NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE BENEFIT OF 802.20 TECHNOLOGIES ON INFORMATION FLOW IN NETWORK-CENTRIC WARFARE

by

Jacob Huffaker

September 2005

Thesis Advisor: Alex Bordetsky
Thesis Advisor: Dan Boger

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	3. REPORT TYPE AND DATES COVERED
	September 2005	Master's Thesis

4. TITLE AND SUBTITLE: The Benefit of 802.20 Technologies on Information Flow in Network Centric Warfare	5. FUNDING NUMBERS
6. AUTHOR(S) Jacob Huffaker	
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	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

This thesis will focus on the area of 802.20 wireless networking and how this technology will vastly benefit the US military forces, especially in the Network Centric concept of operations, where information flow is crucial. It will investigate this technology using published literature and previously gathered experimental data. This thesis will then relate its findings to Network Centric Warfare and the matters that could be most affected by this new technology.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Wireless Networking, Network-Centric Warfare, 802.20, Command and Control	73
	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

THE BENEFIT OF 802.20 TECHNOLOGIES ON INFORMATION FLOW IN NETWORK-CENTRIC WARFARE

Jacob A. Huffaker
Ensign, United States Navy
B.S., United States Naval Academy, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY (JOINT COMMAND, CONTROL, AND COMMUNICATIONS (C3)

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: Jacob Huffaker

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Dr. Dan Boger
Co-Advisor

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will focus on the area of 802.20 wireless networking and how this technology will vastly benefit the US military forces, especially in the Network Centric concept of operations, where information flow is crucial. It will investigate this technology using published literature and previously gathered experimental data. This thesis will then relate its findings to Network Centric Warfare and the matters that could be most affected by this new technology.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to thank Dr. Alex Bordetsky and Dr. Dan Boger for their patience in dealing with his penchant for procrastination. LCDR Bill Parrish also contributed a great deal, sharing both data and explanations with the author. This thesis could not have been completed without these three individuals and their invaluable assistance.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

It has never been a secret that information superiority is the key to military victory. Military leaders have realized this for centuries. There is no substitute for knowledge of the battlespace. Yet, NCW, which utilizes information superiority as its key element, is a relatively new idea.

The reason that NCW has only recently been conceived is simply technology. Recently, technology has evolved at an unprecedented rate, giving birth to new platforms, new capabilities, and new threat scenarios. All this has transformed modern 'battle' into something new and previously unseen. These advances have brought about a situation where time and distance are, for all practical purposes, insignificant. Forces that are not in the same geographical location can still assist one another, and worldwide communications are virtually instantaneous.

However, with this increasingly powerful military technology comes increasingly powerful civilian technology as well. Television brings war to every living room. This intense public examination can cause events to be magnified out of proportion, either in a good direction or a bad direction. Therefore, military commanders have to pay extra attention to their target selections. Collateral damage is almost always unacceptable to the American public. This brings about a new judging point for the military. They are no longer critiqued for mission accomplishment, but now for mission accomplishment with

minimum force and losses. The military must learn to use its NCW assets to achieve more stealthy maneuvers, while at the same time keeping public expectations realistic.

In summary, the considerable recent changes in technology have produced this new concept, NCW. These changes have drastically impacted the military's manner towards information operations, acceptable information losses, and the detail of a given Common Operating Picture (COP). These have enormous implications on the very basics of warfare, and have caused this new outlook and stance.

B. PURPOSE

This thesis introduces the concept of Network Centric Warfare (NCW) to the reader and devotes a chapter to its explanation. It is rather crucial for the reader to realize that NCW is sufficiently vague and still 'in-progress', and this chapter-length explanation of NCW is not intended to be a complete defining work. Rather, it is intended to acquaint the reader with the purpose and reasoning behind NCW.

This study also introduces another new concept to the reader: 802.20 wireless networking. As this technology is also rather new, this thesis presents 802.20 in broad terms, rather than getting down into the minute detail. That is to say, this is a 10,000-foot view of 802.20, vice a more technical manual.

