NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

EXTENDING IEEE 802.11b WIRELESS LOCAL AREA NETWORKS TO THE METROPOLITAN AREA

by

Patrick L. Mallory

December 2001

Thesis Advisor:	John McEachen
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
December 2001

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE: Title (Mix case letters)
Extending IEEE 802.11b Wireless Local Area Networks to the Metropolitan Area

5. FUNDING NUMBERS

6. AUTHOR(S)
Patrick L. Mallory

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)*

The IEEE 802.11b wireless local area networking (WLAN) protocol does not specify a maximum permissible range limitation. Rather, the protocol permits network data rates to vary based on the instantaneous link conditions present. This thesis analyzes the impact of distance on perceived network link quality for IEEE 802.11b WLAN systems. An experimental IEEE 802.11b wireless network testbed is developed and deployed within a metropolitan area (1-40 kilometers) for the quantitative analysis of link quality for various realistic types of network traffic. Additionally, the functional limitations of individual system components are identified for consideration in the planning of future experiments.

14. SUBJECT TERMS
Wireless LAN (WLAN), IEEE 802.11, IEEE 802.11b, complementary code keying (CCK), Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), direct sequence spread spectrum (DSSS), Medium Access Control (MAC) Layer, cost-effective access, Information Infrastructure

15. NUMBER OF PAGES 98

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

EXTENDING IEEE 802.11b WIRELESS LOCAL AREA NETWORKS TO THE METROPOLITAN AREA

Patrick L. Mallory
Lieutenant, United States Navy
B.S., Jacksonville University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2001

Author: Patrick L. Mallory

Approved by: John C. McEachen, Thesis Advisor

Murali Tummala, Second Reader

Jeffrey B. Knorr, **Chairman**
Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The IEEE 802.11b wireless local area networking (WLAN) protocol does not specify a maximum permissible range limitation. Rather, the protocol permits network data rates to vary based on the instantaneous link conditions present. This thesis analyzes the impact of distance on perceived network link quality for IEEE 802.11b WLAN systems. An experimental IEEE 802.11b wireless network testbed is developed and deployed within a metropolitan area (1–40 kilometers) for the quantitative analysis of link quality for various realistic types of network traffic. Additionally, the functional limitations of individual system components are identified for consideration in the planning of future experiments.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACK	ACKnowledgment frame
AP	Access Point
ANSI	American National Standards Institute
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CCK	Complementary Code Keying
COR	Central Outdoor Router
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
dB	decibels (watt reference)
dBi	decibels (isotropic radiator reference)
dBm	decibels (miliwatt reference)
DEM	Digital Elevation Model
DCF	Distributed Coordination Function
DIFS	Distributed Interframe Space
DFE	Decision Feedback Equalizer
DPSK	Differential Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSP	Digital Signal Processor
DSSS	Direct Sequence Spread Spectrum
EP	Extension Point
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
GPS	Global Positioning System
IAPP	Inter-Access Point Protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	InfraRed
IFS	InterFrame Spacing
ISM	Industrial, Scientific, and Medical
LAN	Local Area Network
LOS	Line Of Sight
MAC	Medium Access Control
MAN	Metropolitan Area Network
MBOK	*M*-ary Bi-Orthogonal Keying

Mbps	Megabits Per Second
MKK	Ministery of Telecommunications
MHz	MegaHertz
MOK	M-ary Orthogonal Keying
NAK	No AcKnowledgement frame
NAV	Network Allocation Vector
NOS	Network Operating System
OCDM	Orthogonal Code Division Multiplex
OFDM	Orthogonal Frequency Domain Multiplexing
ORC	Outdoor Router Client
PAN	Personal Area Network
PBCC	Packet Binary Convolutional Coding
PCF	Point Coordination Function
PHY	Physical, Physical Layer
PN	Pseudorandom Number
PPM	Pulse Position Modulation
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
RC4	Rivest stream Cipher 4
RF	Radio Frequency
ROR	Remote Outdoor Router
RTS	Request To Send
SFD	Start of Frame Delimiter
SIFS	Short InterFrame Space
SNR	Signal to Noise Ratio
STA	STAtion
TDMA	Time Division Multiple Access
VOFDM	Vector Orthogonal Frequency Division Multiplexing
USGS	U.S. Geologic Survey
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Networking
WMAN	Wireless Metropolitan Area Network
XOR	eXclusive OR (Logic Operation)

ACKNOWLEDGEMENTS

For Ethanne – though we have been together for almost two decades, these last two years have been my favorite. Your unique strength and tenderness is the foundation of our family, your love brightens my every day and our shared goals give my life meaning. The time and places we have shared will enrich my soul forever. I am so very fortunate to have you as my wife and friend.

For Joshua and Davin – watching you both grow over these last two years has filled my days with pride and wonder. I am so grateful for the moments we have had to play and learn together. Your unconditional love and friendship are a true inspiration.

For Dr. John McEachen and Dr. Murali Tummala – I am sincerely grateful for your remarkable dedication to supporting my research goals. Your superb classroom instruction and unrivaled understanding of computer networks combined with thought provoking direction along the way ensured a most rewarding thesis experience. Thank you for your vision and continuing thoughtful advise and support.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

In this thesis, we investigate the impact that metropolitan terrain and extended ranges have on the performance of IEEE 802.11b wireless local area network (WLAN) standards and applications in order to assess this protocol's suitability for use throughout the Department of Defense. Although the IEEE 802.11b WLAN specification was primarily intended for use in extending "wired" LANs to mobile users within an indoor office environment, we show that this same COTS technology can be applied to an outdoor metropolitan environment as well.

Since the main objective of WLANs is portable data communications, we selected file transfer and web browsing throughput as our performance metrics as they typify the network traffic and services most commonly found throughout the global Internet.

Our wireless metropolitan area network (WMAN) testbed made use of multiple Wi-Fi certified 802.11b wireless routers, access points and mobile stations configured for both point-to-point and point-to-multipoint links. For configurations that tested links extending beyond the range of the immediate campus area, we used signal amplifiers and directive antennas to ensure sufficient link margin. To ensure that our tests results would accurately reflect the performance achieved in a real-world implementation, we used standard WEP-128 encryption to provide data confidentiality across all wireless links.

All performance metrics were collected from a mobile laptop located within the coverage area of our outdoor wireless access point located on the roof of Spanagel Hall. Two area surveys were conducted, one from a small boat on the Monterey Bay and the other from an automobile throughout the Monterey metropolitan area. Throughput measurements were based on both the time required to transfer a standard 15-MB file to and from the laptop and the time required to transfer a series of relatively short data packets representative of web-based network traffic. Additionally, signal power, noise power and signal-to-noise ratio data were collected at each survey location in order to

characterize the local and remote channel conditions presently affecting bit error rate (BER) and packet loss.

The at-sea portion of our survey tested point-to-multipoint links over land and water at ranges from 2.3 to 8.2 miles between the Spanagel Hall access point and the mobile wireless laptop. The signal from the access point was amplified to 1 Watt and transmitted from a 90º 19 dBi sector panel antenna to the mobile station similarly equipped with a 1 Watt amplifier and a 30º 15 dBi radome enclosed Yagi antenna. The configuration achieved throughputs of 1.7 Mbps at 2.3 miles and 900 Kbps at 8.2 miles.

The land-based portion of our survey tested point-to-multipoint links over land at ranges from 0.6 to 8.2 miles between the Spanagel Hall access point and the mobile wireless laptop. The signal from the access point was again amplified to 1 Watt but transmitted this time from a 360º 15 dBi omnidirectional antenna to the mobile station similarly equipped with a 1 Watt amplifier and a 30º 15 dBi radome enclosed Yagi antenna. The configuration achieved upload throughputs of 2.1 Mbps at 0.6 miles and 200 Kbps at 8.2 miles and download throughputs of 2.2 Mbps at 0.6 miles and 100 Kbps at 8.2 miles

An analysis of our combined results indicated throughput falling off with distance in a non-linear fashion. By computing the mean normalized variance of both the local and remote signal-to-noise ratios, we discovered that the SNR became increasingly variable with distance throughout our survey area. This exponentially increasing variability directly affects packet delay due to dropped packets and signal loss, negatively impacting perceived network link quality.

In conclusion, our tests showed that CCK modulation yields acceptable high and medium rate performance near 2 Mbps at ranges of less than 2 miles in outdoor environments. At ranges beyond 2 miles, DQPSK modulation and DBPSK modulation yield standard and low rate performance with graceful near-linear degradation (down to approximately 200 Kbps at 20 miles).

Additionally, we found that the highly variable nature of link signal-to-noise ratio *seen* by a mobile station roaming within the tall office buildings of a city center severely degraded overall throughput performance, but that this degradation was much less noticeable for mobile web users due to the relatively short packets and the frequent alignment of short-lived LOS paths as they roamed throughout the multipath environment.

In summary, we found IEEE 802.11b achieves acceptable file transfer throughputs of 2 Mbps at ranges less than 2 miles and 200 Kbps for ranges out to 20 miles over water. Even the intense multipath fading environments typical of a metropolitan city center can yield acceptable throughputs for email and web-based traffic if sufficiently frequent opportunities exist for LOS paths between the mobile station and the associated access point.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Today more than ever, the success of U.S. naval operations and indeed the success of nearly every modern human enterprise hinges on the timely flow of critical information. Over the past decade, war-fighters and the private sector alike have seen the emphasis of their information requirements expand from one of quality intelligence to a need for <u>continuous</u> quality intelligence. This need for an uninterrupted flow of information up, down and throughout an organization has driven a nearly universal demand for seamless access to network resources from portable devices. Intense demand for fast, continuous, cost-effective computer-to-computer connectivity continues to drive the rapid adoption of wireless local area network (WLAN) technology beyond the expectations of the original standards. Thus, as the United States Navy continues to evolve toward a network-centric philosophy of battle group operations, the potential use of this technology for metropolitan area network (MAN) applications will become increasingly important at the operational and tactical levels of warfare.

Accelerated decision cycles and fundamental changes to traditional organizational structures will drive the distribution of critical intelligence products down to the individual war-fighters on, above and below the sea-borne battle-space. Therefore, the behavior of wireless information networks, when constrained by various environmental and physical limitations, is of critical interest in the development of naval information systems. These limitations include network resource constraints, system configuration options and extrinsic environmental conditions, such as environment geometry and channel noise.

This thesis makes exclusive use of commercially available off-the-shelf WLAN equipment and software throughout all test scenarios in order to explore the limitations of this technology and the effect of real-world geography and environmental conditions on perceived link quality. Although the original standards envisioned use within a confined area of no more than 300 meters, several vendors have introduced technologies which potentially extend WLANs to ranges exceeding 50 kilometers, but the ramifications of such extensions have not been widely studied.

This thesis describes the development of an experimental IEEE 802.11b wireless LAN extended to a metropolitan area and presents a quantitative analysis of the network performance achieved for various realistic types of network traffic. Additionally, the functional limitations of individual system components are identified for consideration in the planning of future experiments.

B. OBJECTIVES

Given the importance of wireless applications within the context of future naval information systems, this thesis analyzes the performance of wireless network links in terms of their robustness and suitability for mobile applications when constrained by a real-world metropolitan environment. Experimental measurements are taken by a mobile node located within the metropolitan area in order to understand how perceived wireless link quality is affected by each of the following important WLAN implementation aspects:

- Transmit Power, Frequency and Interference
- Multipath Propagation, Path Loss and Range
- Installation, Interoperability and Scalability
- Network Security and Encryption
- Health Risks

As a concurrent objective of this work, an experimentation module was developed within the Advanced Networking Laboratory that demonstrates wireless network management applications and serves as a practical testing environment for various electrical engineering coursework and research activities.

C. RELATED WORK

Because wireless LAN technology is still so new and dynamic, significant research results continue to emerge within industry. These technology companies can be lumped into one of two types: long-established, well-known firms and relatively young start-ups. Those in the first category, such as Cisco Systems, Hewlett-Packard, and Lucent, continue to spend billions on the research, development and commercialization of new products. Start-up companies, on the other hand, offer a youthful energy and enthusiasm that often stimulates innovative ideas that either succeed or fail.

Table 1 and the following paragraphs summarize the major industry trade associations, technology alliances, standards bodies, and independent test labs that are investigating wireless network issues related to this thesis.

Organization	Mission	Relevant Technology
IEEE 802.11	The Standards Body that wrote the wireless Local Area Network specification for 802.11	802.11 FH 802.11 DS 802.11 HR 802.11 VHR
IEEE 802.15	The Standards Body that wrote the Wireless Personal Area Network specifications for 802.15 and Bluetooth	802.15 802.15 HR
IEEE 802.16	The Standards Body that wrote the Broadband Wireless Access specification for 802.16	802.16
Wireless Ethernet Compatibility Alliance (WECA)	A Technology Alliance that certifies interoperability of IEEE 802.11 products and promotes Wi-Fi as the global wireless LAN standard	IEEE 802.11
Wireless LAN Association (WLANA)	A Trade Association that educates and promotes the use of wireless networking technology	Personal Area Networks, Local Area Networks, LAN to LAN bridge and Public Access
Broadband Wireless Internet Forum (BWIF)	A Technology Alliance that educates and promotes the use of broadband wireless networking technology	VOFDM - Vector Orthogonal Frequency Division Multiplexing
Bluetooth Special Interest Group (Bluetooth SIG)	A Technology Alliance that writes Bluetooth Specs and promotes Bluetooth and Bluetooth interoperability	Bluetooth
Home RF Working Group	A Technology Alliance that developed a specification for wireless communications in the home	SWAP (Shared Wireless Access Protocol)
OFDM Forum	A Technology Alliance that fosters a single compatible OFDM standard	OFDM - Orthogonal Frequency Division Multiplexing
HiperLAN2 Global Forum	A Standards Body driving the adoption of HiperLAN2 as the global broadband wireless technology in the 5-GHz Band	HiperLAN2
ETSI HiperLAN	A Standards Body that writes specifications for HiperLAN1	HiperLAN1
ETSI BRAN	The Standards Body that wrote the spec for Broadband Radio Access Networks (BRAN) for Europe and beyond	HiperLAN/2 and HIPERACCESS
University of New Hampshire Interoperability Lab	An Independent Test Lab	Various

Table 1. Major Groups within the Wireless Networking Industry.

The Institute for Electrical and Electronic Engineers (IEEE) is the world's largest technical professional society consisting of over 320,000 members in 147 countries. The IEEE is a significant standards-making body responsible for creating, developing, integrating, sharing and applying knowledge about electrical and information technologies and sciences for the benefit of humanity and the profession. Under the auspices of this organization, the IEEE 802 LAN/MAN Standards Committee develops local area network standards and metropolitan area network standards (e.g., the Ethernet family, Token Ring, wireless LAN, bridging and virtual bridged LANs) and contains the 802.11 WLAN, 802.15 Wireless Personal Area Network (WPAN) and 802.16 Broadband Wireless Access Working Groups. The IEEE 802.11b wireless LAN standard is particularly relevant to this thesis.

The Wireless Ethernet Compatibility Alliance (WECA) is an industry-sponsored consortium of member companies that certifies the interoperability of Wi-Fi (IEEE 802.11b High Rate) wireless networking products. Current member companies are listed in Table 2.

2Wire	3Com	Above Cable Acer	Acrowave	ActionTec	Agere Systems
Airwave	Alcatel	AMBIT	AMD	AOW	Apple
ARESCOM	Artem	Askey	Atheros	Atmel	Avaya
Aware	Breeze	Broadcom	BroMax	Buffalo Tech	CCandC
Cilys	Cirrus Logic	Cisco	Colubris Networks	Compaq	Connexion
Dell	Delta Networks	Digital Networks	D-Link	Elsa	Emtac
Enterasys	Envara	Epson	Ericsson	Eumitcomm	Excilan
Fiberlink	Fujitsu	Funk Software	Galtronics	Gateway	GCD
Gemtec	Global Sun Tech	GriC	hereUare	Hewlett Packard	High Speed Surang
HWN	IBM	Icom	Illuminet	Intel	Intermec
Intersil	IO Data	iPass	LGnetwork	LinCom	LinkSys
Lucent	Marconi	MobileStar	Mobilian	NDC	NEC
NETGEAR	NetMotion	NetSeal	NextCom	No Wires Needed	Nokia
NOVA Tech	NTT-ME	OTC Wireless	Parker Vision	PCTEL	Phillips
Proxim	PsiONtecklogix	RealTEK	Resonext	RFmicrodevices	RFtnc
Samsung	ServiceFactory	Sharp	Siemens	Sony	Spectralink

Symbol	Synad	SystemONic	TDK	Tella	Texas Instruments
Toshiba	Toshiba	TOYO	TROY	TSi	TTS LiNX
USi	WaveLink	Wayport	Winmate	Wireless Solutions	Woodside Networks
Z-Com					

Table 2. WECA Member Companies.

The use of Wi-Fi certified WLAN products in this thesis was essential to the ease of installation and administration necessary for an experimental wireless testbed while assuring a sustained equivalent functionality and performance comparable to that of wired 10BaseT networks.

The Wireless LAN Association (WLANA) is a nonprofit consortium of major WLAN vendors established to help educate the marketplace about WLANs and their uses. WLANA develops educational materials on WLAN user's experiences, applications, and industry trends. The association's Web site includes industry studies, white papers, application stories and links to related topics and member Web sites. WLANA's current sponsor companies are 3Com, Cisco, Enterasys Networks, Intersil, Intermec, Nortel Networks, NoWireNeeded and Symbol.

The Broadband Wireless Internet Forum (BWIF) is an incorporated not-for-profit association of 51 promoting and adopting companies committed to driving product roadmaps that will lower costs, simplify deployment of advanced services and ensure the availability of interoperable solutions based on VOFDM technology. The Web site includes information, such as white papers, the BWIF Specifications Document Overview and descriptions of what VOFDM is and how it can be used.

The Bluetooth Special Interest Group (Bluetooth SIG) is a forum for enhancing the Bluetooth specification and providing a vehicle for interoperability testing. The Web site includes information, such as the release of Bluetooth 1.0 Specification and an explanation of what Bluetooth is and how it can be used. The companies leading this group are 3Com, Ericsson, Intel, IBM, Lucent, Microsoft, Motorola, Nokia and Toshiba.

Home RF is an industry alliance of more than 70 companies interested in establishing interoperable wireless digital communication between PCs and consumer electronic devices anywhere in and around the home. The web site includes information such as a description of the HomeRF Protocol Specification and various white papers and presentations.

While not directly relevant to the network studied within this thesis, it is worth noting here that the first draft of 802.11g was approved on 16 Nov 2001 to unify 2.4 and 5-GHz products and systems. Under this proposed specification, 802.11b products would achieve the same 52 Mbps maximum capacity currently enjoyed by 802.11a products operating at 5 GHz.

The OFDM/CCK technology currently proposed for the 802.11g extension would require carrier frequency downshifting from the 5-GHz standard to the 2.4-GHz band, combining the features of the 802.11a and 802.11b technologies in the same band. To maintain backward compatibility, some signaling protocols (header formats), clocking rates and sample rates may be different as the high-bit-rate protocols are blended with the existing 802.11b standard. Similar MAC and modulation schemes will also mean that dual-band radios will be much easier to build, allowing for widespread deployment to accommodate nearly any 802.11-compliant user. Although the formal document is sure to undergo several levels of revision and editing before final publication, the standard is expected to receive final approval in October of 2002 [3].

It is interesting to note that the research into WLAN systems that started some 20 years ago fostered the development of new ideas and techniques that continue to yield new applications and systems today. Moreover, established companies are actively involved in this booming market. While many significant improvements are being made to the related underlying technologies, this thesis focuses on the practical analysis of wireless link quality in super-standard, commercial implementations of the current technology.

D. THESIS ORGANIZATION

This thesis is organized into six chapters and a supporting glossary. Chapter II provides an overview of the relevant aspects of wireless LANs. Chapter III explains the key concepts and underlying technologies that support packet radio networks like 802.11b WLANs. Chapter IV presents a detailed description of the components that comprise the 802.11b wireless metropolitan area testbed. Chapter V describes the experimental procedures and presents the results from various testbed configurations studied in this thesis. Chapter VI summarizes the findings and wraps up with recommendations for further research. Appendix A details the extended signal and noise power measurements collected at each survey location.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS LAN OVERVIEW

A. INTRODUCTION

Today in the country and world over, communications technologies are leading a revolution in the way people live, work, play and fight wars. The number of cellular telephone subscribers and people accessing the Internet, the growth of electronic business and the ease with which the military forces communicate while fighting the war on terrorism all exemplify this evolution in information technology.

Access to information has become a necessity. The information available on the Internet and the ease of accessing that information allows professionals of vastly different fields to leverage the knowledge and skills of others in ways never before possible. The Internet has become a competitive and cooperative necessity, an indispensable consultation tool as well as an open bulletin board on which to showcase information to the world.

It is not surprising, therefore, that in this age of fierce competition, we find the Navy exploring new ways to communicate and share scare resources at all levels while mitigating the combined risk. Wireless LAN applications offer the military forces the reliable, high performance connectivity of wired LANs with the added flexibility, affordability and mobility inherent to the wireless medium. With wireless networking, there is no need to pull extra wires, stretch cabling across a large space, break through walls or dig trenches to the next building. With wireless networking, a temporary LAN connection or network can be established anywhere indoors or outdoors and still provide the full range of local area network resources to mobile computer users, such as email, Internet, corporate database access, etc.

B. WIRELESS LAN PRIMER

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

1. Why use Wireless Networking?

Wireless LANs frequently augment rather than replace wired LAN networks – often providing the last few feet of connectivity between a wired network and the mobile user. Consequently, the use of wireless LANs has exploded throughout the Navy and greater DoD. The widespread reliance on networking within the services and the meteoric growth of the Internet testifies to the benefits of shared data and resources. Industries around the world have also profited from the productivity gained by using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today, wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of users.

With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, convenience, and cost advantages over traditional wired networks:

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

- Installation Speed and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

- Installation Flexibility: Wireless technology allows the network to go where wire and fiber cannot go.

- Reduced Maintenance Costs: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.

- Scalability: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

2. Wireless LAN Operation

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

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

In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard cabling. At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point (or the antenna attached to the access point) is usually mounted high but may be mounted essentially anywhere that is practical in order to obtain the desired radio coverage.

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

3. Wireless LAN Configurations

Wireless LANs can be simple or complex. WLANs can be used either to replace wired LANs, or as an extension of the wired LAN infrastructure. In its most basic form, two or more wireless nodes, or stations (STAs) comprise a basic service set (BSS). In this configuration (Figure 1), stations communicate directly with each other on a peer-to-peer level sharing a given cell coverage area. This type of network is often formed on a temporary basis and is said to be operating in *ad hoc mode*, or as an independent basic service set (IBSS). Such on-demand networks require no administration or pre-configuration and each client would only have access to the resources of the other client and not to a central server. [4].

