor Murali Tummala, Code EC/Tu
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

6. Cryptologic Research Laboratory
   ATTN: Nathan Beltz
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

7. Che Seng Goh
   Republic of Singapore Air Force