Once these two concepts have been introduced and explained, this thesis will address the benefits to the military of involving 802.20 in NCW. It will point out how

this new technology will benefit the military decision makers vastly more than the current technology (802.11).

C. SCOPE

This thesis seeks to answer a series of questions involving both NCW and 802.20:

What makes 802.20 different from 802.11?

What are the affected areas of NCW that this technology would benefit?

Is 802.20 capable of performing in military environments?

Can 802.20 offer more to the military than 802.11?

D. RESEARCH METHODOLOGY

1. Analysis of the current 802.20 protocol
2. Introduction to Network Centric Warfare
3. Comparison between 802.11 and 802.20
4. Proposal of expected benefits to NCW using 802.20

E. CHAPTERS OVERVIEW

Chapter I. – Introduction

Chapter II. – Definition and Explanation of NCW

Chapter III. – Explanation of 802.20

Chapter IV. - Vulnerabilities of 802.11

Chapter V. - 802.20 and the TNT Experiments

Chapter VI. – Conclusion

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORK CENTRIC WARFARE (NCW)

A. DEFINITION

Network Centric Warfare is one of those conceptually driven ideas that is not exactly concrete in its definition. However, there are some ideas and thoughts that repeatedly come up when discussing NCW. These ideas are listed below:

1. "Network Centric Warfare (NCW) is an information superiority enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledge entities in the battlespace." (Logan 2003).

2. "Network-Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and maneuver with precision and speed of response, value-adding command and control (C2) processes—to include high-speed automates assignment of resources to need—and integrated sensor grids closely coupled in time to shooters and C2 processes. Network-Centric

Warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography." (Cebrowski, 1998).

3. "A Warfighting Concept that enables a Network Centric Force to significantly increase combat power by achieving increased awareness, shared awareness, degree of interoperability, survivability, lethality, responsiveness, operational tempo, and ability to self-synchronize." (Alberts & Garcia, Dec 1999).

From the above definitions, it is plain that they share three common elements of NCW that should be focused upon. These are the reasoning behind NCW, the means of establishing it, and the desired outcome.

B. STRUCTURE

1. Underlying Reasoning

Network Centric Warfare relies heavily on having Information Superiority of the Battlefield. Information Superiority is attained when the information gathered by friendly forces gives them a clear and dominant advantage over all their adversaries. This Information Superiority can then be exploited to give friendly forces a decisive competitive advantage. This principle is the reasoning behind Network Centric Warfare.

2. Means

The question now becomes what is the way of reaching this advantageous position? What steps must be followed to ensure Information Superiority? In broad terms, access to all needed information sources must be granted and shared among all involved forces. In particular, sensors, shooters, and decision makers need to be linked to this information-sharing network. This infrastructure is complicated and deserves much more explanation, but for now, suffice it to say that these networks support the compilation and dissemination of common awareness.

3. Desired Outcome (Lim, 2004)

It is crucial to keep in mind that for a successful conversion from a platform-centric force, a different way of thinking must also occur with the changes in technology and networking. With the successful implementation of Network Centric Warfare, the information networking that can be achieved by the friendly forces will ultimately lead to an enhanced combat power. In particular, this enhanced combat power would be most visible in the following areas:

a. Decision Superiority

b. Dominant Maneuver

c. Precision Engagement

d. Focused Logistics

e. Full Dimensional Protection

C. ENHANCED COMBAT POWER

NCW is advertised as bringing with it an intense enhancement of the current combat power of any given platform-centric force. The following paragraphs break

this down into the five previously mentioned categories and provide documented evidence of this enhancement.

1. Decision Superiority

Decision superiority is an immediate result of having information superiority. When military forces have much more information at their disposal, much less guesswork is required to make the correct decision. However, having information superiority does not necessarily imply that one also has decision superiority. Rather, taking the given information and applying experience, training, and judgment leads to decision superiority. Also, it is not a capability of the individual in charge. It refers to the war fighting force as a whole, including the actual combatants, supporting staffs, and the efficiency of the communication back and forth between all involved.