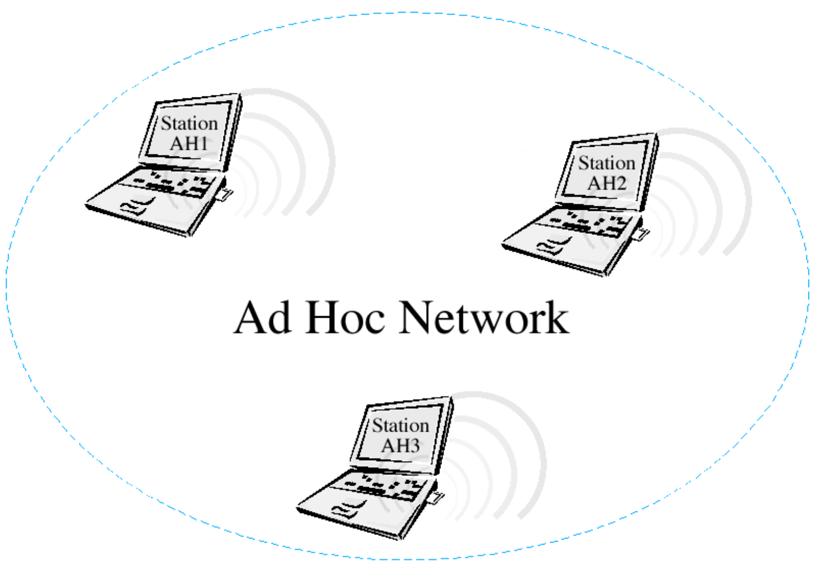

Figure 1. Ad Hoc Wireless LAN Configuration.

In most instances, however, the BSS contains an Access Point (AP). The main function of an AP is to form a bridge between wireless and wired LANs. The AP is analogous to a base station used in cellular phone networks. When an AP is present, stations do not communicate on a peer-to-peer basis. All communications between stations or between a station and a wired network client go through the AP. AP's are not mobile and form part of the wired network infrastructure. A BSS in this configuration is said to be operating in the *infrastructure mode*.

The extended service set (ESS) shown in Figure 2 consists of a series of overlapping BSSs (each containing an AP) connected together by means of a distribution system (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between APs to permit seamless campus-wide coverage.

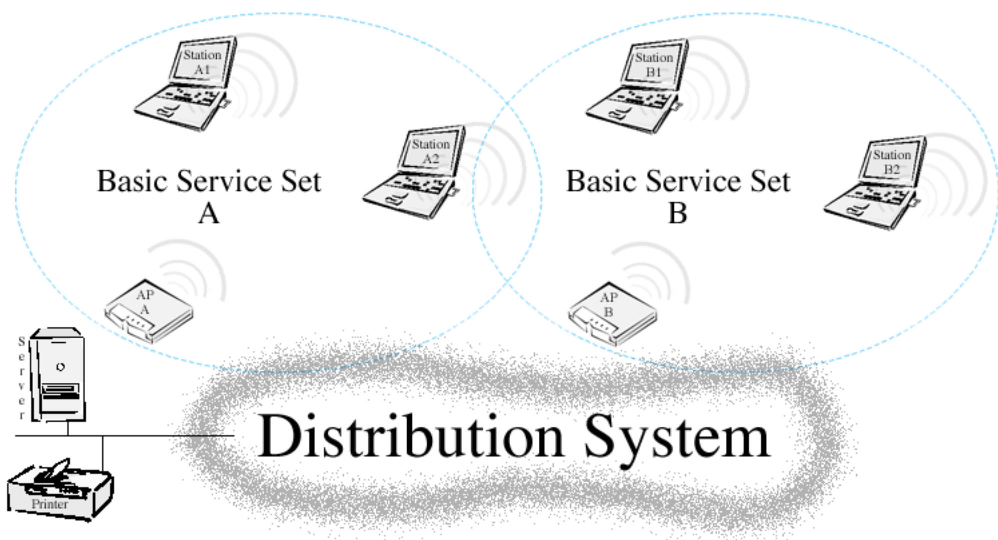

Figure 2. Infrastructure Wireless LAN Configuration.

In access point-based networks, the stations within a group or cell can only communicate directly with the access point. The access point forwards messages to the destination station within the same cell or through the wired distribution system to another access point, through which messages arrive at the destination station. Installing an access point can extend the range of an ad hoc network, effectively doubling the range at which the devices can communicate. Since the access point is connected to the wired network, each client would have access to server resources as well as to other clients. Each access point can accommodate many clients; the specific number depends on the number and nature of the transmissions involved. Many real-world applications exist where a single access point services from 15-50 client devices.

a. Multiple access points and roaming

Typical commercial access points have a finite range, on the order of 100 meters indoors and 300 meters outdoors. In a very large facility such as a warehouse or on a college campus, it will probably be necessary to install more than one access point. Access point positioning is accomplished by means of a site survey; Figure 3 below depicts an example coverage prediction we generated for a single 2.4-GHz 802.11 AP with a nominal output power of 10mW located at six different locations throughout the main floor of the campus library. The goal is to blanket the coverage area with overlapping coverage cells so that clients might roam throughout the area without ever losing network contact. The ability of clients to move seamlessly among a cluster of access points is called roaming. Access points hand the client off from one to another in a way that is invisible to the client, ensuring unbroken connectivity.

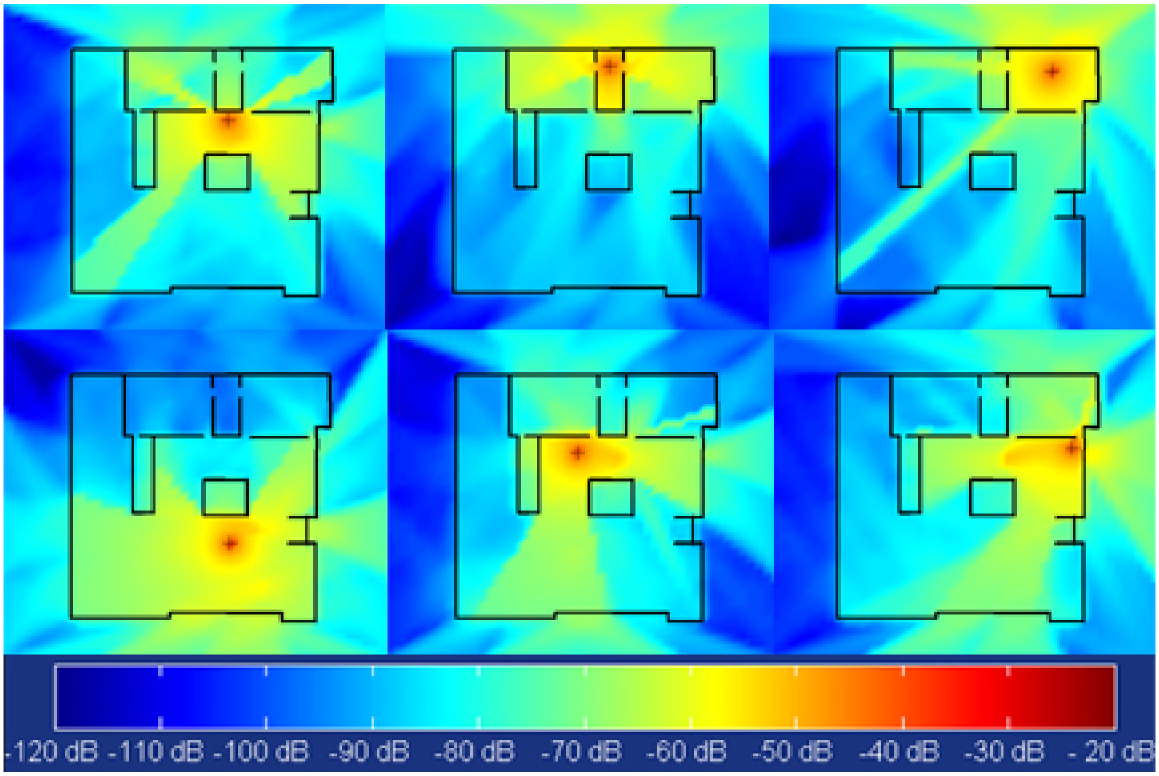

Figure 3. RF Propagation Prediction for Main Floor of NPS Library.

b. *Use of an extension point*

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

c. *Use of directional antennas*

One last item of wireless LAN equipment to consider is the directional antenna. If a wireless LAN located in building X needs to extend a mile away to building Y, one solution would be to install a directional antenna at each building and align them to point at each other. Just as the antenna at building X is connected to your wired network via an access point, the antenna at building Y is similarly connected to an access point which enables wireless LAN connectivity in that facility.

4. User Considerations

While wireless LANs provide installation and configuration flexibility and the freedom inherent in network mobility, the following factors are important when considering wireless LAN systems.

a. Range and coverage

The distance over which RF and IR waves can communicate is a function of product design and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal and even people, can affect how energy propagates and thus, what range and coverage a particular system achieves. Solid objects block infrared signals, thereby imposing additional limitations. Most wireless LAN systems use RF because radio waves can penetrate most indoor walls and obstacles. While the range (or radius of coverage) for typical wireless LAN systems varies from 100 meters indoors to 300 meters outdoors, coverage can be extended through the use of microcells in order to achieve true freedom of mobility via roaming.

b. Throughput

As with wired LAN systems, actual throughput in wireless LANs is product and set-up dependent. Factors that affect throughput include the number of users, propagation factors such as range and multipath, the type of wireless LAN system used, as well as the latency and bottlenecks on the wired portions of the LAN. Data rates for the most widespread commercial wireless LANs are in the 10 Mbps range. Users of traditional Ethernet or Token Ring LANs generally experience little difference in performance when using a wireless LAN [5]. Wireless LANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, Internet access, and access to multi-user databases and applications.

As a point of comparison, it is worth noting that state-of-the-art V.90 modems transmit and receive at optimal data rates of 56.6 Kbps. In terms of throughput, a wireless LAN operating at only 2 Mbps is over thirty times faster.

c. Integrity and reliability

Wireless data technologies have been proven through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare and is usually short-lived within the workplace. Proven wireless LAN technology and the limited distance over which these signals travel, results in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networks [4].

d. Compatibility with the existing network

Most wireless LANs provide for industry-standard interconnection with wired networks such as Ethernet or Token Ring. Wireless LAN nodes are supported by network operating systems in the same fashion as any other LAN node: through the use of the appropriate drivers. Once installed, the network treats wireless nodes just like any other network component [5].

e. Interoperability of wireless devices

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

f. Interference and coexistence

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a wireless LAN system. Microwave ovens are a potential concern, but most wireless LAN manufacturers design their products to account for microwave interference. Other concerns are the co-location of multiple wireless LANs or cordless telephones in the same frequency band. While wireless LAN components from some manufacturers interfere with the wireless LAN components of other manufacturers, others coexist without interference. This issue is best addressed directly with the appropriate vendors.

g. Licensing issues

In the United States, the Federal Communications Commission (FCC) governs radio transmissions, including those employed in wireless LANs. Other nations have corresponding regulatory agencies. Wireless LANs are typically designed to operate in portions of the radio spectrum where the FCC does not require the end-user to purchase a license to use the airwaves. In the U.S. most wireless LANs broadcast over one of the ISM (Instrumentation, Scientific, and Medical) bands. These include 902-928 MHz, 2.4-2.4835 GHz and 5.725-5.850 GHz as illustrated in Figure 4 below. For wireless LANs to be sold in a particular country, the manufacturer of the wireless LAN must ensure its certification by the appropriate agency in that country.

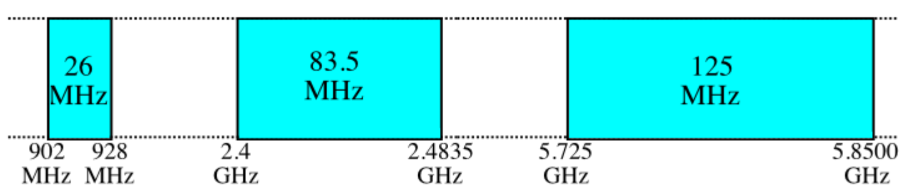

Figure 4. The Industrial, Scientific and Medical (ISM) Frequency Bands.

h. Simplicity and ease of use

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

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

i. Security

Because security has long been a design criterion for wireless devices, security provisions are typically built into wireless LANs to make them more secure than most wired LANs. It is difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic and the addition of encryption techniques make it burdensome for eavesdroppers to gain unauthorized access to network traffic. In general, security professionals should require individual nodes be security-enabled before they are allowed to access privileged network resources.

j. Cost

A wireless LAN implementation includes both infrastructure costs, for the wireless access points, and user costs, for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed; access points range in price from $200 to $2000. The number of access points typically depends on the required coverage region, the number and type of user services that must be supported and the degree to which these users are authenticated and their data is protected.

The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms, and range in price from $100 to $1,000.

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

k. Scalability

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

l. Battery life for mobile platforms

End-user wireless products are designed to run off the AC or battery power of their host notebook or hand-held computer. Wireless LAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.

m. Safety

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

C. SUMMARY

This chapter described the features that make wireless LANs both effective extensions and attractive alternatives to wired networks. Relevant networking concepts and industry terminology were combined to stimulate interest in subsequent chapters of this work. The next chapter introduces the key elements of the 802.11 WLAN standard, architectural details and the common implementation features necessary to understand the basic operation of a WLAN extended to a metropolitan area.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WIRELESS CHARACTERISTICS AND TECHNOLOGIES

A. INTRODUCTION

In this chapter, we define the IEEE 802.11 Wireless LAN Standard and examine why direct sequence spread spectrum (DSSS) modulation is better suited for use in the metropolitan area network testbed. We further consider the major objectives, intended architecture and underlying technologies of 802.11b and conclude with a review of the features that are central to this thesis.

B. IEEE 802.11

802.11 is the Institute of Electrical and Electronics Engineers (IEEE) standard for wireless networking – sending Ethernet data packets through the air. The standard allows for wireless integration with wired IEEE 802.3 Ethernet networks using devices called access points or base stations. Thus, the IEEE 802.11 wireless standard supports all standard Ethernet network protocols including TCP/IP, AppleTalk, NetBEUI and IPX [2].

The completion in 1997 of 802.11 was a key first step in the evolutionary development of wireless networking technologies. Although the first wireless LAN products appeared around 1990, 802.11 is the first standard focused on maximizing interoperability between differing brands of wireless LANs while introducing a variety of performance improvements and benefits. With the ratification of a revised version of the 802.11 standard called 'High Rate' on 20Aug1999, 802.11 now provides even higher data rates while maintaining compatibility with the original 802.11 protocol.

In addition to enabling high performance and robust operation, 802.11 also promises multi-vendor interoperability across products with the same Physical Layers (PHYs). As a consequence, customers are free to mix and match vendor components as their application requirements dictate; thereby fostering the delivery of lower cost components through increased competition. Today, almost all WLAN vendors have driven their product lines to comply with IEEE 802.11 High-Rate specification.

C. IEEE 802.11 MEDIA ACCESS CONTROL

IEEE 802.11 is limited in scope to the physical (PHY) layer and medium access control (MAC) sublayer, with MAC origins to the IEEE 802.3 Ethernet standard. The 802.11 MAC layer protocol is extremely robust and feature rich. It includes Sequence Control and Retry fields supporting a feature called MAC-layer acknowledge that minimizes interference and maximizes usage of the bandwidth available on the wireless channel. Type/Subtype and Duration fields ensure reliable communications in the presence of hidden stations. Wired Equivalent Privacy (WEP) fields provide for data security that is equal to that achievable with standard Ethernet. Sequence Control and More Frag fields support a packet fragmentation feature that can allow a WLAN to operate in the presence of interference or signal fading [1].

The 802.11 MAC can work seamlessly with standard Ethernet, via a bridge or AP, to ensure that wireless and wired nodes on a LAN can interoperate with each other. The basic medium sharing mechanism allows compatible physical layers to operate together by using the carrier sense multiple access with collision avoidance (CSMA/CA) protocol and a random back-off time following a busy medium condition. In addition, all directed traffic uses immediate positive acknowledgement (ACK) frame, in which the sender schedules a retransmission if it does not receive an ACK [1].

While CSMA/CA and Ethernet's carrier sense multiple access with collision detection (CSMA/CD) have similarities, their one fundamental difference is the way they handle collisions. In wire-based networks, such as Ethernet, it is not technically complicated to detect if transmissions from two stations are colliding. Detecting collisions in wireless systems that use only one channel is impractical, however, because of the large dynamic range of receive levels. Therefore, 802.11 chose CSMA/CA, which uses a collision avoidance scheme [1].

The 802.11 CSMA/CA protocol is designed to reduce the collision probability between multiple stations accessing the medium, at the point in time where collisions would most likely occur. The highest probability of a collision would occur just after the medium becomes free following a busy medium, because multiple stations would have been waiting for the medium to become available again. Therefore, a random back-off arrangement is used to resolve medium contention conflicts, as illustrated in Figure 5.

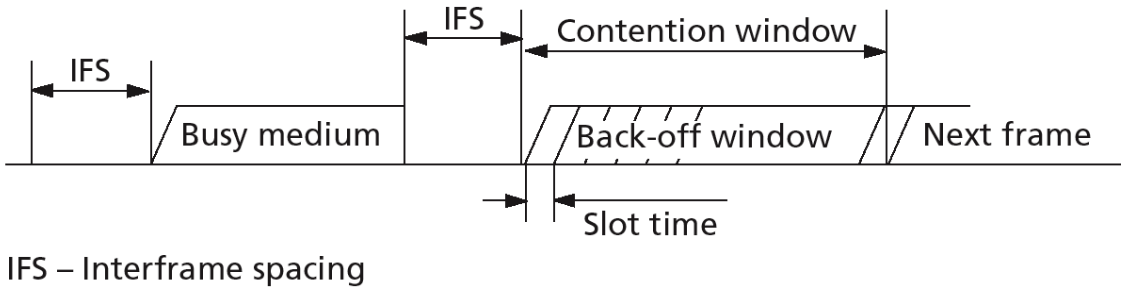

Figure 5. Basic CSMA/CA Behavior.

A very short-duration carrier detect turnaround time is fundamental to this random wait characteristic. The 802.11 standard DSSS uses a slotted random wait behavior based on 20µs time slots, which cover the carrier detect turnaround time.

In addition, the 802.11 MAC defines an option for reserving a medium using request-to-send/clear-to-send (RTS/CTS) polling interaction and point coordination (for time-bounded services). After a busy-medium period, all wireless LAN devices must wait during an interframe spacing (IFS) period. After waiting a random number of time slot intervals, these devices can attempt to transmit, provided no other transmission was detected in the interim.

1. Roaming Provisions

802.11 allows clients to roam among multiple APs operating on the same or different channels. For example, every 100-ms, an AP might transmit a beacon signal that includes a time stamp for client synchronization, a traffic indication map, an indication of supported data rates and other parameters. Roaming clients use the beacon to gauge the strength of their existing connection to an AP; if the connection is too weak, the roaming station can attempt to associate itself with a stronger AP.

2. Power Management

802.11 adds features to the MAC that can maximize battery life in portable clients via power-management schemes. Power management causes problems with WLAN systems because typical power-management schemes place a system in sleep mode (low or no power) when no activity occurs for some specific or user-definable time period. Unfortunately, a sleeping system can miss critical data transmissions.

To support clients that periodically enter sleep mode, the 802.11 specified that APs include buffers to queue messages. Sleeping clients are required to wake periodically and retrieve any waiting messages. APs are permitted to dump unread messages after a specified time passes.

3. Wired Equivalent Privacy

One final area of differentiation between 802.11 and either wired LANs or previously existing WLAN implementations centers on data security. The standard defines a mechanism through which the WLANs can achieve Wired Equivalent Privacy (WEP). If WEP is enabled, then all data transmitted over the wireless network is encrypted.

4. Interoperability

One of the biggest gains from the 802.11 standard is the assurance that products from different vendors will interoperate with each other. This means that users can purchase wireless LAN cards and access points from different vendors and be assured they will communicate with each other; providing greater flexibility in selecting system components that best meet their application needs. An additional level of 802.11b High Rate interoperability testing and certification, known as Wireless Fidelity (Wi-Fi), is performed by the Wireless Ethernet Compatibility Alliance (WECA) for member company products. The details and results of this testing are available from the University of New Hampshire Interoperability Lab. WECA is an industry-sponsored consortium formed to certify the interoperability of Wi-Fi (IEEE 802.11b High Rate) wireless networking products. Once a vendor's WLAN products have successfully completed the IEEE 802.11b High Rate standard industry interoperability testing, they are awarded the Wi-Fi "seal of approval" to assure customers that the products bearing this logo will work together.

As discussed previously, the 802.11 working group continued to make rapid improvements to the specification, culminating with the ratification of the 802.11b High Rate specification in 1999 supporting data rates up to 11 Mbps. The High Rate standard's 11-Mbps PHY layer uses complementary code keying (CCK) technology, a modulation technique based on DSSS that provides data rates up to 11 Mbps with fallback compatibility to 5.5 Mbps, 2 Mbps, and 1 Mbps. CCK uses the same bandwidth as the 2 Mbps DSSS standard to ensure interoperability with legacy IEEE DSSS systems. As in the wired world, higher data rates are increasingly demanded by applications such as streaming video, telephony and multimedia. Moreover, faster peak data rates effectively allow more nodes to connect to a WLAN over a single channel.

D. IEEE 802.11 PHYSICAL LAYER

The de-facto communication technology for wireless LANs that operate unlicensed in the worldwide 2.4-2.5-GHz ISM band is spread-spectrum, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, more difficult to detect. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise.

Spread Spectrum communications benefit from inherent transmission security, resistance to interference from other radio sources, redundancy, and resistance to multi-path and fading effects. As a result, Spread Spectrum systems can *coexist* with other radio systems without disturbing each other. It was primarily for this reason that Spread Spectrum was chosen as the modulation technique to allow license-free operation within the worldwide Industrial Scientific Medical (ISM) band.

The term Spread Spectrum describes a modulation technique in which radio frequency energy is *spread* over a much wider bandwidth than is necessary for the required data rate. While many of the benefits of such systems are not readily apparent, one clear benefit is superior noise rejection. The superior noise rejection of spread spectrum systems makes them ideally suited for operation within the noisy ISM band[†].

Because the standard offers a choice of different RF based PHY layers, vendor implementations use either DSSS or FHSS. The 802.11 wireless standard does not, however, support interoperability across different system types. Therefore, 802.11 DSSS systems are not compatible with 802.11 FHSS, 802.11 DFIR systems, or other wireless solutions such as HomeRF.