2. Dominant Maneuver

Dominant maneuver is the ability of Joint forces to gain a positional advantage over the adversary with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks (US JCS, 2000). NCW enables this dominant maneuver through timed coordination of units, gathering of intelligence and feedback, and the anticipation of events leading to mission success. These allow for the concurrent movement and massing of forces that are widely dispersed, as well as the coordination of their fire, thereby achieving the objective of dominant maneuver.

3. Precision Engagement

Precision Engagement is the ability of Joint Forces to locate, survey, discern, an track objectives or targets; select, organize, and use the correct systems; generate

desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required throughout the full range of military operations (US JCS, 2000)

NCW greatly enhances a force's ability to acquire and engage targets with both greater precision and at a reduced risk to one's own assets. This is achieved through improved situational awareness and cooperative sensing. NCW enables firepower to be much better coordinated by using a high performance cooperative network of sensors. No longer do combat aircraft have to depend solely upon their organic sensors for weapons delivery. In NCW, the aircraft can make use of other sensors, thus staying stealthy for a longer period of time, therefore increasing the element of surprise, mission effectiveness, and certainly its own chance of survival. Now each platform can make use of information that far exceeds its own respective organic assets.

4. Focused Logistics

Focused Logistics is the ability to provide the Joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity across the full range of military operations (US JCS, 2000). A real-time, Internet based information system is used by NCW to boost this capability. It provides total asset visibility as part of a common operating picture that is viewed by all other participants in the battle space. This has the effect of linking the operators with the logistics and support units, thus intensifying the efficiency of the fighting force as a whole.

5. Full Dimensional Protection

Full Dimensional Protection is the ability of the Joint force to protect its personnel and other assets required to decisively execute assigned tasks (US JCS, 2000). This is achieved through applying a multilayered defense mechanism in both the active and passive domains. Since the capabilities of sensors and weapons are rapidly increasing with time, geographical location of forces tends to lose importance, as forces no longer have to be in the same area to assist each other with the mission. NCW uses this to both augment sensor power as well as to minimize risk, since assets do not have to be geographically located close to each other.

D. MEASURES OF SUCCESS

To make NCW a viable decision, a number of key features must be present. These are having the organization focused on the same goal, establishing a modern and freethinking environment, and establishing viable measurements of effectiveness (MOE) for NCW.

1. Focused Goals

As is the case in any major organization planning to make a drastic shift in policy, having everyone prepared and focused along the desired goal is crucial. The commitment of not only the decision makers, but also everyone, down to the shooters and support staff, must be firm and resolute. This is because the effort required to shift a doctrine from a platform-centric institution to a network-centric one is one that will take quite some time. For that reason, there must be an alignment of attitudes throughout the military.

2. Promoting a Successful Environment

With all the technological advances that have been discussed, it is important to notice that in order to employ these technologies to their maximum ability, there must exist a climate accommodating to this technology. That is, if a climate of innovation and progressive thinking is present, it will result in creative new and better ways of accomplishing missions and mission objectives. Although it is much easier said than done, the military must learn to discard its old planning methods and strategies, and apply new, more modern plans that incorporate all the aspects of NCW. Success in implementing NCW not only depends upon the proper technology advances, but also the proper methods of applying these changes. The military must implement new network-centric ways of operating that use the full spectrum of the technologies involved.

3. Infrastructure

To be a success, NCW must have a secure and coherently networked infrastructure. Without this seamless and robust infrastructure, network-centric operations simply cannot be performed. Realistically, performing network-centric operations without the proper infrastructure in place will probably compromise the mission much more than it would assist it. Therefore, it is obvious that before its implementation, there must be an effort to develop and establish the proper infrastructure. While involved in this process, there must be serious consideration given to the cost-effectiveness of proposed solutions. While financial prudence is a good trend to follow, system requirements must not be compromised simply to meet expense

goals. Especially in NCW, where technology is a keystone, systems level requirements must be planned and achieved. Of course, that's not to say that open source and off-the-shelf technology should not be used at all, just not when the performance of the system is at stake.