In 802.11, the DSSS PHY specifies a 2 Mbps peak data rate with optional fallback to 1 Mbps in very noisy environments while the FHSS PHY specifies a 1 Mbps peak data rate with optional fall-forward to 2 Mbps in noise-free environments. However, most vendors have chosen to implement DSSS as specified by the 802.11 High Rate (11 Mbps) standard, providing an easy migration from a 2 Mbps 802.11 DSSS system to an 11 Mbps 802.11 HR system as the underlying modulation scheme is very similar. Because 2 Mbps 802.11 DSSS systems can co-exist with 11 Mbps 802.11 HR systems, this migration strategy also assured customers a smooth transition to the higher data rate technology.

The two Spread Spectrum techniques standardized under IEEE 802.11 and allowed by the FCC in the ISM band are frequency hopping and direct sequence. In frequency hopping spread spectrum (FHSS) communications, the channel between a synchronized transmitter and receiver is rapidly changed according to a standardized pseudo-random pattern so that the signal appears to occupy a wide bandwidth over time.

[†] The portion of the ISM band located at 2.4 GHz is sometimes called the *junk* band because it is contaminated by microwave oven emissions at 2.43 GHz. Until very recently, it was felt that no communication system would ever want to co-occupy this band. However, in 1985, facing pressure to allocate more spectrum to communications, the FCC set up rules for unlicensed operation within this so called “worthless” band [6].

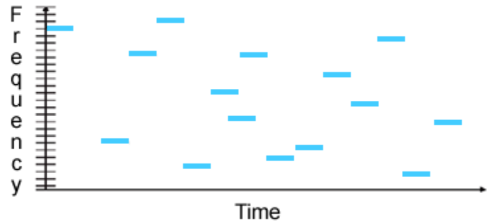

Figure 6. Frequency Hopping Spread Spectrum Channel Utilization.

This *hopping* of the transmitter from channel to channel, as in Figure 6, spreads out the signal energy across a relatively large frequency spectrum in an attempt to minimize the average power seen in any narrow portion of the band. In North America, for example, IEEE 802.11b specifies the use of seventy-nine 1 MHz sub-channels within a 78 MHz wide band located at 2.402-2.480 GHz [18 pg. 129]. Because the FCC insists that any spread spectrum frequency hopping system operating in the ISM band must visit at least 79 of these 1MHz sub-channels at least once every 30 seconds, we can work out a minimum hop rate of 2.63 hops per second or a sub-channel dwell time of at most 0.38 seconds per hop.

In direct sequence spread spectrum (DSSS) communications, the data to be transmitted is mixed (XOR) with a high rate pseudo-random (PN) sequence before being phase shift keying (PSK) modulated onto the RF carrier. This modulation sequence can be many orders of magnitude higher in rate than the underlying data. In the ISM band, it must be at least a 10:1 spreading ratio. This high rate phase modulation spreads the spectrum out while simultaneously reducing the corresponding power spectral density. As a result, a DSSS signal is much less likely to interfere with narrow band users. Additionally, DSSS offers some measure of interference immunity to narrow band emitters.

The processing of DSSS receivers begins with dispreading the signals by mixing the spread signal with the same PN sequence that was used for spreading (upper portion of Figure 7); thereby collapsing the desired signal to its original bandwidth and form while simultaneously spreading all other signals that do not correlate with the spreading signal. The result is that a narrowband noise source (interferer) will get spread in this operation and will not fit through the narrow data filter (middle portion of Figure 7). As the signal energy collapses down to the data bandwidth, its power spectral density increases by the amount of processing gain – which is proportional to the bandwidth reduction. Thus, a signal that was received at or below the noise floor is now elevated above the noise and is therefore easily demodulated.

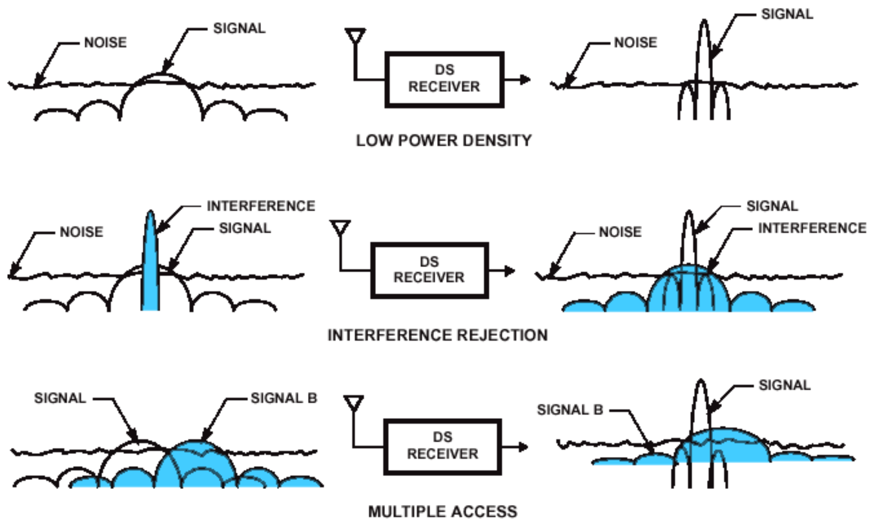

Figure 7. Direct Sequence Spread Spectrum Properties.

Additionally, DSSS modulation techniques can allow more than one user to occupy the same channel through a feature called multiple access. Since each Direct Sequence receiver collapses only correlated signals to the data bandwidth, other, non-correlated signals will remain spread across the spectrum. Therefore, once the desired signal is filtered to the available signal bandwidth, only a small fraction of the undesired signal will remain (bottom portion of Figure 7).

Throughout the world of WLAN literature, the term *packet radio* or *packet communications* is commonly used wherever the communications medium is not well controlled. There are many reasons why a radio communications link may be interrupted; one example is the microwave oven. The microwave oven radiates in the middle of the ISM band with a 50% duty cycle and a pulse rate locked to the power line. Thus, the microwave is “off” for 8ms every 16ms. These off periods allow the transmission of bursts (or packets) of up to 1,000 bytes at a time. Similarly, the nature of FHSS means that the radio communications channel is interrupted at least every 400ms while the sending and receiving radios are retuned to a new frequency. Thus, the breaking up of a large block of data into small “packets” is a common technique in communications that helps insure error-free communications can take place even in the presence of frequent interruptions. Conversely, it is clear that if the medium or channel is corrupted intermittently, a large block of data will never make it through without errors. In the packet technique, this block is broken into small packets that each have some error detection bits added. Then, if an error is detected, a retransmission of the small packet that was corrupted will not unduly burden the network. This packet communications technique employs short control packets that checks to see if the medium is clear and the other end is ready to receive. This short control packet is also used to request a retransmission if a packet did not get through correctly, as in Figure 8 below. Although this level of data integrity comes at the cost of some overhead expense that reduces the net system throughput, packet lengths can be optimized to minimize overhead while ensuring the greatest possible throughput. When continuous data is packetized, the instantaneous rate must increase since the time allowed for data transmission is reduced to allow time for the packet protocol interchange, packet headers and other overhead.

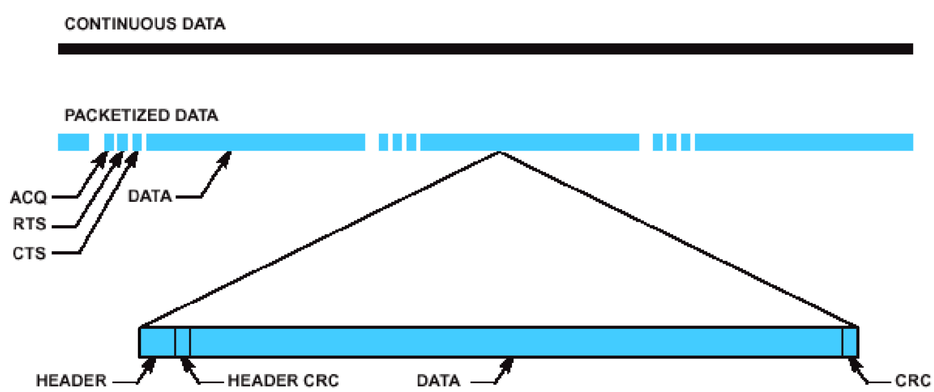

Figure 8. Packet Transmission.

Packet communications can be used with various access protocols such as carrier sense multiple access (CSMA) or time division multiple access (TDMA). CSMA allows asynchronous communications, but requires each communicator to first establish that the medium is not busy. It then establishes the link with an interchange consisting of a Request To Send (RTS), followed by a Clear To Send (CTS), the data packet and acknowledgement or not (ACK/NAK). TDMA allows synchronous communications where each user is allocated a time slot to communicate in. The network overhead in this scheme is in the wasted time when some users have nothing to send and in the packets from the controller necessary to allocate the time slots.

It is in this way that spread spectrum and packet radio communication techniques for 802.11 wireless local area networks are combined to provide robust communications in a crowded and noisy band.

1. Frequency Hopping Spread Spectrum Modulation

Frequency hopping spread spectrum (FHSS) modulation spreads the signal by hopping from narrow band to narrow band within a wide bandwidth, occupying each frequency for only a relatively short duration before hopping to another frequency for another short burst and so on. FHSS wireless LAN stations send one or more data packets at one carrier frequency, the hop to another carrier frequency to send one or more packets, and continue this hop-transmit sequence, called *slow frequency hopping*. The time these FHSS radios dwell on each frequency is fixed. The hopping pattern appears random, but it is actually a periodic sequence tracked by both the sender and receiver. Thus, the source and destination of a transmission must be synchronized so they are on the same frequency at the same time. The hopping pattern (frequencies and order in which they are used) and dwell time (time at each frequency) are restricted by the regulatory agencies of most countries. For example, the FCC requires that 75 or more frequencies be used and a maximum dwell time of 400 ms.

A FHSS transmitter converts the bit stream into a symbol stream in which each symbol represents one or more bits. Two frequencies are applied for binary frequency shift keying modulation, and four frequencies are applied for quaternary FSK modulation. Frequency hopping is applied to the FSK-modulated signal. The transmitter front-end supplies conversion to a higher RF and power amplification. The 802.11 FHSS uses a GFSK modulation technique with a low modulation index which gives a relatively narrow spectrum and allows a higher bit rate in the 1 MHz narrow hop channels. However, these FSK conditions increase the sensitivity to noise and other impairments.

The 802.11 standard defines hops over channel center frequencies according to a periodic sequence that looks like a random pattern within a set of 79 frequencies (e.g., 2.402-2.480 GHz in the U.S. and Europe)[1].

2. Direct Sequence Spread Spectrum Modulation

Direct sequence spread spectrum (DSSS) modulation avoids excessive power concentration by spreading the signal energy across a wider frequency band, thereby increasing the occupied bandwidth. A DSSS transmitter converts a bit stream into a symbol stream in which each symbol represents a number of bits depending on the phase shift keying (PSK) modulation technique. The symbol information is converted into a complex-valued signal that is fed to the spreader. The spreader multiplies its input signal with a pseudo noise (PN) sequence, called a *chip sequence*. This multiplication creates a signal with a wider bandwidth. The in-phase and quadrature components of the spreader output signal are fed to a quadrature modulator. The transmitter front-end provides filtering, conversion to a higher RF, and power amplification.

In Figure 9, each information bit is combined via an XOR function with a longer Pseudo-random Numerical (PN) sequence. The result is a high-speed digital stream, which is then modulated onto a carrier frequency using Differential Phase Shift Keying (DPSK).

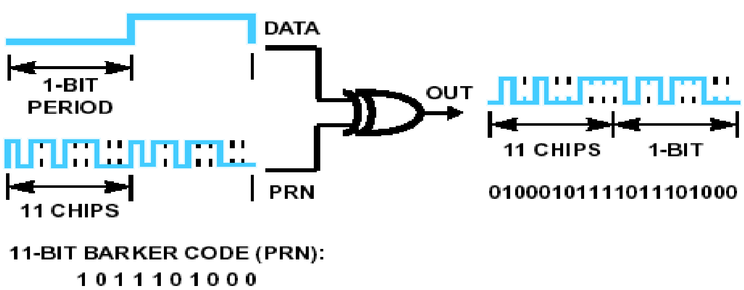

Figure 9. Combining PRN Sequence and Data.

At the destination, the chips are mapped back into a bit, reproducing the original data. In general, the transmitter and receiver should be synchronized to operate properly. The ratio of chips per bit is called the "spreading ratio". A high spreading ratio assures the system is sufficiently resistant to signal noise interference while a low spreading ratio increases the net bandwidth available to a user.

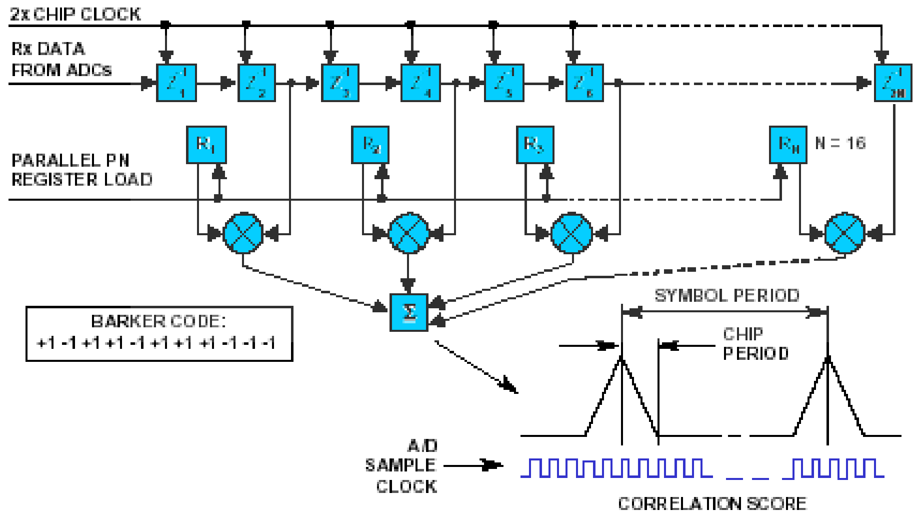

Figure 10. Matched Filter Correlator.

When receiving the DSSS signal, a matched filter correlator is used as shown in Figure 10. The correlator removes the PN sequence and recovers the original data stream. At the higher data rates of 5.5 and 11 Mbps, DSSS receivers employ different PN codes and a bank of correlators to recover the transmitted data stream. The high rate modulation method is called *Complimentary Code Keying (CCK)* and will be discussed in detail later in this chapter. The effects of using PN codes to generate the spread spectrum signal are shown in Figure 11[9].

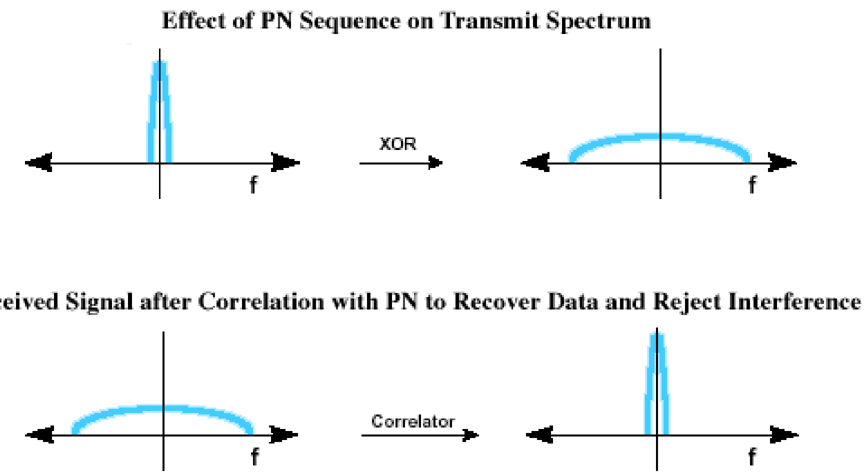

Figure 11. Effect of Spreading and Correlation on DSSS Signals.

As shown in the upper portion of Figure 11, the PN sequence spreads the transmitted bandwidth of the resulting signal (thus the term, "spread spectrum"), thereby reducing the *peak* power while leaving the *total* power unchanged. Upon reception, the signal is correlated with the same PN sequence to reject narrow band interference and recover the original binary data (lower portion of Figure 11). Regardless of whether the data rate is 1, 2, 5.5, or 11 Mbps, the channel bandwidth is 22 MHz for DSSS systems. Therefore, the ISM band will accommodate up to three non-overlapping channels as illustrated in Figure 12 below.

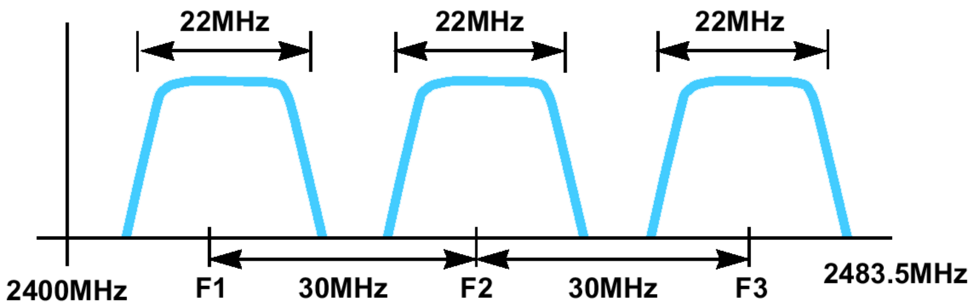

Figure 12. Non-Overlapping Channels in the ISM Band.

The 802.11 DSSS, based on the 11-chip Barker sequence +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1, is used as the PN code sequence, and the symbol duration corresponds to the time of 11 chip intervals. The 11-chip spreading makes the occupied bandwidth larger and increases the effective bandwidth from 1 MHz to 11 MHz. The 802.11 standard specifies two bit rates – 1 Mbps with BPSK and 2 Mbps with QPSK, with a spectrum that looks the same for both bit rates.

DSSS has a more robust modulation and a larger coverage range that FHSS, even when FHSS uses twice the transmitter power output level. FHSS gives a large number of hop frequencies, but the adjacent channel interference behavior limits the number of independently operating collocated systems. Hop time and a smaller packet size introduce more transmission time overhead into FHSS, which affects the maximum throughput. Although FHSS is less robust, it gives a more graceful degradation in throughput and connectivity. Under poor channel and interference conditions, FHSS will continue to work over a few hop channels a little longer than over the other hop channels. DSSS, however, still gives reliable links for a distance at which very few FHSS hop channels still work. For collocated networks (access points), DSSS yields a higher potential throughput with fewer access points and a corresponding reduction in infrastructure costs versus FHSS.

Several DSSS products in the market allow users to deploy more than one channel in the same area. They accomplish this by separating the 2.4-GHz band into multiple sub-bands, each of which contains an independent DSSS network. Because DSSS modulation truly spreads a signal across the spectrum, the number of independent, non-overlapping channels in the 2.4-GHz band is small, as illustrated by Figure 13. Only a very limited number of co-located networks can therefore operate without interference from adjacent channels.

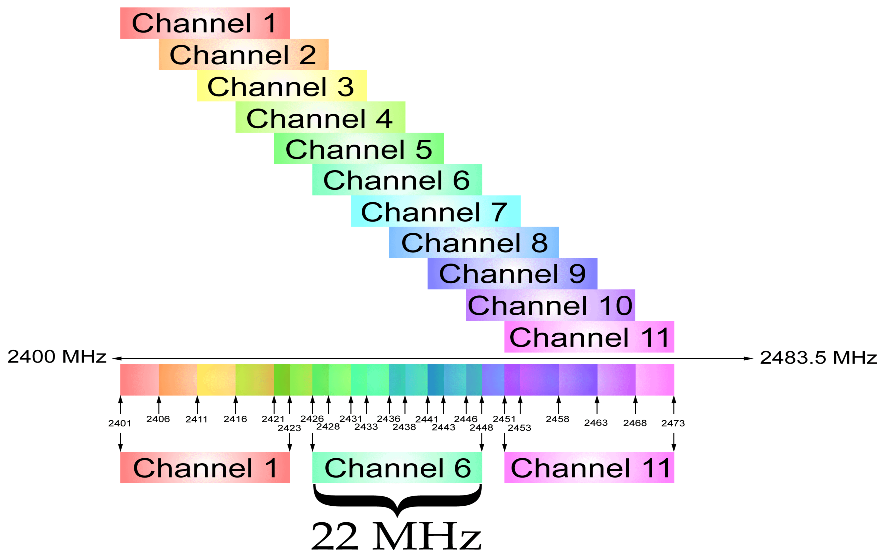

Figure 13. Non-Overlapping Channels in the ISM Band.

Regulations under which radio spectrum may be used and frequencies in which wireless LANs can be deployed have made the 2.4-GHz ISM band available worldwide but without a unified regulation for spectrum occupation or power levels. The regional variations across the fourteen center frequency channels allocated for 802.11 DSSS are listed in the Table 3.

Channel ID	Frequency (MHz)	FCC (USA)	IC (Canada)	ETSI (Europe)	Spain	France	MKK (Japan)
1	2412	√	√	√			√
2	2417	√	√	√			√
3	2422	√	√	√			√
4	2427	√	√	√			√
5	2432	√	√	√			√
6	2437	√	√	√			√
7	2442	√	√	√			√
8	2447	√	√	√			√
9	2452	√	√	√			√
10	2457	√	√	√	√	√	√
11	2462	√	√	√	√	√	√
12	2467			√		√	√
13	2472			√		√	√
14	2484						√

Table 3. Non-Overlapping Channels in the ISM Band [1].

3. Multiple Access

The basic access method for 802.11 is the Distributed Coordination Function (DCF), which uses Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). In CSMA/CA, each station is required to listen for other users. If the channel is idle, the station may transmit. However if it is busy, each station waits until transmission stops, and then enters into a random back off procedure. This procedure prevents multiple stations from seizing the medium immediately after completion of the preceding transmission.

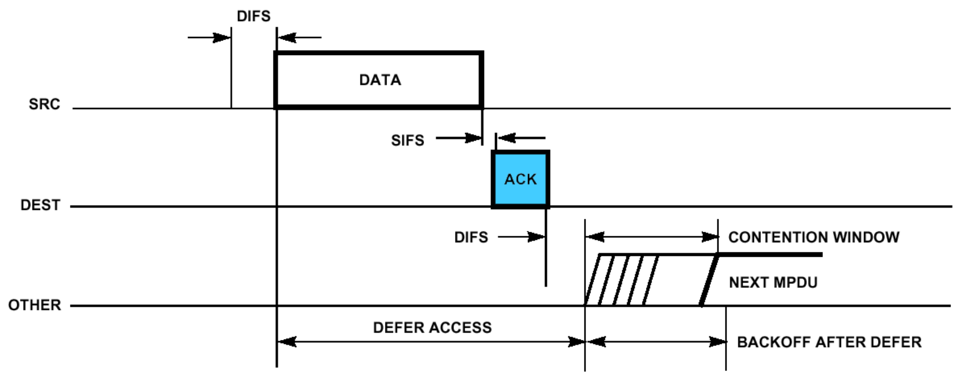

Figure 14. Distributed Coordination Function Acknowledgement.