4. Measures of Effectiveness (MOE)

As with any new system, it is vital that goals be realized before the actual implementation of the project. The value of various investments toward NCW must be established, and there must be a method of establishing progress using both explicit and indefinite measures. In measuring NCW goals, one must make certain to differentiate between functional requirements and quality attributes that are more desired than needed. There are a number of methods and metrics for the evaluation of MOE. One of the more common methods is shown in Figure 1 below.

The figure consists of five basic levels of measures. At the first level, the performance of each command and control system, combined into one infrastructure, is measured. This refers to the computation power and ability to transmit or distribute information, that is, connectivity and bandwidth. This level of measurement does not automatically translate into increased mission effectiveness. The other end of the measurement hierarchy is the measurement related directly to mission effectiveness or utility. For combat operations, common measures that have been employed have included attrition rates, fratricide, leakage, and time to accomplish a given mission (Alberts et al., 1999)

Figure 1: Hierarchy of Measures of Merit (From: Alberts, D.S., Garstka, J.J. & Stein, F.P. 1999. Network Centric Warfare: Developing and Leveraging Information Superiority. 2nd Edition. CCRP.)

E. SUMMARY

It should be clear to the reader that Network Centric Warfare is by no means linear and straightforward. Rather, it is cyclical and reiterative in nature. Concentrated evolution and constant adjustments are required to shape this concept as it proceeds further into the future. Without superb leadership, organizational commitment, and a robust infrastructure, the focus of NCW could get lost in all the minutiae. The military needs to constantly monitor NCW and its development to ensure maximum effectiveness on the battlefield.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE IEEE 802.20 STANDARD

A. OVERVIEW

1. 802.20 Working Group

At this juncture, it is important to note that as of the writing of this thesis, 802.20 is not official. That is, it is not a standard approved by the IEEE, such as the more commonly used 802.11. In December of 2002, the IEEE Standards Board approved the establishment of IEEE 802.20, the Mobile Broadband Wireless Access (MBWA) Working Group. This group's task is to develop the specification for an efficient packet based air interface that is optimized for the transport of IP based services. The goal is to enable worldwide deployment of affordable, ubiquitous, always on and interoperable multi-vendor mobile broadband wireless access networks that meet the needs of business and residential end user markets. They have set the following as their scope:

"Specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5 GHz, optimized for IP-data transport, with peak data rates per user in excess of 1 Mbps. It supports various vehicular mobility classes up to 250 Km/h in a MAN environment and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than achieved by existing mobile systems (ieee.org, 2005)."

2. Flarion

Flarion Technologies is one of the key members of the 802.20 Working Group, and they have provided NPS with

802.20 technologies and equipment to be used in the Tactical Network Topology (TNT) experiments. The TNT experiments will be discussed in greater detail in Chapter Five. Therefore, from this point in the thesis, it will be Flarion's 802.20 technologies that will be discussed.

B. EXPLANATION

1. Overview

The 802.20 system is a fully IP-based, packet-switched wireless network. As illustrated in Figure 2, the Flarion system philosophy is quite simple:

(a) Provide an efficient and secure air interface (radio access) to support IP-based information exchange,

(b) Design the radio access to seamlessly connect with IP-based routers

(c) Reduce the latency to create a TCP / IP –based application friendly environment.