Packet reception in DCF requires acknowledgement as shown in Figure 14. The period of time between completion of packet transmission and start of the ACK frame is one Short Inter Frame Space (SIFS). ACK frames have a higher priority than other traffic. Fast acknowledgement is one of the salient features of the 802.11 standard, because it requires ACKs to be handled at the MAC sublayer.

Transmissions other than ACKs must wait at least one DCF Inter Frame Space (DIFS) before transmitting data. If a transmitter senses a busy medium, it determines a random back-off period by setting an internal timer to an integer number of slot times. Upon expiration of a DIFS, the timer begins to decrement. If the timer reaches zero, the station may begin transmission. However, if the channel is seized by another station before the timer reaches zero, the timer setting is retained at the decremented value for subsequent transmission.

The method described above relies on the *Physical Carrier Sense*. The underlying assumption is that every station can “hear” all other stations. This is not always the case. Referring to the Figure 15, Station A is within range of the AP, but out of range of Stations B, C and D. Because Station B, C and D would not be able to detect transmissions from Station A, the probability of collision is greatly increased. This is known as the *Hidden Node* problem and Stations B, C and D are known as *hidden nodes*.

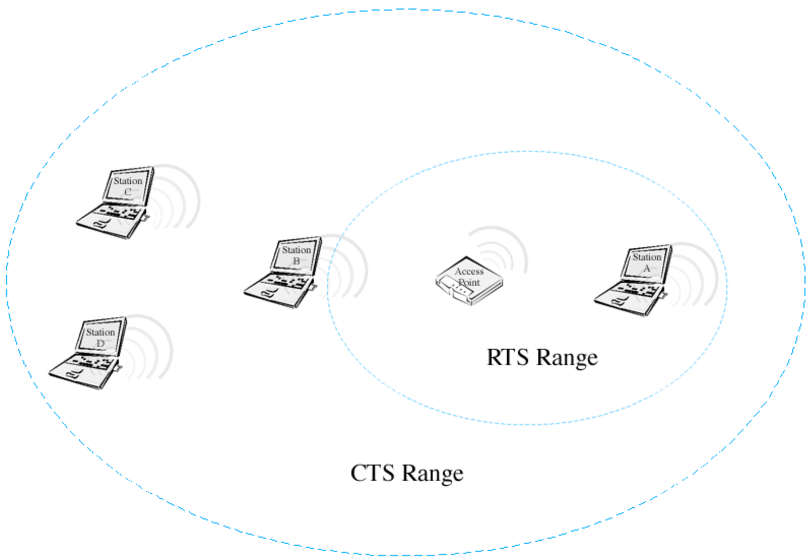

Figure 15. RTS and CTS Ranges.

To combat this problem, a second carrier sense mechanism is available. *Virtual Carrier Sense* enables a station to reserve the medium for a specified period of time through the use of RTS/CTS frames. In the previously described scenario, Station A sends an RTS frame to the AP, but this RTS will not be heard by Stations B, C or D. The RTS frame contains a duration/ID field which specifies the period of time for which the medium is reserved for a subsequent transmission by Station A. The reservation information is stored in the Network Allocation Vector (NAV) of all stations detecting the RTS frame.

Upon receipt of the RTS, the AP responds with a CTS frame, which also contains a duration/ID field specifying the period of time for which the medium is reserved. While Stations B, C and D did not detect the RTS, they will detect the CTS and update their NAVs accordingly. Thus, collision is avoided even though some nodes are hidden from other stations. The RTS/CTS procedure is invoked according to a user specified parameter. It can be used always, never, or for packets which exceed an arbitrarily defined length.

As mentioned above, DCF is the basic media access control method for 802.11 and it is mandatory for all stations. The Point Coordination Function (PCF) is an optional extension to DCF which provides a time division duplexing capability to accommodate time bounded, connection-oriented services such as cordless telephony [2].

4. Logical Addressing

The authors of the 802.11 standard allowed for the possibility that the wireless media, distribution system, and wired LAN infrastructure would all use different address spaces. IEEE 802.11 only specifies addressing over the wireless medium, though it was intended specifically to facilitate integration with IEEE 802.3 wired Ethernet LANs. IEEE802 48-bit addressing scheme was therefore adopted for 802.11 in order to maintain address compatibility with the entire family of IEEE 802 standards. In the vast majority of installations, the distribution system is an IEEE 802 wired LAN and all three logical addressing spaces are identical.

5. Security

IEEE 802.11 provides for security in two ways: *authentication* and *encryption*. Authentication is the means by which one station is verified to have the authority to communicate with a second station in a given coverage area. In the infrastructure mode, authentication is established between an AP and each station.

Authentication can be either *Open System* or *Shared Key*. In an Open System, any station (STA) may request authentication. The STA receiving the request may grant authentication to any request, or only those from stations on a user-defined list. In a Shared Key system, only stations which possess a secret encrypted key can be authenticated. Shared Key authentication is only available to systems having the optional encryption capability enabled.

Encryption is intended to provide a level of security comparable to that of a wired LAN. The Wired Equivalent Privacy (WEP) feature uses the RC4 PRNG algorithm from RSA Data Security, Inc. The WEP algorithm was selection criteria were that it be reasonably strong, self-synchronizing, computationally efficient, exportable and optional.

6. Timing and Power Management

All station clocks within a Basic Service Set (BSS) are synchronized by periodic transmission of time stamped beacons. In the infrastructure mode, the AP serves as the timing master and generates all timing beacons. Synchronization is maintained to within 4 microseconds plus propagation delay.

Timing beacons also play an important role in power management. There are two power saving modes defined: *awake* and *doze*. In the *awake* mode, stations are fully powered and can receive packets at any time. Nodes must inform the AP before entering doze. In this mode, nodes must "wake up" periodically to listen for beacons which indicate that the AP has queued messages waiting for it.

7. Roaming

Roaming may be the least defined feature among those defined by the standard. The standard identifies the basic message formats required to support roaming, but everything else is left up to network vendors. In order to fill the void, the Inter-Access Point Protocol (IAPP) was jointly developed by Aironet, Lucent Technologies, and Digital Ocean. Among other things, IAPP extends multi-vendor interoperability to the roaming function and addresses roaming within a single Extended Service Set (ESS) and between two or more ESSs.

E. 802.11B HIGHER-SPEED PHYSICAL LAYER EXTENSION

Soon after the IEEE 802.11 standards board approved the 1 and 2 Mbps standard for wireless local area networks in 1997, a working group started on a higher rate extension to the physical layer of the standard with the intent to deliver Ethernet like speeds over 802.11 WLAN systems. After months of evaluating various modulation proposals such as m-ary orthogonal keying (MOK), pulse position modulation (PPM), packet binary convolutional coding (PBCC), orthogonal frequency division multiplex (OFDM) and orthogonal code division multiplex (OCDM), the working group could not come to consensus on a single modulation method [7].

As a result, Harris Semiconductor and Lucent Technologies joined forces and developed an approach called complementary code keying (CCK) which was subsequently adopted by the 802.11 working group in July 1998 as the basis for the high rate physical layer extension to deliver data rates of 5.5 and 11 Mbps at 2.4 GHz. This higher rate extension was adopted primarily because the MAC is kept unchanged, ensuring an easy path for interoperability with the existing 1 and 2-Mbps networks by maintaining the same bandwidth and incorporating the same preamble and header [8].

Thus, the IEEE 802.11 High Rate PHY today specifies four modulation formats and data rates. Both the basic access rate of 1 Mbps and the enhanced access rate of 2 Mbps use DBPSK modulation while the two high rate access rates of 5.5 Mbps and 11 Mbps use CCK modulation. In addition, an optional packet binary convolutional coding (PBCC) mode is also provided for potentially enhanced performance.

To transmit at 5.5 Mbps and 11 Mbps in the 2.4-GHz band, a new modulation scheme was defined, based on the DSSS PHY standard. In the original PHY, a chip rate of 11 Mcps/s was selected, with a symbol rate of 1 Msps. The data rates of 1 and 2 Mbps are obtained through the use of BPSK and QPSK. The chip rate is maintained in the extension to higher data rates, as is the QPSK modulation. Accordingly, much of the hardware and the channel structure are compatible with the lower data rates. However, the original DSSS modulation is no longer useful, as the chip rate is equal to or double the bit rate. The process gain would be 1 or 2. Instead, a modulation format called complementary code keying (CCK) is used [8].

1. Complementary Code Keying

CCK is a variation on *m*-ary orthogonal keying modulation that uses an I/Q modulation architecture with complex symbol structures. Because CCK is based on the complementary codes, it has good performance with regard to mutual interference and allows for multi-channel operation in the 2.4-GHz ISM band through use of the existing 802.11 1 and 2 Mbps DSSS channelization scheme. The spreading employs the same chipping rate and spectrum shape as the 802.11 Barker word spreading functions, allowing for three non-interfering channels in the 2.4 to 2.483-GHz band [8].

In CCK *m*-ary orthogonal keying modulation, one of *m* unique (nearly orthogonal) signal codewords is chosen for transmission. Figure 16 shows the spreading function for CCK is chosen from a set of *m* nearly orthogonal vectors by the data word. To transmit 11 Mbps, CCK chooses one vector from a set of 64 complex (QPSK) vectors for the symbol and thereby modulates 6-bits (one-of-64) on each 8 chip spreading code symbol. Two more bits are sent by QPSK modulating the whole code symbol, thereby modulating 8-bits onto each symbol. Thus, a group of eight chips (each transmitted with one of the QPSK phases) jointly codes eight bits. Two of the bits are coded in the average phase rotation of the eight chips, and the other six bits in the selection of one out of four complementary codes. These four bits form a subset among the 64 bits used for 11 Mbps [7].

$$c = \{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1}\} \quad (3.1)$$

The equation (3.1) above is used to derive the CCK codewords used for spreading in both 5.5 Mbps and 11 Mbps data rates, where C is the codeword {c0..c7}. This formula creates 8 complex chips (c0 to c7) where c0 is transmitted first in time and the terms ϕ_1, ϕ_2, ϕ_3 and ϕ_4 are the four phase terms. The phase term ϕ_1 modulates all of the code chips of the sequence and is used for the DQPSK rotation of the whole code vector. The three others modulate every odd chip, every odd pair of chips and every odd quad of chips respectively. Chip c7 of the symbol defined above is the chip that indicates the symbol's phase and is transmitted last [2].

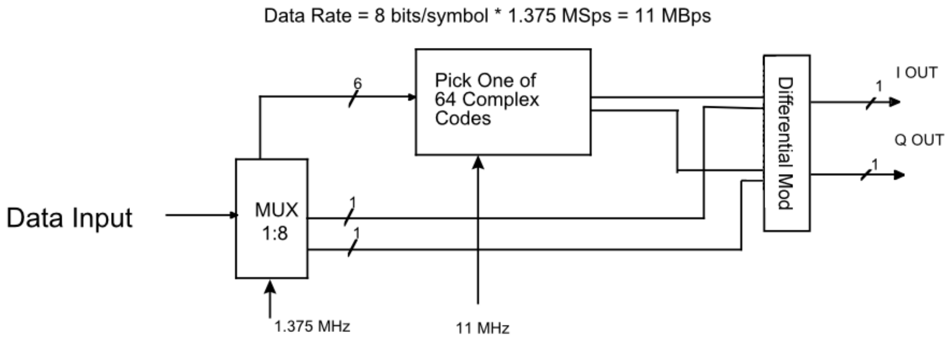

Figure 16. Complementary Code Keying Modulation.

Walsh functions were used for the *m*-ary bi-orthogonal keying (MBOK) modulation first considered by the 802.11b working group. They are the most well known orthogonal BPSK vector set and are available in 8 chip (powers of 2) vectors. To transmit enough bits per symbol, the MBOK modulation was used independently on the I and Q channels of the waveform, effectively doubling the data rate. CCK, on-the-other-hand, uses a complex set of Walsh/Hadamard functions known as complementary codes. Walsh/Hadamard properties are similar to Walsh functions but are complex; thus they have more than two phases while still being nearly orthogonal. With complex code symbols, we cannot independently transmit simultaneous code symbols without suffering amplitude modulation. However, since the set of complementary codes is more extensive, we have a larger set of nearly orthogonal codes to pick from and can get the same number of bits transmitted per symbol without simultaneous transmission of symbols. Additionally, the multipath performance of CCK is better than MBOK due to the lack of cross rail interference [7].

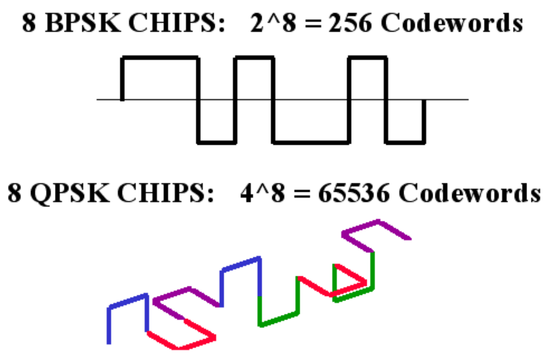

Figure 17. Walsh and Complementary Codes.

Figure 17, compares the modulation schemes. For MBOK, there are 8 BPSK chips that have a maximum vector space of 256 code words in which orthogonal sets of 8 can be found. Two independent BPSK vector sets are selected for the orthogonal I and Q channels which modulate 3-bits on each. Two additional bits are used to BPSK modulate each of the spreading code vectors. For CCK, there are 65,536 possible code words, and sets of 64 that are nearly orthogonal. This is because it really takes 16 bits to define each code vector. To get a half data rate version, a subset of 4 of the 64 vectors having superior coding distance is used [7].

One advantage of CCK over MBOK is that it suffers less from multipath distortion in the form of cross coupling of I and Q channel information. The information in CCK is encoded directly onto complex chips. These chips cannot be cross-couple corrupted by multipath since each channel finger has an $Ae^{j\theta}$ distortion. Thus, a single channel path gain-scales and phase-rotates the signal while a gain scale and phase rotation of a complex chip still maintains I/Q orthogonality. This superior encoding technique avoids corruption that results from encoding half the information on the I-channel and the other half on the Q-channel, as in MBOK, which easily cross-couple corrupts with multipath's $Ae^{j\theta}$ phase rotation [7].

Figure 18, shows a composite view of the CCK modulation modes and the original 1 and 2-Mbps modes. For 1 Mbps, the signal is modulated BPSK by one bit per symbol and then spread by BPSK modulating with the 11 chip Barker code at 11 Mchip/s. For 2 Mbps, the signal is QPSK modulated by two bits per symbol and then BPSK spread as before. For the 5.5-Mbps CCK mode, the incoming data is grouped into 4 bit nibbles where 2 of those bits select the spreading function out of the set of 4 while the remaining 2 bits QPSK modulate the symbol. The spreading sequence then DQPSK modulates the carrier by driving the I and Q modulators. To make 11-Mbps CCK modulation, the input data is grouped into 2 bits and 6 bits. The 6 bits are used to select one of 64 complex vectors of 8 chips in length for the symbol and the other 2 bits DQPSK modulate the entire symbol. The chipping rate is maintained at 11 Mcps for all modes.

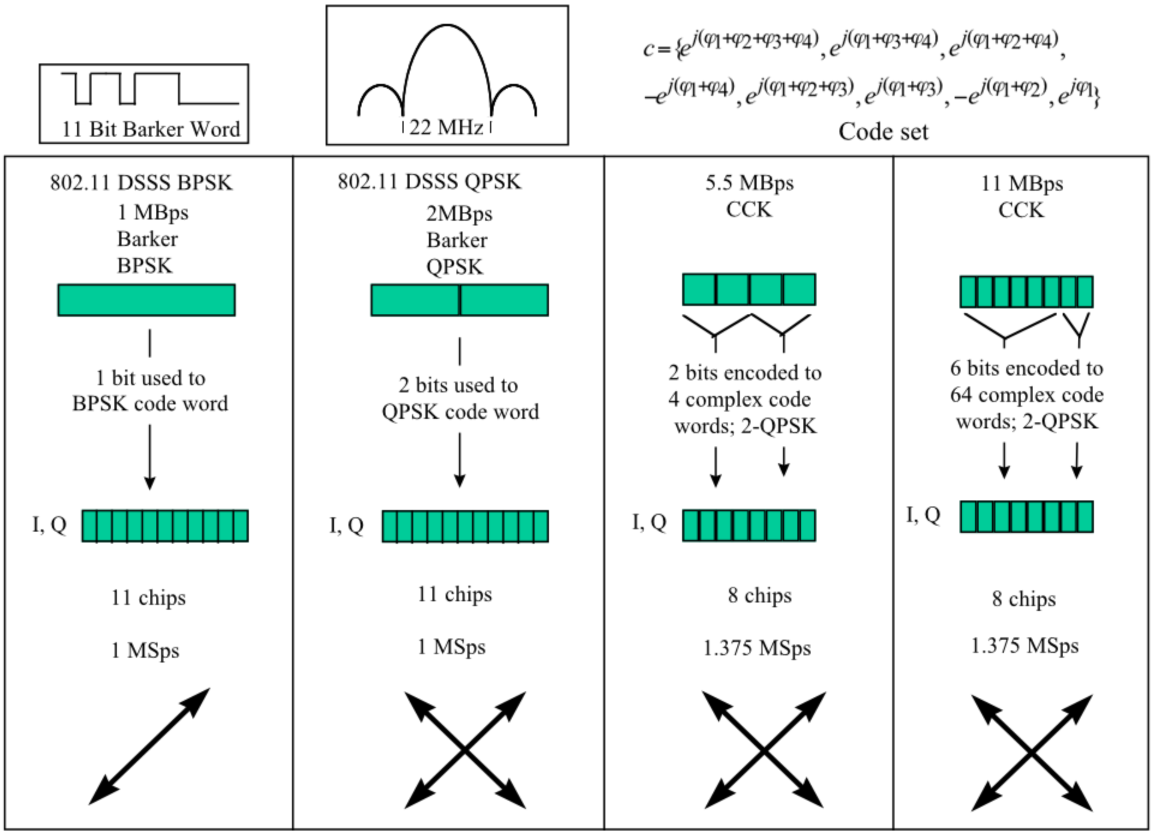

Figure 18. CCK Modulation Modes.

2. 802.11 Interoperability

Interoperability was a priority for the 802.11 working group in the selection of the waveform for higher rates. The signal acquisition scheme for 802.11 uses a specific preamble and header for the 1-Mbps modulation and a provision for sending the payload at different rates. Although the packet frame structure and protocol of 802.11 is very similar to 802.3 Ethernet, 802.11 must operate wirelessly in a harsh RF environment. This means that the signal levels may become corrupted and subject to multipath. Consequently, signal acquisition and synchronization of the preamble and header are critical. The preamble and header consists of six fields: preamble, SFD, Signal (rate), Service, Length and CRC. The header requires 48 bits and the total length of the acquisition sequence is 192 µs. The preamble and header is modulated using the 1-Mbps modulation rate and is scrambled with a self-synchronizing scrambler. The high rate scheme re-uses the previous acquisition sequence as it already had a rate field that could be programmed for 1, 2, 5.5 or 11 Mbps. Additionally, the high rate 802.11 standard has a provision for an optional shorter acquisition sequence that yields a lower packet overhead when only high rate capable equipment is present within the network.

The 802.11 packet transmission protocol is carrier sense multiple access with collision avoidance (CSMA/CA). The deviation from the "wired" Ethernet carrier sense multiple access with collision detection (CSMA/CD) scheme was necessary because radios can not detect collisions. They therefore use collision avoidance, which is essentially a listen-before-talk and random-back-off deferral mechanism. Since all stations use the same acquisition sequence at the lowest basic rate, all stations can see the traffic and process the signals at the appropriate rate. If legacy 1 and 2 Mbps stations receive the packet header, but are not capable of processing the higher rate, they can still defer the medium as they know that an 802.11 signal was sensed and they know the length of time it will be on the air [4].

To insure that the modulation has the same bandwidth as the existing 802.11 DSSS modulation, the chipping rate is kept at 11 Mchip/s while the symbol rate is increased to 1.375 Msymbols/s in order to account for the shorter symbols and make the overall bit rate 11 Mbps. This approach makes system interoperability with the 802.11 preamble and header much simpler. Because the spreading rate remains constant and only the data rate changes, the spectrum of the CCK waveform is the same as the legacy 802.11 waveform [7].

3. Walsh and Complementary Codes

Walsh codes are formed throught the simple operation illustrated in Figure 19. For the 2-ary case, the basic symbols are formed by taking a 2x2 matrix of 1s and inverting the lower right quadrant of the matrix. The 4-ary case is formed by taking four of the 2x2 matrices and making a 4x4 matrix with the lower right hand quadrant again inverted. The procedure can be repeated for the 8-ary case and beyond.

11	
10	

2

11	11
10	10
11	00
10	01

4

11	11	11	11
10	10	10	10
11	00	11	00
10	01	10	01
11	11	00	00
10	10	01	01
11	00	00	11
10	01	01	10

8

Figure 19. Walsh Codes.

Walsh functions have a regular structure and at least one member that has a substantial DC bias (the first row with all 1s). All other members are composed of half 1s and half 0s. The DC bias can be reduced on the worst member of the set by multiplying all members with a cover code. However, doing so introduces a (smaller) bias in half of the members.

The main concern about MBOK is due to the fact that it uses independent codes on the in-phase and quadrature signals, which creates a significant amount of cross-rail interference in the presence of multipath. To avoid this, one would ideally transmit only symbols for which processing could be done on I and Q simultaneously, and use code words that all have good autocorrelation properties, such that there is minimal inter-symbol and inter-chip interference. Such codes actually exist in the form of the complementary codes. For an 8-chip code length, 256 possible sequences *c* can be constructed using four QPSK phases $\varphi 1$ through $\varphi 4$.

Because $\varphi 1$ is present in all 8 chips, it simply rotates the entire code word. To decode this code set, one needs 64 correlators plus an additional phase detection of the code that gave the largest correlation output. The correlation can be significantly simplified by using techniques like the Fast Walsh transform (analogous to an FFT butterfly circuit). In fact, when the four input phases $\varphi 1$ to $\varphi 4$ are binary, then the complementary code set reduces to a modified Walsh code set.

4. Performance Parameters

The FCC requires that DSSS modulations used in the 2.4-GHz ISM band have a minimum processing gain of 10 dB. Spreading and de-spreading operations using CCK provides 11 dB of processing gain when used in accordance with the FCC rules. The reduction in bandwidth provides 9 dB and MOK coding constitutes 2 dB of coding gain. After de-spreading, the SNR improves by 11 dB over the SNR in the spread bandwidth. Under these conditions radios designed with CCK modulation satisfy the FCC's requirements with ample margin for the CW jamming test.