The system can operate in frequencies from 400 MHz to 3.5 GHz. For trials, the wireless system operates in the 700 MHz band. This relatively low frequency compared to 2.4 GHz and 5.2 GHz (both ISM bands) enable the system to provide better RF propagation characteristics. It supports various vehicular mobility classes up to 250 km/hr and targets spectral efficiencies, sustained user data rates and numbers of active users that are all significantly higher than achieved by existing mobile systems (Power, 2004)

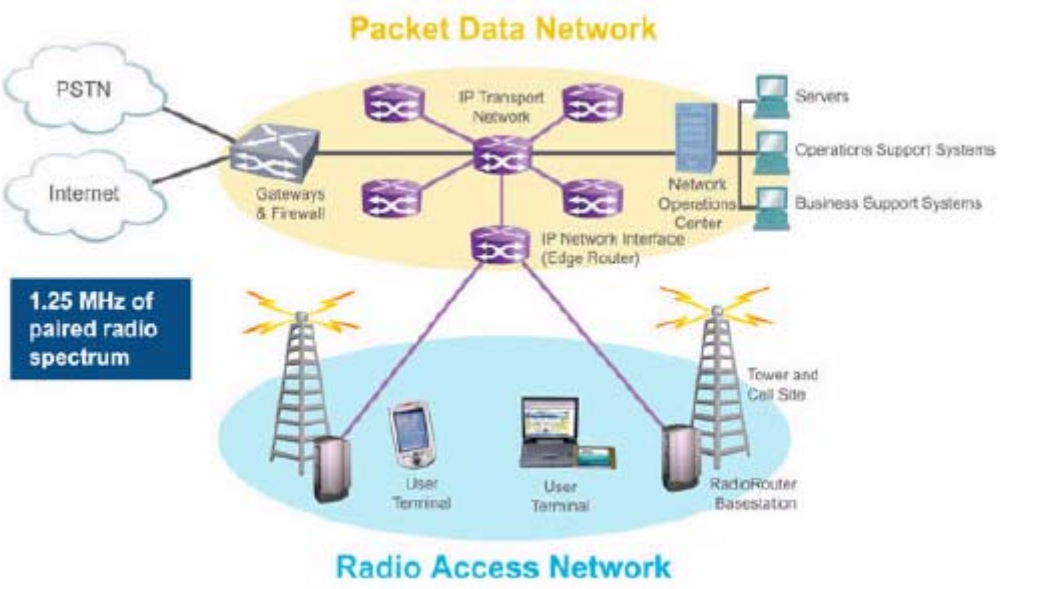

Figure 2: 802.20 System Concept (From: Michael T. Lander, "Flash-OFDM Technical Update," Signals Ahead, Vol 2, No.3, 7 Feb 2005.)

2. FLASH-OFDM

Flarion's technology makes use of an encoding scheme called FLASH-OFDM. Like its predecessors, TDMA and CDMA, FLASH-OFDM is an air interface technology designed for wide area networks in the licensed spectrum. However, unlike its predecessors, the FLASH-OFDM system is pure-IP and packet-switched, delivering broadband data and voice to a greater number of mobile users.

The emerging success of the FLASH-OFDM mobile communications network can be attributed to its high-speed downlink and uplink, and low latency performance replicating a wired broadband experience. Based on Orthogonal Frequency Division Multiplexing (OFDM), FLASH-OFDM segments a wireless communications channel so that many users can share it. Segmenting according to frequency rather than time or codes (TDMA and CDMA respectively), FLASH-OFDM uses fast hopping across those tones to create a

highly secure and high capacity Physical Layer (wireless pipe). This Physical Layer is vertically integrated with innovative control layers (MAC and Link Layers) to create a fast, reliable, and efficient process of moving data and voice packets wirelessly. Finally, the FLASH-OFDM Network Layer utilizes an all-IP and packet-switched infrastructure to route those packets in a cellular environment.

3. Low Latency

Latency is defined as the time it takes for the network to respond to a user command. If latency is high, causing noticeable delays in downloading web pages, then the experience feels nothing at all like broadband, no matter how high the data rates are.