Antenna diversity helps insure a reliable 11-Mbps link for indoor environments. High rate modulation schemes are always more susceptible to multipath interference and filter distortion than lower rate modulations due to the higher required SNR (E_s/N_0) [10].

A CCK transmitter is very similar to an IEEE 802.11 DSSS transmitter, as the only changes are in the way the chip phases are chosen. This is typically done in the digital signal processing (DSP) part of the hardware. Therefore, a software actualization may be enough. At the receiver side, things are different, as the longer bit period of the DS receiver allows the implementation of 1 and 2-Mbps receivers with the RAKE technique. The multipath delay spread is much lower than the symbol rate. In the 5.5 Mbps and 11 Mbps version, some kind of equalization must be used, in combination with the RAKE receiver. For high multipath environments, such as factory and manufacturing plants, a CCK demodulator using a RAKE receiver can tolerate delay spreads of 100nsec and >100nsec when combined with a decision feedback equalizer (DFE) [8].

F. SUMMARY

This chapter provided an overview of the IEEE 802.11 Wireless LAN Standard and the underlying mechanisms of the Higher-Speed Physical Layer Extension that are relevant to this thesis. We highlighted the key communications concepts and techniques necessary for subsequent discussions regarding the implementation details of the wireless testbed. The next chapter introduces the system specifics, architecture and background information necessary for a thorough examination of the performance of the wireless metropolitan area network testbed.

IV. WIRELESS MAN TESTBED COMPONENTS

A. INTRODUCTION

This chapter discusses the major wired and wireless networking components and configurations used during this study within the framework of the Advanced Networking Laboratory Wireless MAN testbed.

B. WIRELESS MAN TESTBED COMPONENTS

The wireless MAN testbed made use of the highest quality WLAN components available. Product purchase decisions were driven primarily by a desire to maximize multi-vendor compatibility with user cards while ensuring the highest possible level of 802.11b feature maturity in order to assure maximum utility and security.

The testbed was composed entirely of Central and Remote Outdoor Routers, Outdoor Router Clients (wireless cards) and Outdoor Antennas/Amplifier assemblies interconnected by various cables and connectors and configured by associated router and client management software. All Outdoor Routers (CORs and RORs) and wireless PCMCIA cards were Lucent ORiNOCO® products. All outdoor antennas, amplifiers, splitters, cables and assemblies are HyperLink Technologies Inc. products.

C. KEY COMPONENT DESCRIPTIONS

Outdoor Routers are actually bridge/routers and can function as IP routers while performing transparent Ethernet bridging of all standard Ethernet protocols. In addition to the (wired) Ethernet interface, Outdoor Routers can support up to two wireless interfaces, providing the following major modes of operation for high-speed outdoor wireless links, including wireless broadband Internet access:

- Central Outdoor Router
- Remote Outdoor Router
- IEEE 802.11b Access Point

1. Central Outdoor Router

A Central Outdoor Router (COR) depicted in Figure 20 is an Outdoor Router or wireless base station that provides high-speed wireless network access to two or more clients. The COR manages usage of the wireless network, and can provide access to many Remote Outdoor Routers and Outdoor Router Clients simultaneously.

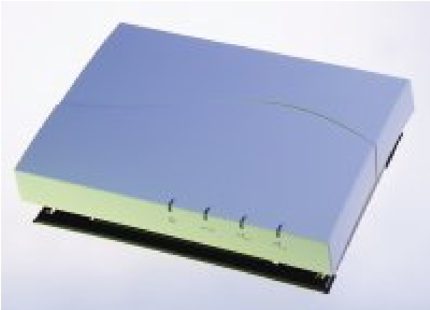

Figure 20. Photo of ORiNOCO® Central Outdoor Router (Model COR-1100).

2. Remote Outdoor Router

A Remote Outdoor Router (ROR) depicted in Figure 21 is an Outdoor Router or wireless satellite unit capable of connecting wired LAN's to the wireless network. A Remote Outdoor Router can connect to either one Central Outdoor Router or one other Remote Outdoor Router.

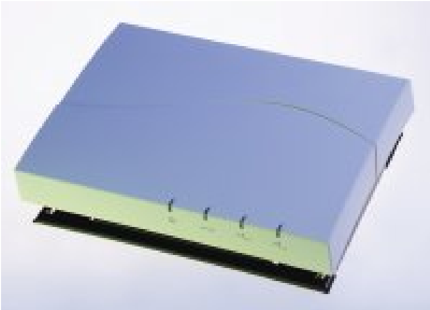

Figure 21. Photo of ORiNOCO® Remote Outdoor Router (Model ROR-1000).

3. Outdoor Router Client

An Outdoor Router Client (ORC) is an end-user laptop or desktop computer which connects directly to the Outdoor Router network using a wireless PC Card (Figure 22) running the OR Client driver. With the OR Client driver, a network administrator can limit the end user's bandwidth usage by using the Data Rate throttle setting.

Figure 22. Photo of ORiNOCO® Gold PC Card.

4. IEEE 802.11 Compatible 2.4 GHz WLAN Amplifiers

For the wireless testbed configurations that required wireless links with additional link margin, a combination of Outdoor Antennas and their associated amplifiers was used. These wireless testbed configurations employed an IEEE 802.11 compatible 2.4-GHz wireless LAN amplifier to deliver up to 1 Watt of transmit power for as little as 5mW of input power. The WLAN Amplifier and its associated DC Power Injector, illustrated in Figure 23 and described in Table 4, were used exclusively throughout the tests.

Figure 23. Photo of HyperLink Technologies® WLAN Amplifier & DC Injector (Model HA2401).

Frequency Range	2400 – 2483 MHz
Receive Gain	20 dB
Receive Noise Figure	2.5 dB nominal
Transmit Gain	30 dB maximum
Transmit Power	1 Watt
Frequency Response	± 1 dB over operating range
Impedance	50 Ohms (Input & Output)
Weight	< 0.3 Lbs (each)
Dimensions	4.6” x 2.6” x 1.7” (both)
Cable Pigtail	59” RG8

Table 4. Specifications of HyperLink Technologies® WLAN Amplifier & DC Injector (Model HA2401).

5. Indoor and Outdoor Antennas

Each of the wireless testbed configurations included a laptop computer configured with an ORiNOCO® wireless PC Card and an AP attached to one or more of the Indoor or Outdoor Antennas illustrated in Figures 24 through 31 and described in Tables 5 through 12.

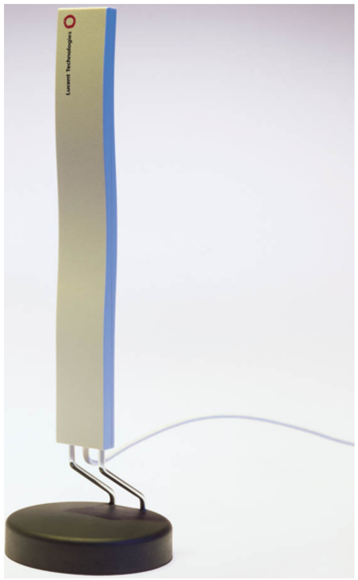

Figure 24. Photo of ORiNOCO® Range Extender Indoor Antenna.

The Range Extender Indoor Antenna, depicted in Figure 24 and described in Table 5, was used to boost the signal provided to the survey laptop computer in order to quickly determine signal power levels and connection quality while roaming within the metropolitan area. The primary advantage of this antenna is that it produces a significant improvement in signal quality in both indoor and outdoor environments without the need for an additional amplifier and comes wired with a proprietary Lucent connector to plug directly into the external antenna port on all Lucent IEEE 802.11b PC cards.

Frequency Range	2400 – 2500 MHz
Gain	2.5 dBi
Impedance	50 Ohms
Weight	0.3 Lbs
Dimensions	9” height x 1” wide x 3” base
Cable Pigtail	59” RG8

Table 5. Specifications of ORiNOCO® Range Extender Indoor Antenna.

Figure 25. Photo of HyperLink Technologies® 8 dBi Mini-Patch Indoor Antenna (Model HG2408P).

Frequency Range	2400 – 2500 MHz
Gain	8 dBi
-3 dBi Horizontal Beam Width	75º
-3 dBi Vertical Beam Width	65º
Impedance	50 Ohms
VSWR	< 2:1, 1.5:1 nominal
Polarization	Horizontal & Vertical
Wind Survival	>100 MPH
Weight	< 0.5 Lbs
Dimensions	4.2” diameter x 1.2” deep
Cable Pigtail	12” RG8

Table 6. Specifications of HyperLink Technologies® 8 dBi Mini-Patch Indoor Antenna (Model HG2408P).

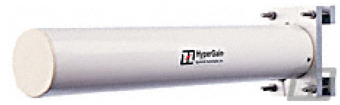

Figure 26. Photo of HyperLink Technologies® Radome Enclosed Yagi Antenna (Model HG2415Y).

The Radome Enclosed Yagi Antenna, depicted in Figure 26 and described in Table 7, proved to be the most convenient for use in the survey due to its light weight and good combination of gain and beam width that allowed for ease in setup.

Frequency Range	2400 – 2500 MHz
Gain	14 dBi
-3 dBi Horizontal Beam Width	30º
Impedance	50 Ohms
Max. Input Power	50 Watts
VSWR	< 2:1, 1.5:1 nominal
Polarization	Vertical
Wind Survival	>150 MPH
Weight	1.8 Lbs
Dimensions	19” length x 3” diameter
Cable Pigtail	24” RG8

Table 7. Specifications of HyperLink Technologies® Radome Enclosed Yagi Antenna (Model HG2415Y).

Figure 27. Photo of HyperLink Technologies® 15 dBi Omni Outdoor Antenna (Model HG2415U).

The Omni Outdoor Antenna, depicted in Figure 27 and described in Table 8, proved to be the most convenient antenna for use with the AP in that it provided good signal coverage throughout most of the metropolitan area, eliminating the need for beam re-direction.

Frequency Range	2400 – 2500 MHz
Gain	15 dBi
Max. Input Power	100 Watts
VSWR	< 1.5:1 nominal
Polarization	Vertical
Wind Survival	>150 MPH
Weight	2.5 Lbs
Dimensions	70” length

Table 8. Specifications of HyperLink Technologies® 15 dBi Omni Outdoor Antenna (Model HG2415U).

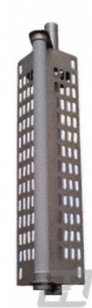

Figure 28. Photo of HyperLink Technologies® Panel Outdoor Antenna (Model HG2415P).

The 180º Panel Outdoor Antenna, depicted in Figure 28 and described in Table 9, provided excellent coverage throughout the La Mesa housing area. Two antennas mounted at the top of our 80 foot mast were sufficient to provide 360º coverage as highlighted in blue in the left panel of Figure 34.

Frequency Range	2400 – 2500 MHz
Gain	15 dBi
-3 dBi Horizontal Beam Width	180º
-3 dBi Vertical Beam Width	± 10º
Impedance	50 Ohms
Max. Input Power	300 Watts
VSWR	< 1.5:1 average
Polarization	Vertical
Wind Survival	> 150 MPH
Weight	14 Lbs
Panel Dimensions	32” x 9” x 2”

Table 9. Specifications of HyperLink Technologies® Panel Outdoor Antenna (Model HG2415P).

Figure 29. Photo of HyperLink Technologies® Panel Outdoor Antenna (Model HG2417P).

The 90º Panel Outdoor Antenna, depicted in Figure 29 and described in Table 10, provided good coverage within a sector of the metropolitan area. Although not as convenient as the omni-directional antenna described above, this antenna extended the signal coverage to the hills and valleys of the metropolitan area.

Frequency Range	2400 – 2500 MHz
Gain	17.2 dBi
-3 dBi Horizontal Beam Width	90º
-3 dBi Vertical Beam Width	± 7.5º
Impedance	50 Ohms
Max. Input Power	250 Watts
VSWR	< 1.3:1 average
Polarization	Vertical
Wind Survival	> 150 MPH
Weight	15 Lbs
Panel Dimensions	32” x 12” x 2”

Table 10. Specifications of HyperLink Technologies® Panel Outdoor Antenna (Model HG2417P).

Figure 30. Photo of HyperLink Technologies® Panel Outdoor Antenna (Model HG2420P).

The 90º Panel Outdoor Antenna, depicted in Figure 30 and described in Table 11, also provided excellent coverage within a sector of the metropolitan area. Similar to Figure 29, this antenna is not as convenient as the omni-directional antenna described above. This antenna may extend signal coverage across the bay as well as to the hills and valleys of the metropolitan area.

Frequency Range	2400 – 2500 MHz
Gain	19.2 dBi
-3 dBi Horizontal Beam Width	90º
-3 dBi Vertical Beam Width	± 6.5º
Max. Input Power	250 Watts
VSWR	< 1.3:1 average
Polarization	Vertical
Wind Survival	> 150 MPH
Weight	24 Lbs
Panel Dimensions	32” x 12” x 2”
Cable Pigtail	NONE

Table 11. Specifications of HyperLink Technologies® Panel Outdoor Antenna (Model HG2420P).

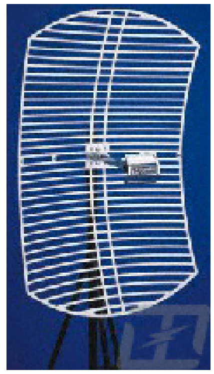

Figure 31. Photo of HyperLink Technologies® Parabolic Grid Outdoor Antenna (Model HG2424G).

The 8º Parabolic Grid Outdoor Antenna, depicted in Figure 31 and described in Table 12, proved to be almost perfectly suited for use in point-to-point applications such as between the COR and the Remote LANs located at the La Mesa Housing Area. The light-weight design of this antenna combined with its very tight beam width, however, cause link quality to vary considerably during high wind or rain conditions as it is very difficult to stabilize the grid sufficiently.

Frequency Range	2400 – 2500 MHz
Gain	24 dBi
-3 dBi Horizontal Beam Width	8º
-3 dBi Vertical Beam Width	± 5º
VSWR	< 1.5:1 average
Wind Survival	> 150 MPH
Weight	4.8 Lbs
Grid Dimensions	39.5” x 23.5”
Cable Pigtail	24” RG8

Table 12. Specifications of HyperLink Technologies® Parabolic Grid Outdoor Antenna (Model HG2424G).

5. IEEE 802.11b Access Point

An IEEE 802.11b Access Point is a mode of operation for the Outdoor Router in which a particular wireless interface services standard IEEE 802.11b clients. It is recommended that the Outdoor Router be setup to provide IEEE 802.11b services only in indoor environments with no hidden nodes.

6. OR Manager

The Outdoor Router Manager software can be run on any station in the network, whether wired or wireless, and used to configure Outdoor Routers, monitor the performance of wireless networks, and analyze links between two wireless stations.

D. WIRELESS MAN TESTBED TOPOLOGIES

Although the wireless metropolitan area network (MAN) testbed could be easily extended to cover a very large number of fixed and mobile nodes within the metropolitan area, we were primarily interested in testing configurations that were more typical of small to intermediate size Naval activities. Thus, the wireless topology was that of a main building wirelessly connected to a small number of remote sites with mobile wireless users (within range) able to access infrastructure resources directly from the main building or indirectly via any remote building.

The hub of the MAN testbed was the antenna mast located on the roof of Spanagel Hall (upper right portion of Figure 32). Standing 150 feet above sea level, the antenna mast was equipped with cables and amplifiers sufficient to support all of the previously described Outdoor antennas and provided clear line-of-sight to most of Monterey. The Central Office Router (COR) was connected to an infrastructure network via 10BaseT Ethernet and provided two wireless cards for use in point-to-point links (as the master) or point-to-multipoint links (as an access point) via any of the six outdoor antenna types available to us.

Figure 32. Monterey Wireless Metropolitan Area Network Point-to-Point Links.

Remote sites in the MAN testbed were configured on an as-needed basis and were located either on the NPS campus (within a 1 km radius), the NPS housing area at La Mesa (within a 3 kilometer radius) or at private residences within Monterey (within 5 kilometer radius). Each remote site was configured with a Remote Outdoor Router (ROR). At the La Mesa housing area, two 180º panel antennas (Figure 33) were semi-permanently installed on top of the 80 foot HAM radio tower. These two antennas provide 360º of WLAN coverage at 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps for up to 32 ORCs per channel throughout the entire housing area with the exception of areas shaded by dense tree cover, as shown in Figure 34.

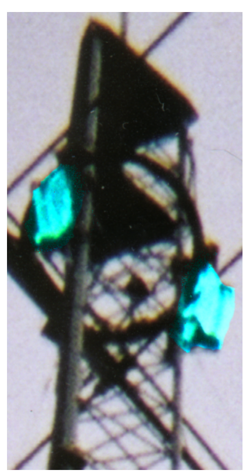

Figure 33. La Mesa Panel Antennas Atop 80’ Mast.

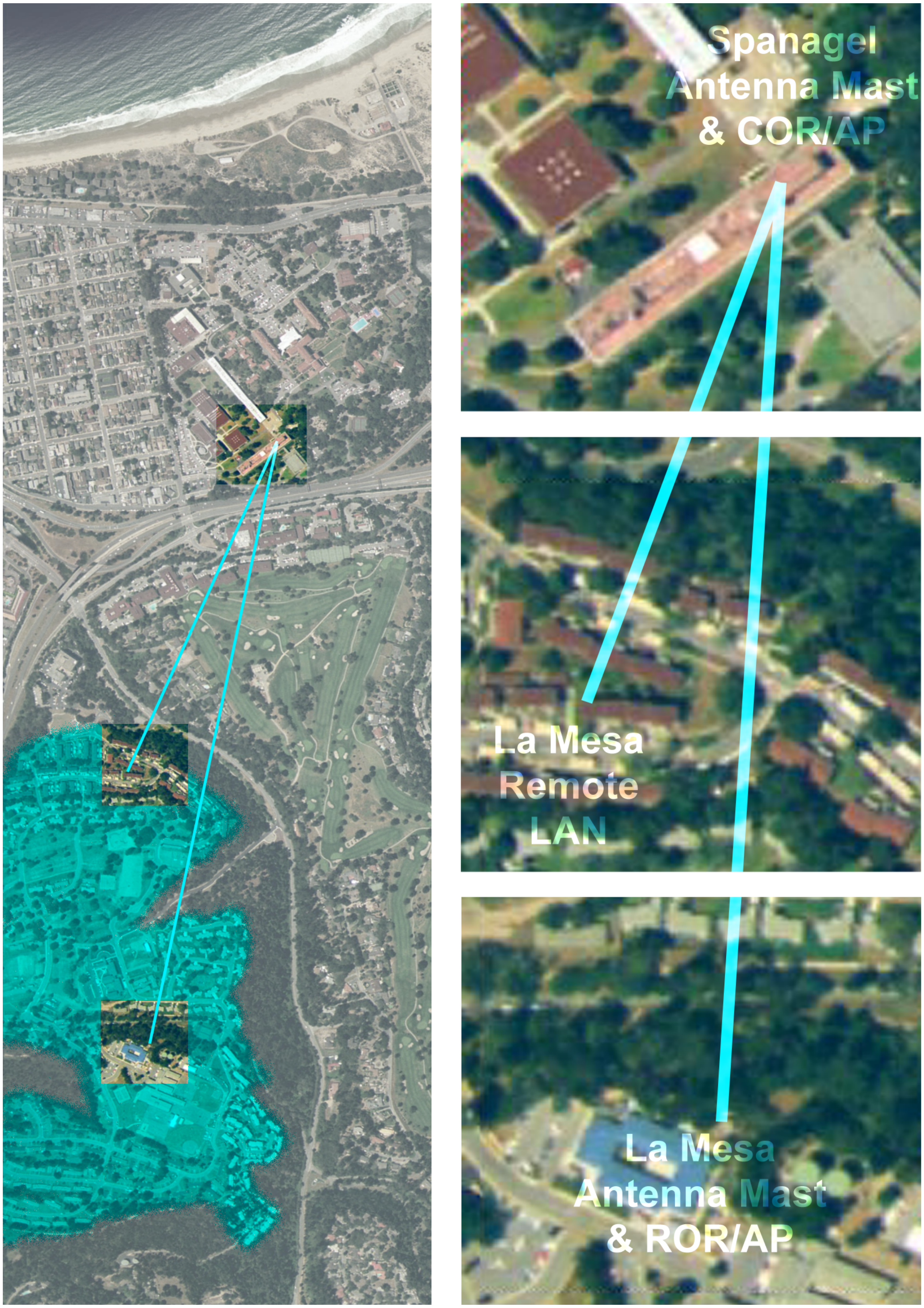

Figure 34. Monterey Wireless Metropolitan Area Network Point-to-Point Links.

The ROR was attached to the local infrastructure network (if present) via 10BaseT Ethernet and provided up to two wireless cards for use in point-to-point links (as the slave) or point-to-multipoint links (as the access point) again via any of the six outdoor antenna types available to us.

E. SECURITY

Each of the Outdoor Router networks configured and tested within the study were identified by a unique System Access Pass Phrase. Before any station could successfully connect to and access any of the networks, it must first have been pre-configured for ORiNOCO® proprietary mode, programmed with a System Access Pass Phrase that matched that specified within the COR and encrypting all data with the current valid 128 bit RC4 WEP key. Additionally, authentication based on MD-5 CHAP and access filtering based on PC card MAC address lookup and RADIUS authentication was employed to a limited extent.

F. SUMMARY

This chapter provided an overview of the specific components used in the wireless MAN testbed and the background information necessary for understanding the test plan methodology. In the next chapter, we examine the test procedures and performance results collected on the wireless metropolitan area network testbed.

V. EXPERIMENTAL MEASUREMENTS AND ANALYSIS

A. INTRODUCTION

Network performance metrics were collected from many locations within the Monterey metropolitan area, both on land and at-sea. The purpose of the testing was to gather sufficient data to characterize and predict the network link quality a mobile user could expect, given typical LOS obstruction over both land and water for various equipment configurations.

1. At-Sea Survey

The at-sea portion of the survey was conducted on Saturday, 17 November from within a privately-owned 25-foot pleasure craft using the equipment detailed in Table 13. The antenna was mounted on the wind-shield approximately six feet from the bow of the boat and continuously reoriented to keep it aligned with the AP. The laptop and signal amplifier were powered by a portable uninterruptible power supply. The goal was to collect the signal and noise power sampling data as seen by both the AP and the mobile station at several different ranges.

AP Location	Upper East roof of Spanagel Hall (150 feet above sea level)
AP Link Configuration	COR wireless PC Card, Lucent pigtail, 1 Watt amplifier, 20 dBi 90º Outdoor Panel Antenna (HG2420P) via 50' of LMR-200 cable.
AP Antenna Alignment	325ºT
Mobile Station Link Configuration	Laptop wireless PC Card, Lucent pigtail, 1 Watt amplifier, 14 dBi 30º Radome Enclosed Yagi Antenna (HG2415Y) via 10' of WBC-200 cable.

Table 13. Equipment Configuration for At-Sea Wireless MAN Survey.

The at-sea survey began at 10:00 am just north of the launch point at the Monterey Coast Guard pier. Waypoints '1' through '6', illustrated in Figure 35 below, roughly mark the center of each survey leg. Table 14 details the specific location data for each of these legs as reported by a hand-held GPS receiver for this at-sea portion of the survey.

Waypoint	Position	Leg Distance	Leg Time	Average Speed
1	N36.64653 W121.94055	5.3 Mi	46 min.	6.9 MPH
2	N36.66989 W121.95569	2.3 Mi	19 min.	7.4 MPH
3	N36.69074 W121.93629	3.1 Mi.	24 min.	7.7 MPH
4	N36.70511 W121.95493	3.1 Mi.	18 min.	10 MPH
5	N36.66406 W121.93290	3.1 Mi.	18 min.	10 MPH
6	N36.63541 W121.89586	3.1 Mi.	18 min.	10 MPH

Table 14. At-Sea Wireless MAN Survey Waypoint Data.

The test track closely followed the Monterey Peninsula and on out to sea some six miles north-east of Point Pinos. Once clear of the point, the sea state increased significantly, producing 15-20 foot swells. As the boat rode down into a trough, the LOS path to the COR was typically obstructed for a few seconds, dramatically reducing received signal power at both the mobile station and the AP. Consequently, throughput rates achieved during this period are markedly lower. Table 15 lists the average throughput rates achieved while downloading a 15 MB binary file from a unix server located on the infrastructure network behind the AP at various locations along the survey track. Data Set 2 was not collected because the link repeatedly dropped out as the boat pitched and rolled in the swells, making it impossible to keep the 30º beam of the Yagi antenna directed at either the horizon or the correct azimuth.

Data Set	Position (ºLatitude/ºLongitude)	Local Time	Download Time (Seconds)	Throughput (Kbps)	AP Range (Miles)	Bearing (ºTrue)
1	N36.63863 W121.92183	10:52	80.346	1231.933	4.0	319
2	N36.66989 W121.95569	11:11	N/A	N/A	6.2	311
3	N36.66989 W121.95569	11:22	62.780	1576.614	6.9	319
4	N36.69935 W121.94616	11:48	101.105	978.981	8.2	331
5	N36.69327 W121.94940	12:17	97.520	1014.972	8.0	329
6	N36.65598 W121.92372	12:35	55.259	1791.192	5.0	327

7	N36.62540 W121.89129	12:57	56.882	1740.105	2.3	337

Table 15. At-Sea Wireless MAN Survey Throughput.

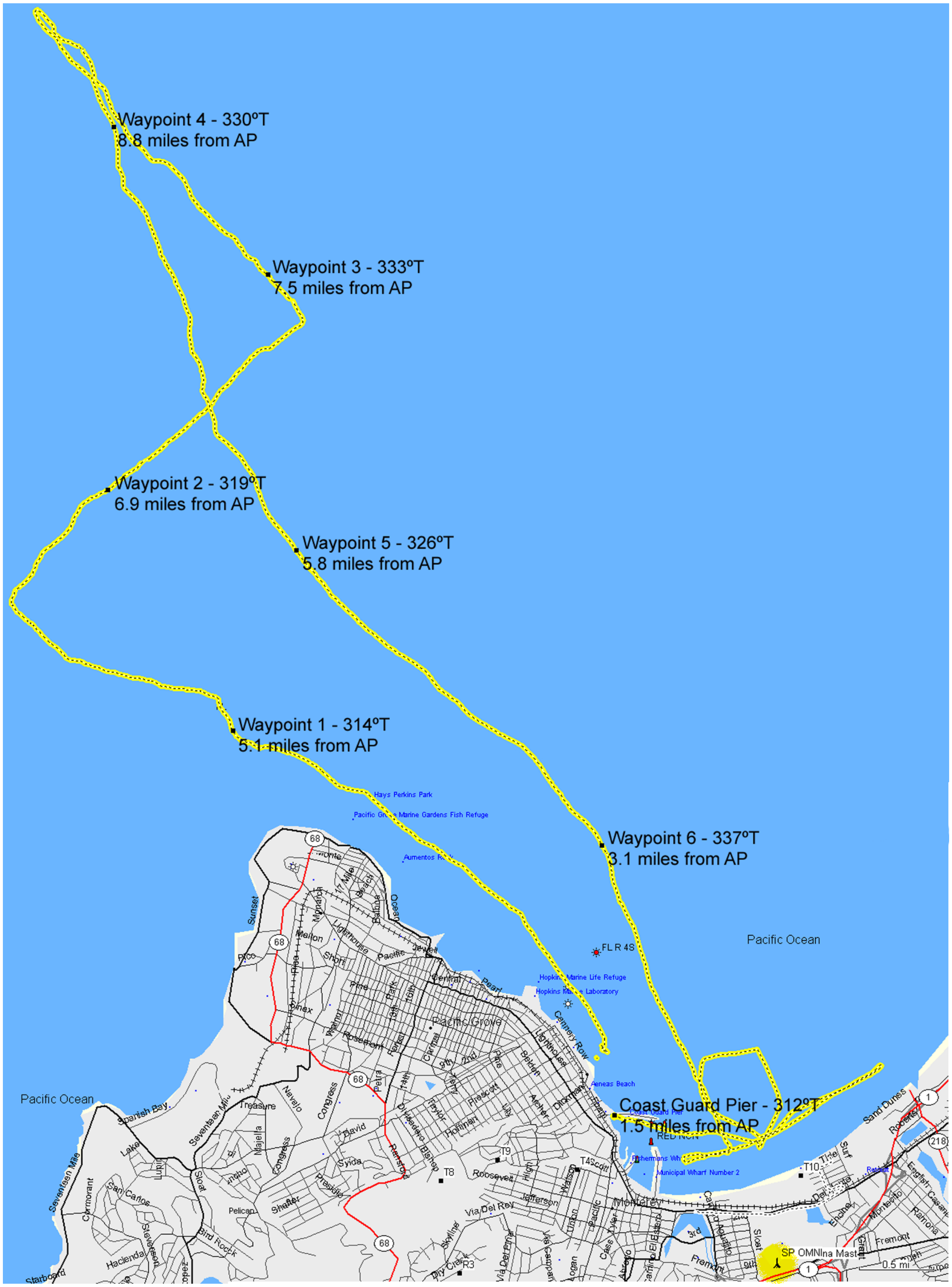

Figure 35. Survey Track Along North-East Coast of Monterey Peninsula.

2. Land-Based Survey

The land-based portion of the survey was conducted on 11 November and again on 2 December 2001 from within a privately owned automobile using the equipment detailed in Table 5-2 below.

AP Location	Upper East roof of Spanagel Hall (150 feet above sea level)
AP Link Configuration	COR wireless PC Card, Lucent pigtail, 1 Watt amplifier, 15 dBi 180º Outdoor Omni Antenna (HG2415U) via 50’ of LMR-200 cable.
AP Antenna Alignment	300ºT (11 November 2001) 357ºT (2 December 2001)
Mobile Station Link Configuration	Laptop wireless PC Card, Lucent pigtail, 1 Watt amplifier, 14 dBi 30º Radome Enclosed Yagi Antenna (HG2415Y) via 10’ of WBC-200 cable.

Table 16. Equipment Configuration for Land-Based Wireless MAN Survey.

Throughout the land-based survey, the mobile station configuration employed an antenna mounted on a three-meter fiberglass pole attached to the trunk of the car, as in Figure 36. The laptop and signal amplifier were powered by a portable Uninterruptible Power Supply. As in the at-sea portion of the survey, the goal was to collect the signal and noise power as seen by both the AP and the mobile station at several different ranges.

Figure 36. Antenna Mount Configuration for Land-Based Survey.

For the land-based survey, a large scale 7.5-minute Digital Elevation Model (DEM) of Monterey county was downloaded from the U.S. Geologic Survey (USGS) website at http://www.gisdatadepot.com/dem/. The DEM was rendered and carefully reviewed to identify potential survey locations that would yield both satisfactory LOS to the AP and adequately represent the topographic diversity present with the Monterey metropolitan area. Figure 37 illustrates the terrain surrounding the Monterey Bay and highlights the most diverse survey locations against the DEM image.

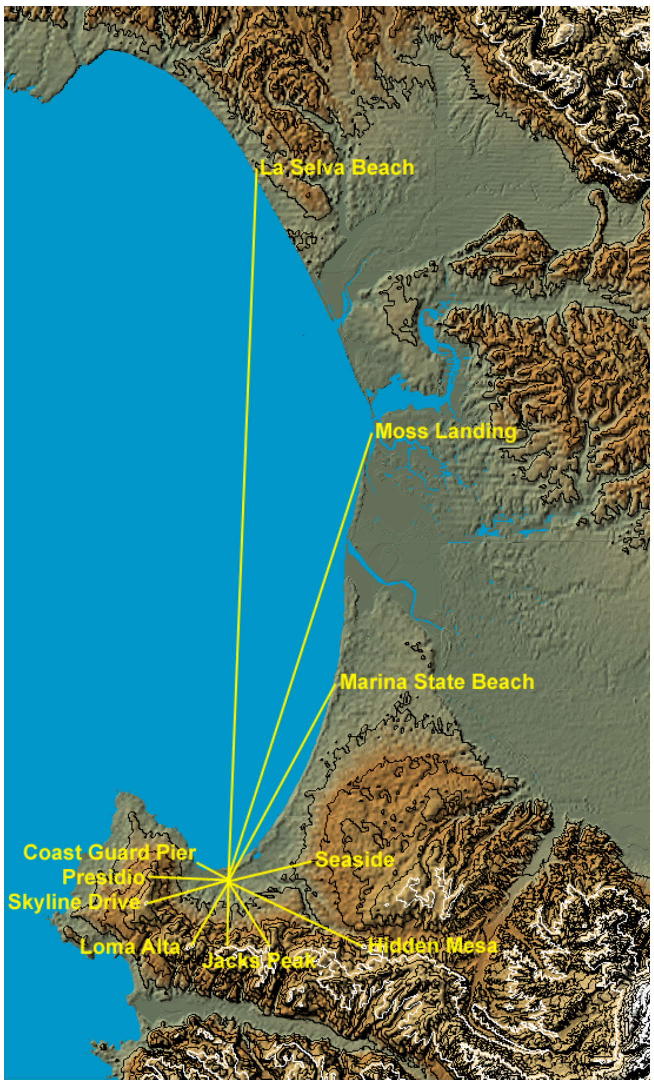

Figure 37. Diverse Monterey Bay Geography.

Table 17 details the specific location data for each of the land-based survey points.

Test	Location	Time	Range (mi)	Bearing (ºTrue)
B1	N36 35.692 W121 52.494	09:28	0.0	0
B2	N36 35.692 W121 52.494	09:35	0.0	0
B3	N36 35.692 W121 52.494	09:38	0.0	0
#1	N36 35.692 W121 52.494	10:24-10:39	0.0	0
#2	N36 35.233 W121 52.728	12:04-12:22	0.6	203
#3	N36 35.426 W121 55.066	13:09-13:25	2.4	263
#4	N36 36.102 W121 54.520	13:41-13:55	2.0	284
#5	N36 36.236 W121 53.930	14:08-14:19	1.5	295
#6	N36 36.559 W121 53.648	14:32-14:42	1.5	313
#7	N36 56.032 W121 51.805	16:41-17:26	23.6	1

Table 17. Land-Based Survey Locations.

During the initial survey of 11 November, signal data was collected at 18 locations but for only a few hundred data points each. Upon returning to the lab and analyzing these data sets for signal mean and variance characteristics, it was realized that many more points were necessary to smooth out the wildly fluctuating data. Thus, another survey was conducted on 2 December, this time gathering several thousand signal parameter data points at each of seven survey locations. The data collected on 11 November was however useful as a reference for the final data set collected on 2 December.

Table 18 summarizes the throughput results for a standard 15MB test file downloaded from and uploaded to an infrastructure-based unix file server. Additionally, throughput metrics were collected from the Windows-based WS_Ping ProPack utility running on the survey laptop. For each survey location, average throughput was calculated by the utility based on the round-trip delay of one-hundred 1,025 byte test packets generated on the laptop and sent to the AP subject to a maximum permissible delay of 100 ms and a maximum timeout of 500 ms. This test was thought to be more typical of Internet-based web traffic than the FTP throughput test.

	15MB FTP Throughput Test		WS_Ping ProPack Test	
Test	Download (Kbps)	Upload (Kbps)	Throughput (Kbps)	% Packets Lost
B1	2330	2405	2170	0
B2	2375	2315	517	0.02
B3	2380	2320	1460	0
#1	2250	2205	2120	0
#2	2254	2158	2130	0.03
#3	1061	1807	1630	0.03
#4	2105	2143	2100	0.01
#5	1978	1851	1620	0.07
#6	2225	2225	2160	0.01
#7	133	194.8	467	0.03

Table 18. Land-Based Throughput Data.

Table 19 summarizes the link test results for each of the land-based survey locations. Test cases B1 through B3 were baseline tests conducted early in the day from within the Advanced Networking Laboratory on campus in order to establish best-case loss and data rates. B1 tested the “wireless” network path between the survey laptop and a wireless AP identical to the AP of the wireless testbed. B2 tested the “wired and wireless” network path between the survey laptop, the identical wireless AP and the default gateway router of the infrastructure network. B3 tested the network path between the survey laptop, the identical wireless AP, the infrastructure default gateway router and the testbed wireless AP. These three baseline test cases provided an estimate of the best-case link throughput we could expect across the remaining test cases.

Test cases #1 through #6 were conducted during a rain storm localized over Monterey. Consequently, the rain and wind present at each location tended to manipulate the Yagi antenna, causing signal metrics to be characteristically variable. Test case 7, however, was conducted from the outskirts of Santa Cruz. For this test, only the AP antenna was in the rain and wind.

As described previously in Table 16, the AP signal was transmitted at 150 feet above sea level from the roof of Spanagel Hall (8^{th} deck). Test case #1 was conducted within 2 meters of the actual wireless testbed COR/AP and surveyed the “wireless” network path between the survey laptop and the wireless testbed AP under minimal free-space loss conditions. Test case #2 was conducted from the La Mesa housing area located 0.6 miles away from the AP. At 150 feet above sea level, LOS was level, skimming over roof tops and between a few tall trees (Figure 38).

Figure 38. La Mesa Housing Area Survey Location.

Test case #3 was conducted from the road side on Skyline Drive, 2.4 miles away from the AP. At 505 feet above sea level, LOS was looking down a steep hillside through a clearing within a dense forest. Test case #4 was conducted from the top of

Harrison Street near the main entrance to the Presidio of Monterey, 2.0 miles away from the AP. At 325 feet above sea level, LOS was looking down the hill over the major downtown hotels and office buildings. Test case #5 was conducted from the top of Scott Street near the main entrance to the Presidio of Monterey, 1.5 miles away from the AP. At only 94 feet above sea level, LOS was looking slightly up, over the major downtown hotels and office buildings. Test case #6 was conducted from the base of the Monterey Coast Guard Pier, 1.5 miles away from the AP. At sea level, LOS was looking slightly up, over a thick grove of trees that obscures the view of Spanagel Hall (Figure 39).

Figure 39. Monterey Coast Guard Pier Survey Location.

Test case #7 was conducted from Gospondnevich Road in La Selva Beach, 23.6 miles away from the AP. At 150 above sea level, LOS was level, looking over the waves of the Monterey Bay.

	ORiNOCO Client Manager Link Test Messages			Messages Received by Fixed AP				Messages Received by Mobile Station			
Test	Sent	Lost	% Lost	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
B1	1000	0	0.00%	500	0	0	0	500	0	0	0
B2	1000	0	0.00%	500	0	0	0	500	0	0	0
B3	1000	0	0.00%	500	0	0	0	500	0	0	0
#1	2711	7	0.26%	2704	0	0	0	2641	38	25	0
#2	3000	3	0.10%	2997	0	0	0	2996	1	0	0
#3	2999	29	0.97%	2968	2	0	0	2759	176	35	0
#4	2555	4	0.16%	2551	0	0	0	2544	7	0	0
#5	2000	1	0.05%	1998	1	0	0	1998	1	0	0
#6	1526	3	0.20%	1523	0	0	0	1501	12	10	0
#7	8003	195	2.44%	0	0	2224	5584	0	0	0	7808

Table 19. Wireless MAN Link-Test Data for December 2, 2001.

Table 19 summarizes the link test results. The link test logs were started immediately upon successfully establishing the wireless link between the survey station and the AP. Once all FTP and WS_Ping throughput tests were complete, the link test logs were stopped, saved and the wireless link was torn down. Consequently, the link test results offer a comprehensive look at the wireless link that spans all other test data collected at each survey location. During a link test, test messages are sent from the survey station to the AP and back to the survey station at the rate of approximately four messages per second. Each test message that is sent and successfully received results in a single line of test data in the log containing the signal metrics listed below:

- Messages Received
- Messages Lost
- Average/Minimum/Maximum Local Signal to Noise Ratio (dB)
- Average/Minimum/Maximum Local Signal Level (dBm)
- Average/Minimum/Maximum Local Noise Level (dBm)
- Average/Minimum/Maximum Remote Signal to Noise Ratio (dB)
- Average/Minimum/Maximum Remote Signal Level (dBm)
- Average/Minimum/Maximum Remote Noise Level (dBm)

After a quick review of the link test results below, test case #7 stands out from the others with the highest percentage of message loss at 2.44%. Test case #7 is also noticeably different from the other cases in that its traffic utilized the lower data rates of 1 Mbps and 2 Mbps exclusively. This is due to the auto-fall back feature of 802.11b. It is also clear from this same data that the AP perceived a higher quality channel than did the mobile station. This conclusion is reinforced by the evidence of the higher upload throughput that results from occasional use of the 2 Mbps data rate vice the 1 Mbps data rate. Because both antennas were located at 150 feet above sea level, the horizon distance is calculated as 17.3 miles in a standard atmosphere (K=4/3) or 12.3 miles in substandard atmosphere conditions (K=2/3); both of which yield a surface diffraction loss of nearly 20 dB. Given the extreme distance involved, it is surprising that the link was able to sustain FTP upload and download throughputs three times that of telephone modems.

The second most notable test case was #3. The LOS for this test was the most obscured of the six tests, with almost no perceivable visibility through the dense forested area. Additionally, at 2.4 miles and 505 feet above sea level, the angle to the survey station from the AP was approaching the 5^{o} beam-width of the omni-directional antenna, reducing the power transmitted and received at the AP by half. Never the less, the link performed satisfactorily with a sustained throughput greater the 1 Mbps.

The last notable test case was #1. Recall that this test took place from within the room housing the AP with the antenna located outside on the roof two stories above. Although the LOS for this test was totally obscured by a poured concrete floor, there was sufficient multipath present to sustain an FTP throughput of 2 Mbps.

3. Metropolitan Area Survey Results

Figure 40 is a composite graphic in logarithmic scale of mobile (local) and AP (remote) SNR, local and remote signal power, and local and remote noise power versus distance. Each average sample point is based on extended measurements of power parameters at each survey location. Plots of power levels for each individual location are included in Appendix A. Not surprisingly, local noise power was very low during the at-sea portion of the survey, once we were greater than six miles from land. Both local and remote signal power was impressive at ranges beyond six miles, due primarily to the essentially unobstructed LOS paths over the Monterey Bay.

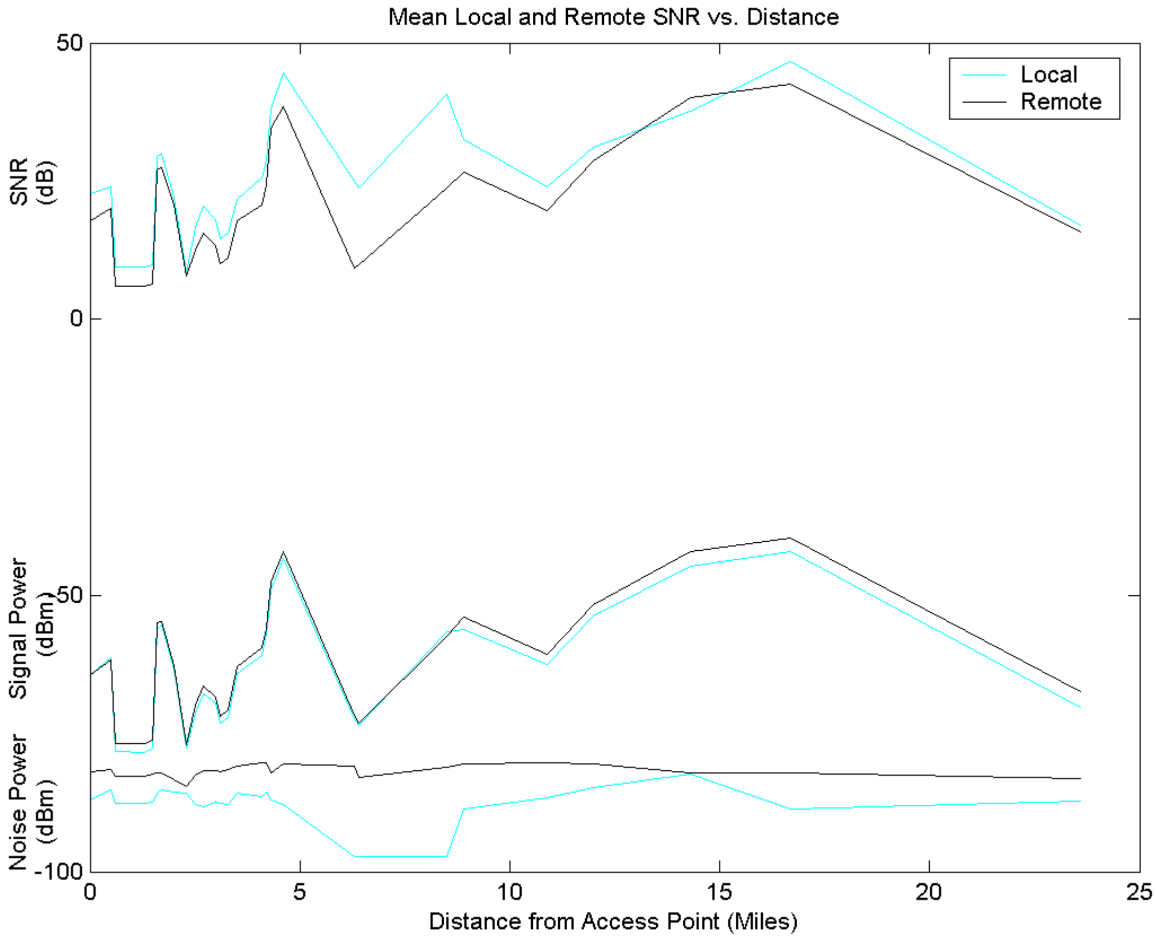

Figure 40. Summary of Wireless MAN Mean Survey Data.