In terms of latency, the Flarion packet-based technology has an edge over current 2.5G and 3G technology. In a recent trial with Nextel, the Flarion system registers a latency of 80 milliseconds. Contrast this to a Qualcomm CDMA-2000 EV-DO ("Evolution – Data Optimized") system that generally registers latency of 400 milliseconds. In general, since the Flarion system is a packet-based system, it has a lower latency compared to 2, 2.5G technologies that are circuit-based in nature. Circuit-switched systems require end-to-end setup latency, which is not suitable for instantaneous packet traffic (Power, 2004).

4. Quality of Service (QoS)

QoS is defined as a collective measure of service delivered to the customer, and can be characterized by several basic performance criteria such as availability, uniformity, error performance, response time and throughput. Flarion places its QoS feature over the air link, thereby supporting fast and intelligent packet

scheduling at the point of delivery in a way that can optimize IP QoS delivery for the operator and customer.
Not only does Flarion provide QoS on the downlink, the network allows for a unique, non-contention based uplink that allots a different level of access to each packet, causing traffic to flow in an orderly manner. Air link QoS also allows for multi-tiered marketing, where users are classified in Platinum, Gold, Silver or Bronze designations to share specific resources, with more resources being allocated per mobile device for higher service levels (Flarion QoS, 2003).

5. Wireless Security

Wireless networks are inherently less secure than wired networks. This is because in the wireless network data is transmitted over an open medium (air). This permits eavesdropping on the communication between two wireless devices simply by being in the area. Since wireless transmissions are, in effect, just radio waves, placing an RF receiver in the general area of wireless communications will allow a user to pick up, or 'sniff' wireless traffic in the area. This has always, and probably will always, be a major concern to wireless network providers and operators.

a. Layered Security (Flarion Security, 2003)

FLASH-OFDM provides security for wireless traffic. It is discussed below, differentiated by the different network layers.

Air Link Layer Security

The FLASH-OFDM link layer security deals with protecting the air interface between the wireless device

and the network access node. This is the task of the link layer, and it may involve authentication, encryption or both.

First, the link layer protocol may specify an authentication protocol by which the identity of the communication device(s) is verified. Traditionally, the wireless device needs to prove its identity in order to obtain network access. This is referred to unilateral authentication, and is meant to thwart device cloning (theft of service). However, there has been recent interest in protecting the wireless device from rogue access nodes. Through mutual authentication, the wireless device can also verify that the access node through which it desires to communicate is indeed legitimate.

Second, the link layer may specify an encryption algorithm for user data and/or signaling data. Traditionally, in packet-based networks such as the one discussed in this thesis, encryption is applied to link layer frames over the air link. A symmetric key (rather than a public/private key) algorithm is normally used, meaning that the same key is utilized to encrypt and decrypt data. In addition, the encryption algorithm should not be computationally burdensome to the wireless device, which is power and memory-limited. Encryption keys should always be linked to the authentication phase, as encryption without authentication opens the door to security attacks.

Third, key management for the FLASH-OFDM system is achieved most often with the aid of a backend security server, which stores secret information associated with devices and users, and aids in the authentication task. Of

the aforementioned aspects, strong authentication of the user device is the paramount link layer security requirement. It is necessary to prevent device cloning and to ensure proper accounting and billing.

Network Layer Security

End-to-end security is the only acceptable form of security for commercial and enterprise communications. Therefore, the Flarion security architecture also calls for security features above the link layer in order to achieve end-to-end security. End-to-end security consists of protecting the communication path between the applications or network stacks at the two (or more) communicating end nodes. For example, it is desirable to secure the communication between a user performing online banking and the network server associated with a financial institution.

To address security concerns that affect multiple protocol layers and applications, an enterprise can cost-effectively employ end-to-end security at the network layer. A typical example is an enterprise that provides a Virtual Private Network (VPN) for its remote users to securely access its network (via a public, unsecured network). Network layer security also involves three aspects: authentication, encryption, and key management. A commonly used network-layer security standard is IPSec (Internet Protocol Security). IPSec is applied at the IP layer of the TCP/IP stack, providing authentication and encryption of each packet, using keys negotiated between the two endpoints. Additionally, network security deals

with protecting the network nodes from attacks within the wired network, such as denial of service, spoofing, and network intrusion.