Figure 41 illustrates the rate at which throughput falls off with distance within our survey area. Disregarding outliers, a consistent, non-linearly decreasing trend can be identified as distance is increased. It is worth noting, however, that even at 24 miles, an acceptable throughput of 200 Kbps can be achieved while staying within FCC power constraints.

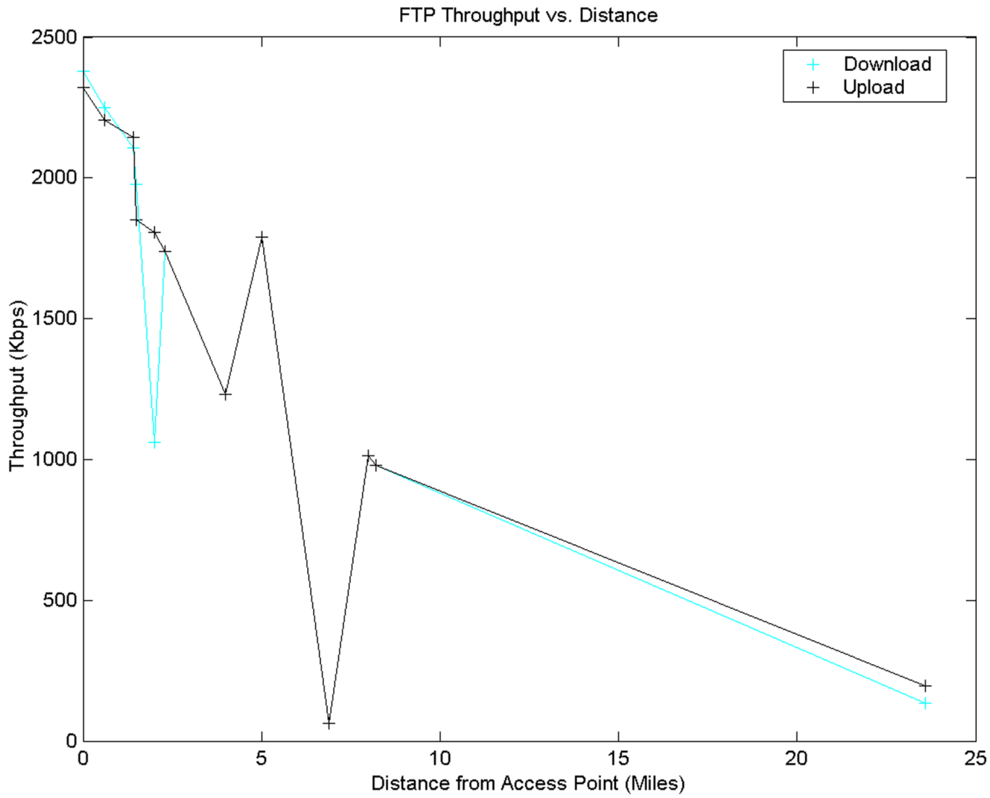

Figure 41. Wireless MAN FTP File Throughputs.

Figure 42 illustrates the rate at which both the local and remote signal-to-noise ratios become increasingly variable with distance throughout our survey area. This exponentially increasing variability directly affects packet delay due to dropped packets and signal loss, negatively impacting perceived network link quality. This in large part explains the behavior seen in Figure 41. As the inconsistency in signal presence increases exponentially, the throughput is affected significantly.

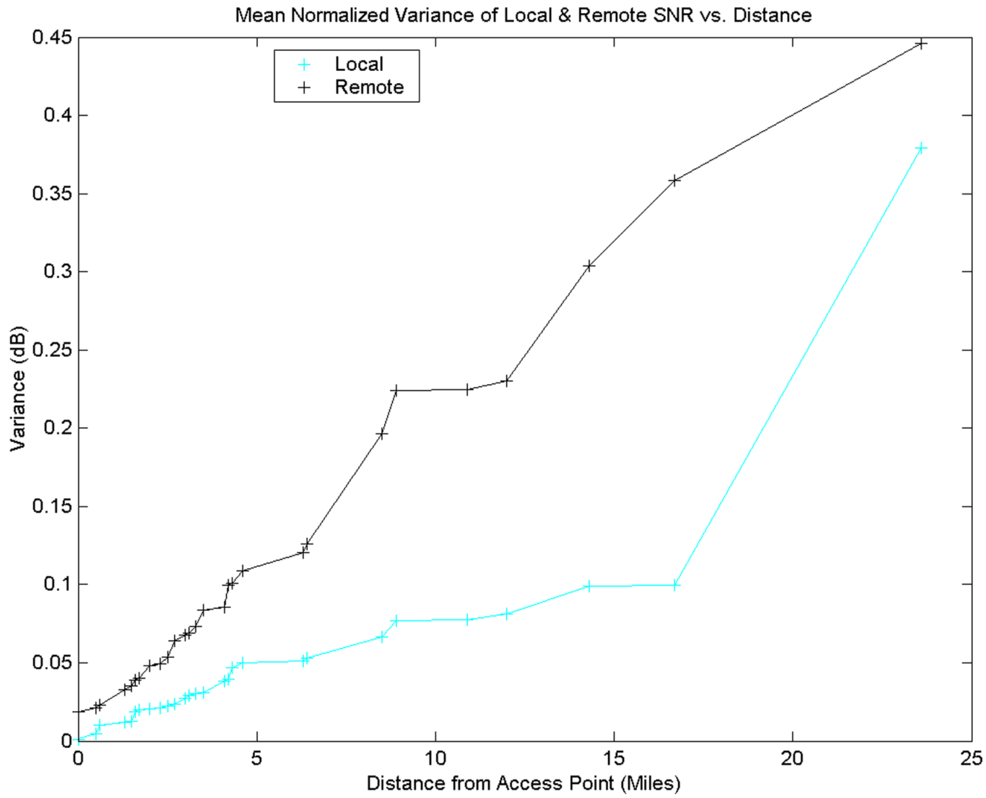

Figure 42. Wireless MAN Mean Normalized SNR Variance.

B. SUMMARY

In this chapter we examined the test procedures and performance metrics collected during the evaluation of our IEEE 802.11b compliant wireless metropolitan area network testbed. We analyzed the signal power and throughput characteristics obtained throughout a continuous at-sea survey composed of seven intermediate way-points and a land-based survey of seven test locations.

This concludes the performance analysis of our wireless metropolitan area network testbed. In the next and final chapter, we will review the results of this thesis with an eye toward areas of potentially useful related research and make some closing statements.

VI. CONCLUSIONS AND RECOMMENDATIONS

The goal of this thesis was to assess the performance of IEEE 802.11b wireless local area network standards and applications when extended to the range of a metropolitan area. Although the IEEE 802.11b WLAN specification was primarily intended for use in extending “wired” LANs to mobile users within an indoor office environment, we have shown that this same technology can be applied to an outdoor metropolitan environment as well. Our exclusive use of IEEE 802.11b network cards and routers throughout this study helped ensure a standard performance baseline across dramatically varying signal channel conditions. Because the main objective of WLANs is portable data communications, the performance metrics of this study were based exclusively on network traffic that is characteristic of the core internetwork services of file transfers and web browsing.

A. CONCLUSIONS

Our tests showed that CCK modulation yields acceptable high and medium rate performance near 2 Mbps at ranges of less than 2 miles in outdoor environments. At ranges beyond 2 miles, DQPSK modulation and DBPSK modulation yield standard and low rate performance with graceful near-linear degradation (down to approximately 200 Kbps at 20 miles).

Another significant finding of our study was related to the highly variable nature of link signal-to-noise ratio typified by a mobile station roaming within the tall office buildings of a city center. We found that FTP throughput performance was severely degraded in the majority of locations as the LOS path to the AP was obstructed, but that the throughput performance degradation experienced by a web user could be largely off-set by continuous motion of the ORC through the multipath environment. At speeds typical of downtown automobile traffic, we found that the high and medium data rates provided by CCK modulation were sufficient to transfer the relatively short-duration data packets typical of web-based traffic within the brief periods of minimally sufficient link

SNR. Thus, the relatively short-duration web-based data packets and their acknowledgements were able to traverse the link and relieve buffer queues.

B. RECOMMENDATIONS

There are numerous opportunities for further research using the existing wireless testbed configurations as developed in this thesis. An interesting test that could yield useful results would be to compare achievable throughputs between a mobile station associated with a COR AP interface and a remote EP that is wirelessly connected to the same COR over a point-to-point link interface. The goal would be to determine the throughput penalty due to the additional propagation and processing delays of the range extending EP.

Additionally, the testbed could easily be extended as future technologies, such as 802.11a and 802.11g, become available. Further research could then focus on testing these physical networks and comparing the performance data with simulation results from existing OPNET models to explore the operational applicability and performance characteristics of multiple roaming 802.11a/b/g WLAN units in outdoor and tactical environments. In addition, determining the intermediate threshold range at which the mobile unit achieves a better SNR and throughput for either the EP or AP would be equally interesting.

The security aspects of 802.11 networks are particularly relevant, many of which have not been adequately studied. Further research could compare and contrast the usefulness of Wired Equivalent Privacy, Secure Shell, per user, per session, unique broadcast and session keys in protecting the confidentiality of network data and the negative performance impacts of each on overall network throughput for a given level of security overhead. Some of these aspects are already implemented within the Radius terminal access control functionality of the testbed AS-2000.

The mobility of users throughout the network is a major concern for tactical systems. The wireless testbed could be extended to include multiple outdoor access points or even mobile access points through the use of two 802.11 interfaces on each router. The performance of such a “mobile” infrastructure configuration could then be compared to ad-hoc configurations in order to determine the effectiveness of existing bridging and routing protocols. Performance could also be compared to existing OPNET models of mobile ad-hoc networks to validate their simulation results.

C. CLOSING COMMENTS

The IEEE 802.11b WLAN protocol standard provides the mobility and high data rate wireless connectivity required to deliver limited multimedia application traffic in a multi-user, multiple access environment. Our test assumptions were sufficiently general to ensure our test results could be easily applied to nearly any geographic setting.

As the first serious and universally accepted standard for WLANs, IEEE 802.11 will continue to improve the speed and quality of mobile data communications. The performance data and analysis presented in this thesis resulted from an implementation of the 802.11b specification. There are, however, other 802.11 specifications like 802.11a and the proposed 802.11g standard for higher rate (20+ Mbps) extensions in the 2.4-GHz band that may unify 2.4 and 5-GHz products and systems. 802.11 products may then achieve the same 52 Mbps maximum capacity already enjoyed by 802.11a products operating at 5 GHz while affording the greater range due to the lower frequency. While the formal document for 802.11g will undergo several levels of revision and editing before final publication, the standard is expected to receive final approval in October of 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A: WIRELESS MAN SURVEY DATA

Figures A1 through A14 illustrate the signal power, noise power and signal-to-noise ratios present for each of the at-sea and land-based survey locations.

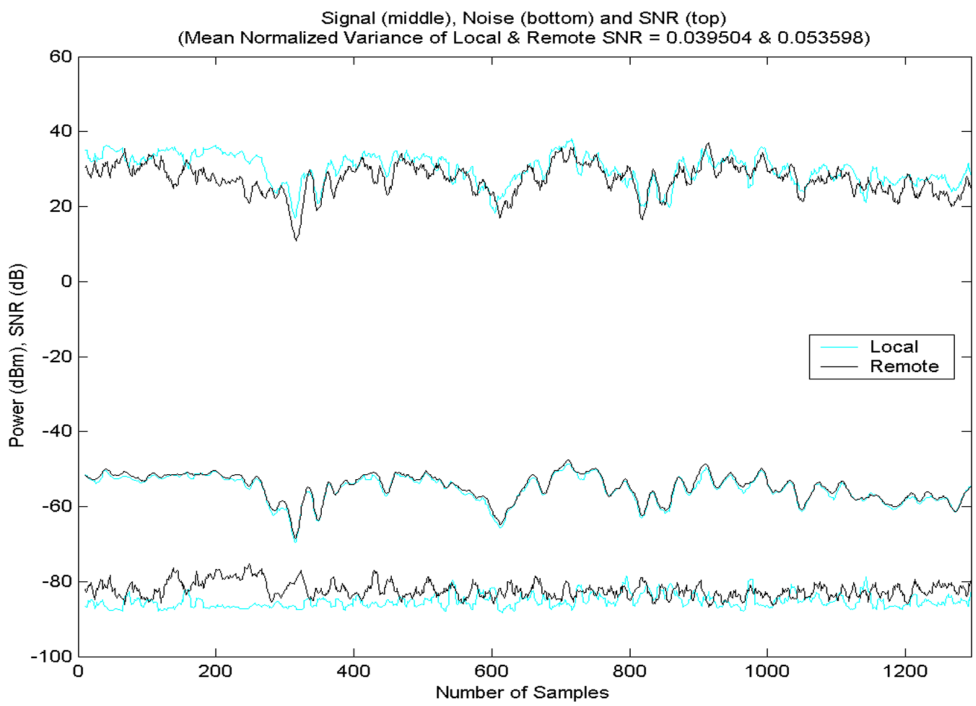

Figure A1. Signal Power Levels for At-Sea Survey Data Set 1.

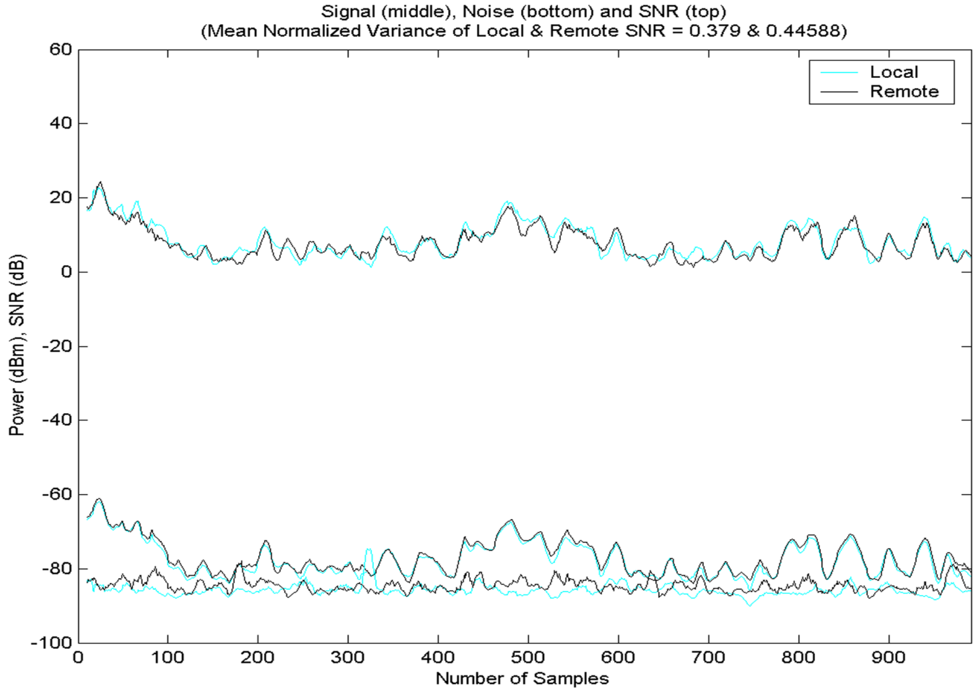

Figure A2. Signal Power Levels for At-Sea Survey Data Set 2.

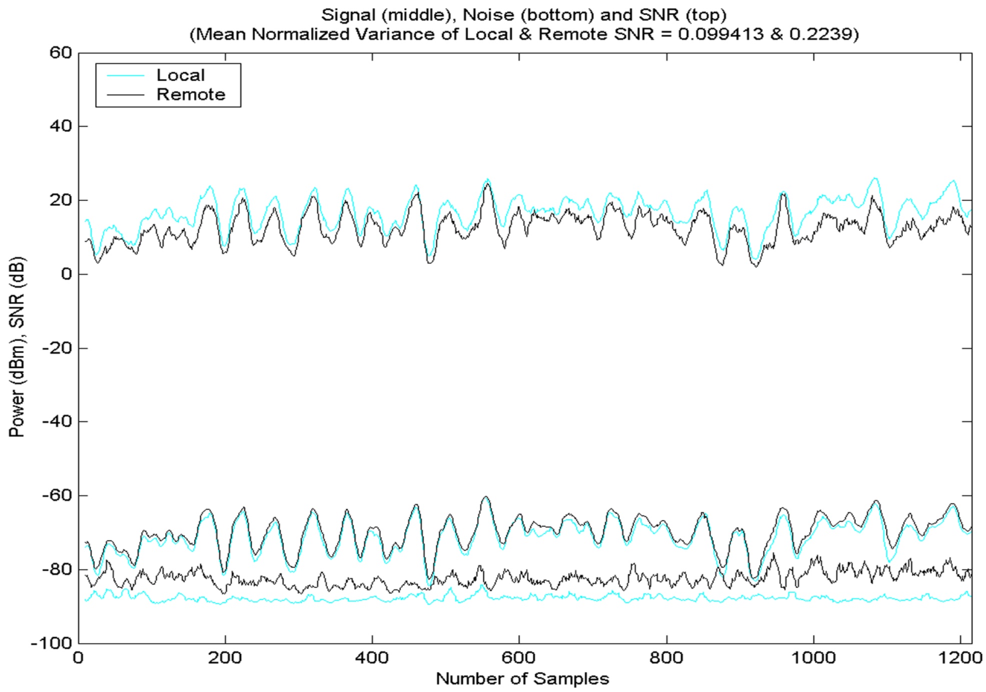

Figure A3. Signal Power Levels for At-Sea Survey Data Set 3.

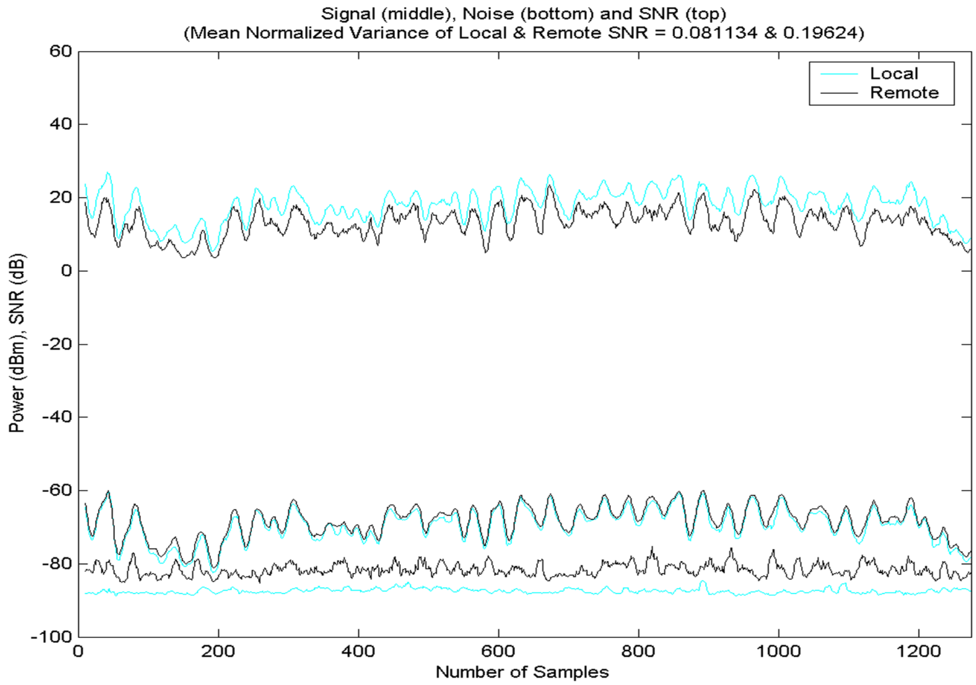

Figure A4. Signal Power Levels for At-Sea Survey Data Set 4.

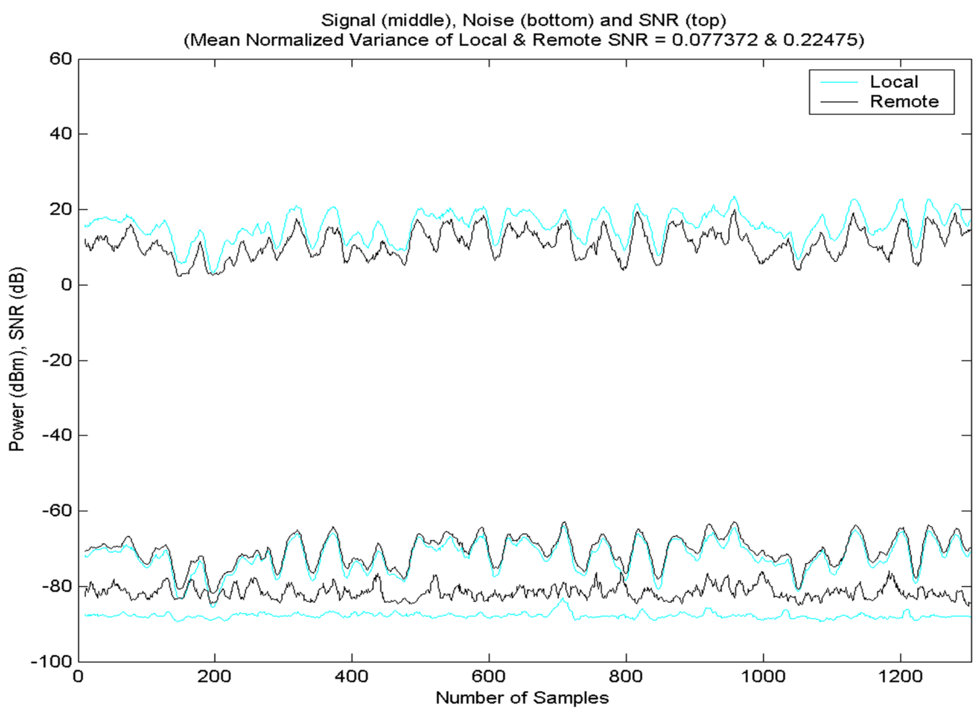

Figure A5. Signal Power Levels for At-Sea Survey Data Set 5.

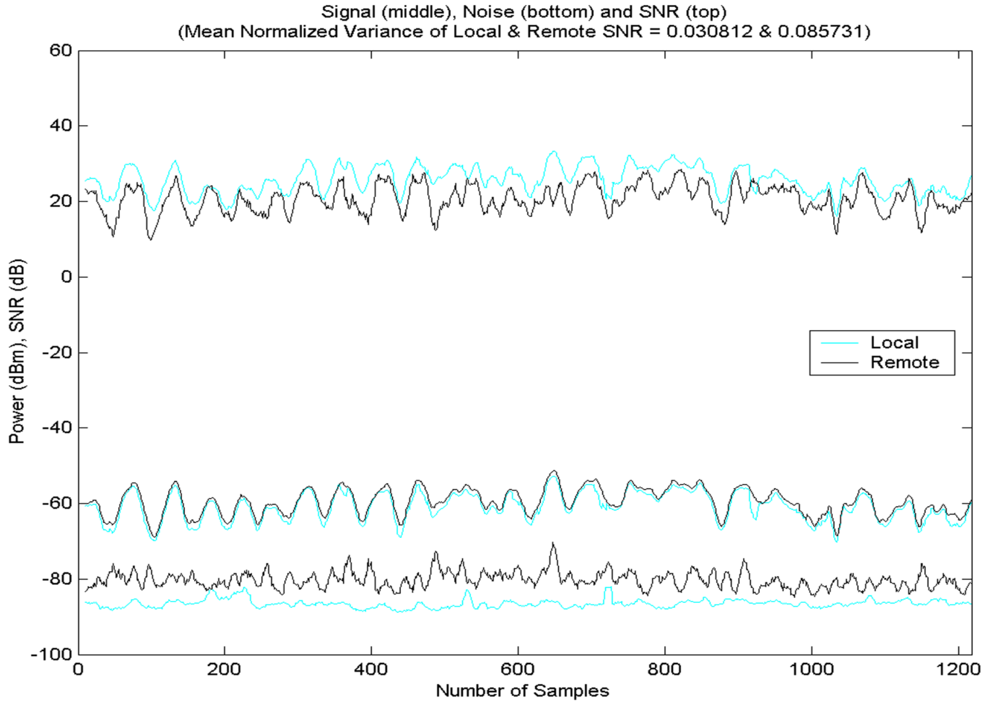

Figure A6. Signal Power Levels for At-Sea Survey Data Set 6.

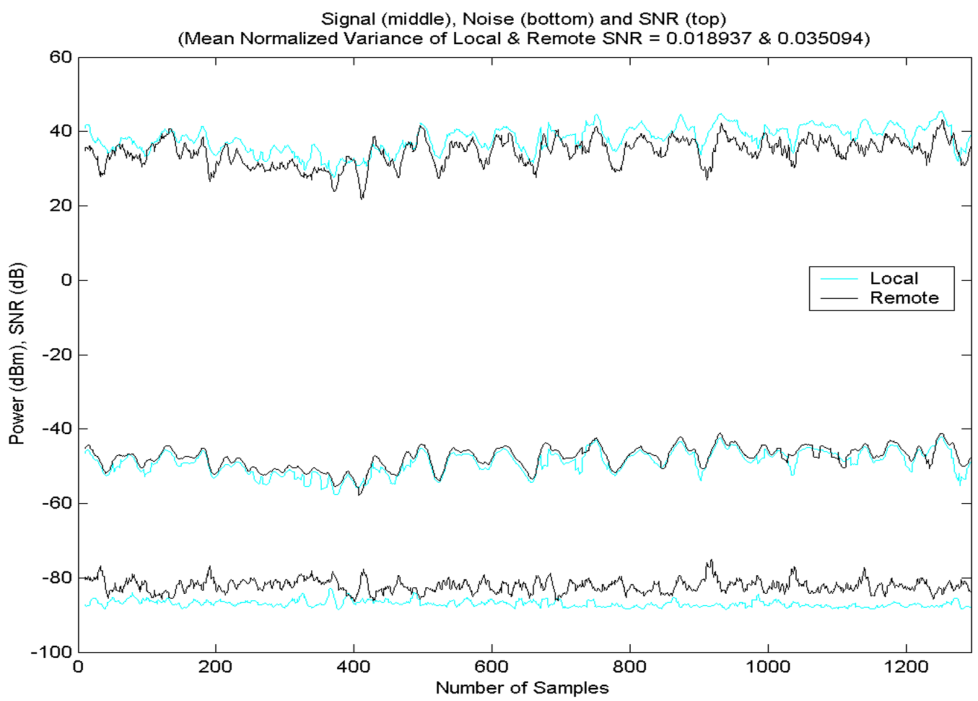

Figure A7. Signal Power Levels for At-Sea Survey Data Set 7.

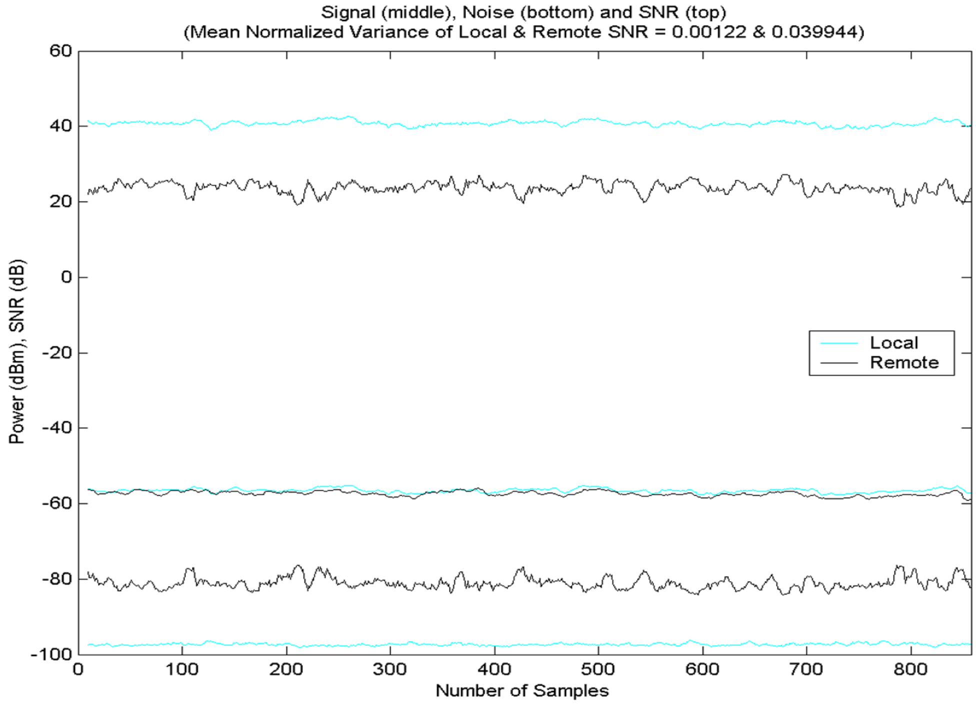

Figure A8. Signal Power Levels for Land-Based Survey Test Case #1.

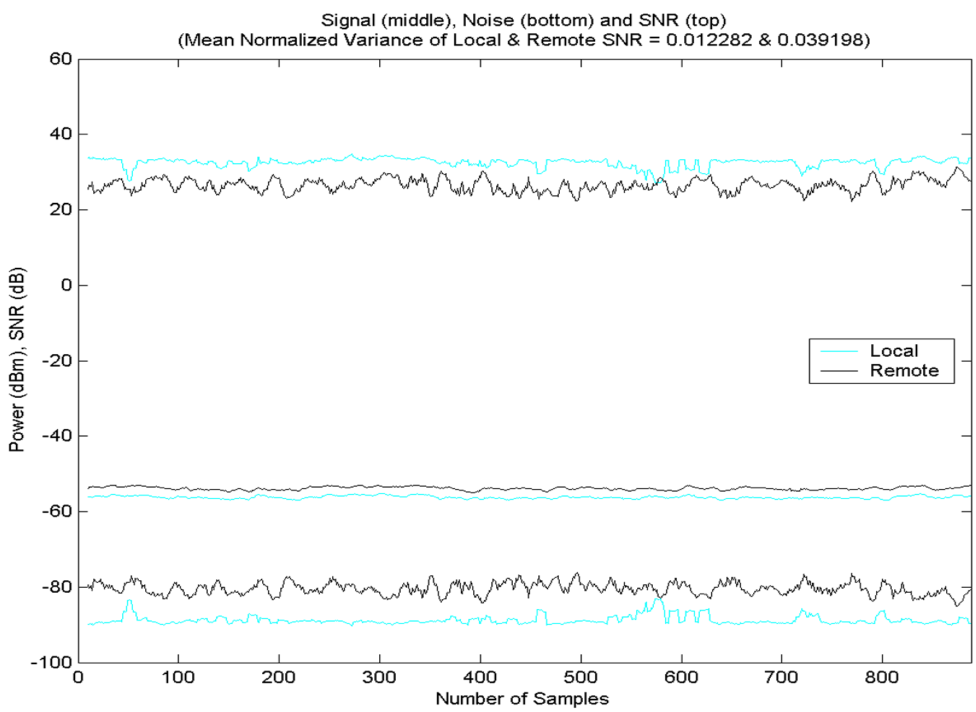

Figure A9. Signal Power Levels for Land-Based Survey Test Case #2.

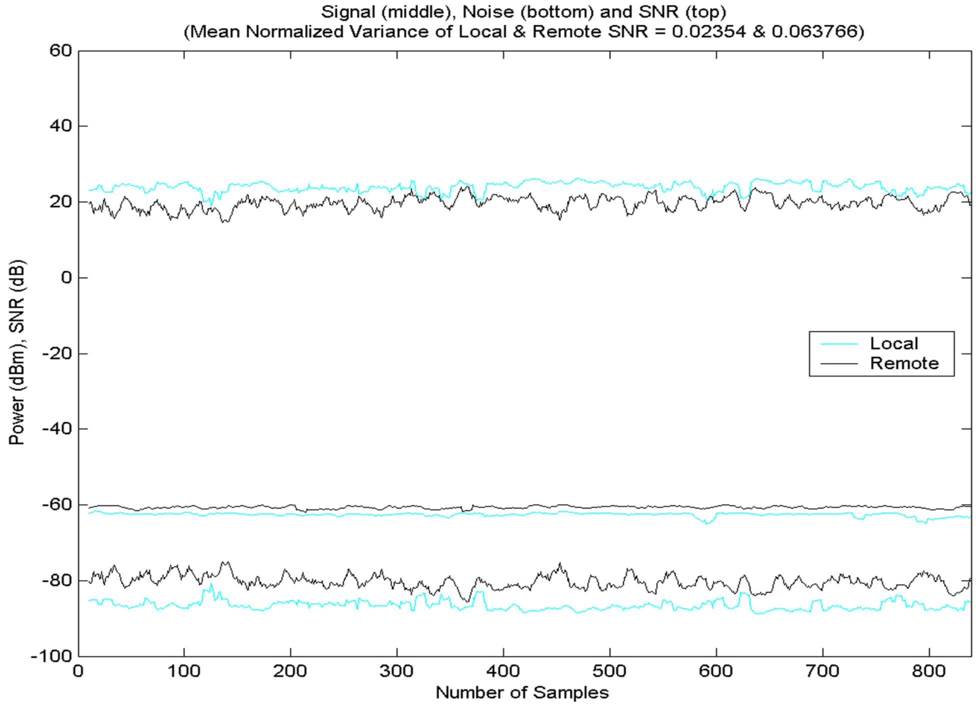

Figure A10. Signal Power Levels for Land-Based Survey Test Case #3.

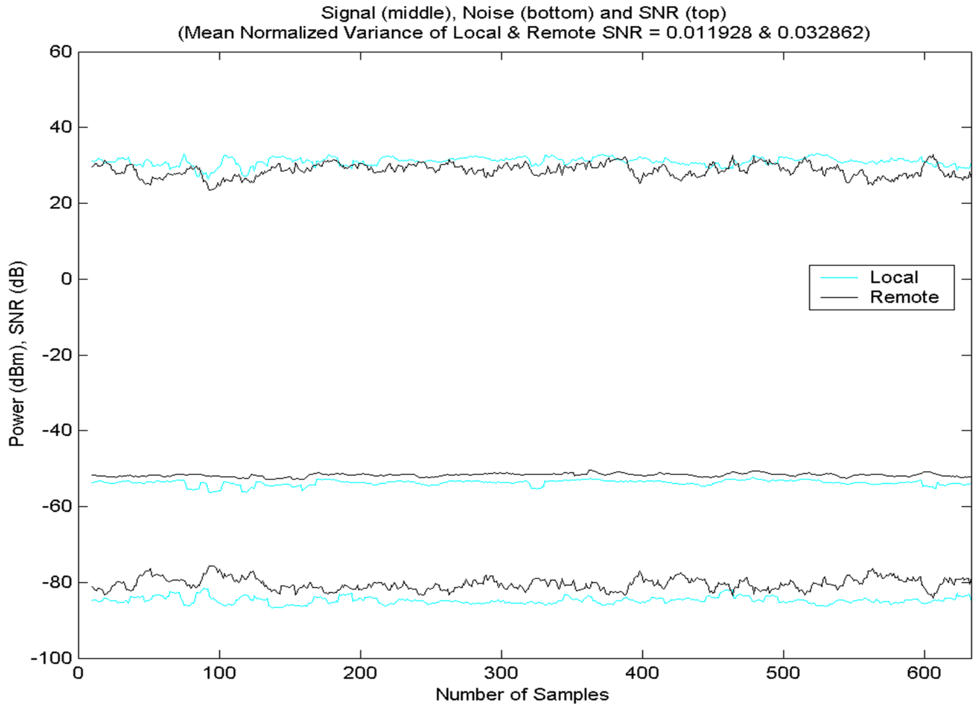

Figure A11. Signal Power Levels for Land-Based Survey Test Case #4.

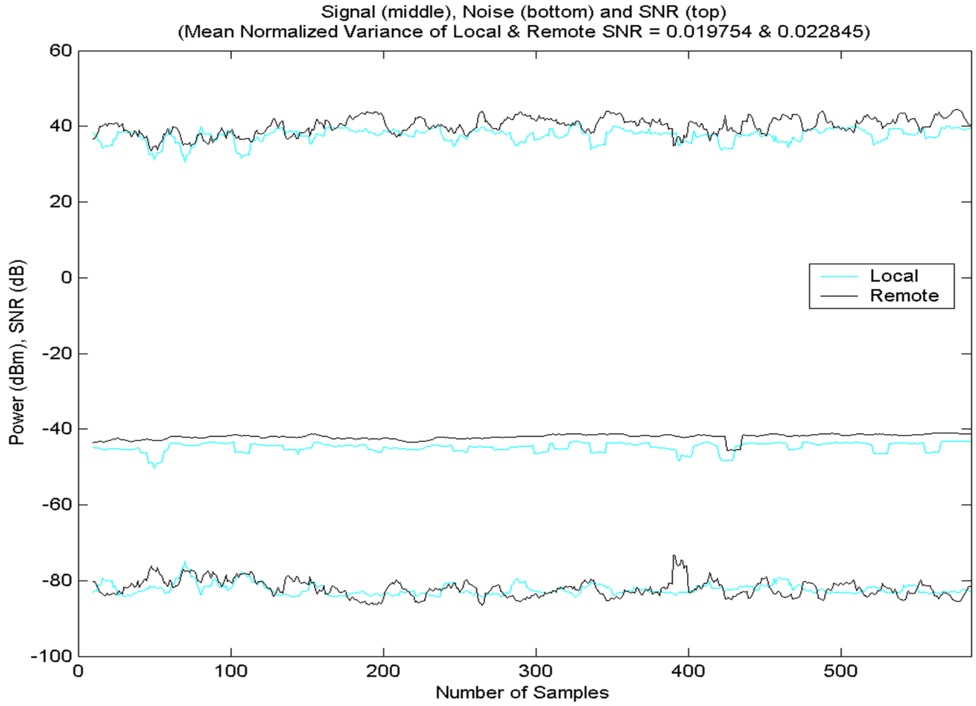

Figure A12. Signal Power Levels for Land-Based Survey Test Case #5.

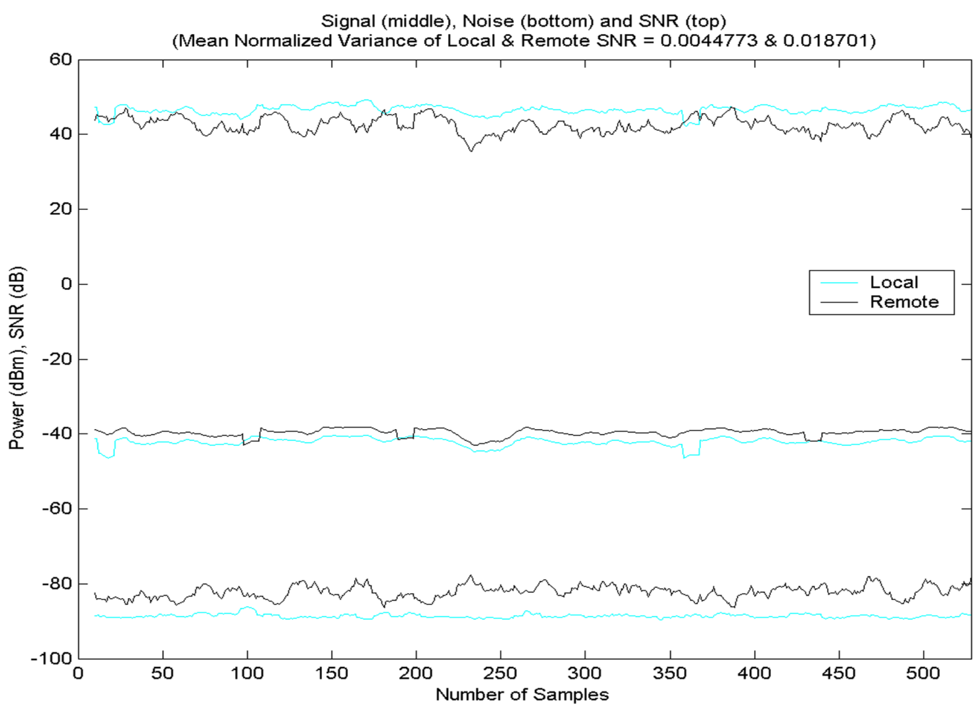

Figure A13. Signal Power Levels for Land-Based Survey Test Case #6.

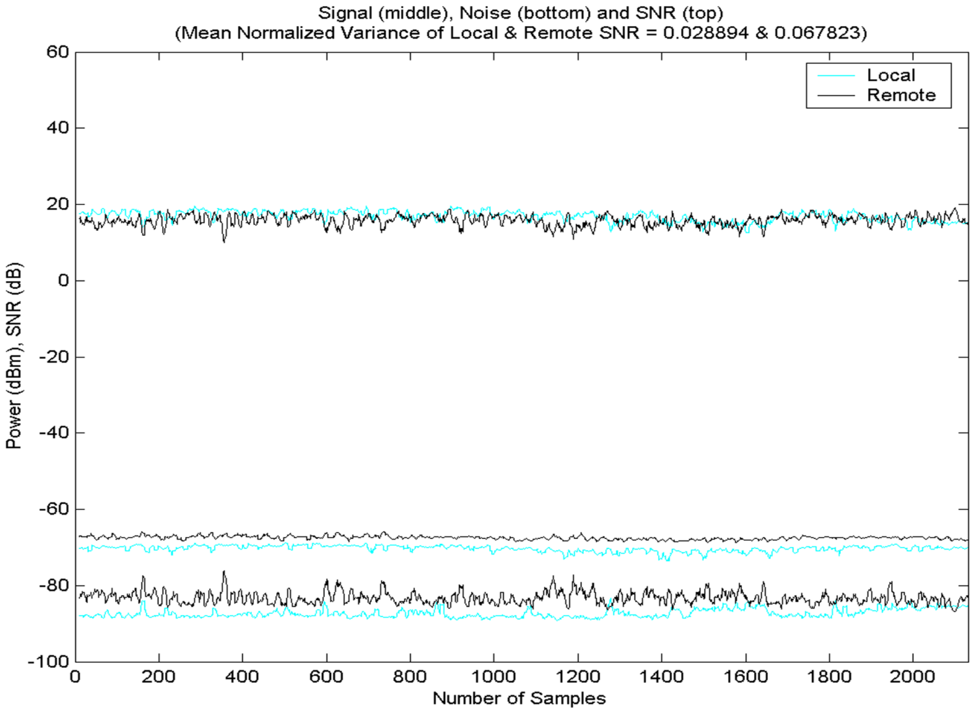

Figure A14. Signal Power Levels for Land-Based Survey Test Case #7.

LIST OF REFERENCES

1. Institute of Electrical and Electronics Engineers, ANSI/IEEE Std 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 20 August 1999.

2. Institute of Electrical and Electronics Engineers, IEEE Std 802.11b/D8.0, *DRAFT Supplement to STANDARD for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, September 2001.

3. Institute of Electrical and Electronics Engineers, 802.11 Task Group G, *Standard for Higher Rate (20+ Mbps) Extensions in the 2.4GHz Band*, 16 November 2001, [http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm]

4. O'Hara, B., Petrick, A., *The IEEE 802.11 Handbook: A Designer's Companion*, IEEE, 1999.

5. Spurgeon, C., *Ethernet: The Definitive Guide*, O'Reilly & Associates, 2000.

6. Geier, J., *Wireless LANs: Implementing High Performance IEEE 802.11 Networks*, Sams, 2001.

7. Andren, C., Webster, M., "CCK Modulation Delivers 11 Mbps for High Rate IEEE 802.11 Extension." Wireless Symposium/Portable By Design Conference, 26 Feb. 1999. pp. 7-10.

8. Santamaría, A., López-Hernández, F., *Wireless LAN Standards and Applications*, Artech House, 2001.

9. Bing, B., *Broadband Wireless Access*, Kluwer Academic, 2000.

10. Bertoni, H., *Radio Propagation for Modern Wireless Systems*, Prentice Hall, 2000.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

4. Professor John C. McEachen, Code EC/Mj
   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. CAPT John O'Dwyer
   Naval Information Warfare Activity
   Fort George G. Meade, MD

7. CAPT Chris Parente
   Deputy Director for Intelligence, Surveillance and Reconnaissance
   Space and Naval Warfare Systems Command
   San Diego, CA

8. CDR Jan Tighe, USN
   Naval Information Warfare Activity
   Fort George G. Meade, MD

9. CDR Tim White, USN
   Chief of Naval Operations, Code N201
   Arlington, VA

10. LCDR Al Kinney, USN
    Naval Security Group Activity
    Yokosuka, Japan

11. LT Bryan Braswell, USN
Naval Information Warfare Activity
Suitland, MD

12. LT Patrick Mallory, USN
Space and Naval Warfare Systems Command, PMW-189
San Diego, CA

13. Mr. John Audia
SPAWAR Systems Center San Diego, Code 272
San Diego, CA