Application Layer Security

An application requiring specialized/additional authentication or encryption support, or those that may need to run over networks unsecured by end-to-end means also employ their own end-to-end security. Several security mechanisms have been developed for application usage such as electronic mail (PGP, S/MIME), client/server (Kerberos), electronic transactions and Web access (SET/SSL), and remote login (SSH). Pretty Good Privacy (PGP) provides confidentiality and authentication service for electronic mail and file storage applications. Kerberos is a traditional method for authenticating users-to-servers and servers-to-users using a central server. Secure Sockets Layer (SSL) uses TCP to provide reliable end-to-end service to other applications such as Web client/server interaction (e.g. HTTP). Secure shell (SSH) is used for securing remote access links via IP networks. The newest version, SSH2, provides encryption of user names and passwords, authentication of users/clients and servers, and tunneling of applications/ports based on TCP/IP.

b. Security Requirements and Solutions

By virtue of being developed far after 802.11, 802.20 has the distinct advantage of picking and choosing parts. That is to say, 802.20 can incorporate those aspects of 802.11 that are useful and secure, and make extra efforts to reinforce security where 802.11 has shown vulnerabilities.

One of 802.20's ultimate goals is having fast hand-offs, so the security solutions have to maintain this baseline while providing a more secure connection. 802.20 is also charged with meeting current Department of Defense requirements for protection of sensitive but unclassified information.

The security solution chosen by the 802.20-working group is an AES-CCM based solution. This solution is the only algorithm/mode pair that the group felt supported all of 802.20's pre-determined operating characteristics. As the author is not in any way a computer security expert, this thesis will not discuss this solution in detail. It will; however, try to provide an overview of the solution.

The Advanced Encryption Standard (AES) is a block cipher, and it can be used in many different modes. A block cipher is a symmetric key cipher, which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take a block of plaintext as input, and output a corresponding block of ciphertext with the same number of bits as the plaintext input. The exact transformation is controlled using a second input – the secret key. Decryption is similar: the decryption algorithm takes a block of ciphertext together with the secret key, and yields the original block of plaintext.

The CCM (Counter with CBC-MAC) is one mode of operation for the AES block cipher. The 'counter' mode describes an encyption method that essentially turns block ciphers into stream ciphers by encrypting successive values

of a given counter. The counter can be any simple function that produces a random sequence that is designed not to repeat itself. CBC-MAC stands for Cipher Block Chaining-Message Authentication Code. This is a message integrity method that encrypts each block of plaintext with the cipher, and then XOR's that ciphertext with the second encrypted block. That result is XOR'd with the third encrypted block, and so on in series (ieee.org 2005).

When AES is used in the CCM mode of operation, the security of the transmissions is very formidable, which is one of the reasons why the 802.20-working group chose this particular solution. As you can see, this creates more security for the wireless transmissions, while maintaining the mobility and speed requirements that 802.20 is based on.

C. CONCLUSION

As has been shown in this chapter, 802.20 offers a new alternative to the wireless networking world. It is more robust, more secure, and offers a variety of other options simply not available anywhere else at the present time. Especially given the military's unique needs and specifications, this Flarion 802.20 system would certainly be well employed in any given situation and circumstance.

IV. FAULTS OF 802.11

A. INTRODUCTION TO 802.11

1. Background

The IEEE 802.11 standard is extremely popular and used worldwide in wireless networks. Virtually without exception, whether it is a campus lab or an office building wireless LAN, the standard governing its performance is 802.11. The military uses 802.11 as well just as often as everyone else. The IEEE 802.l1 standard is very successful. The 802.11 market share is estimated at $2.2 billion for 2004 and $3 billion by 2007. That means that by 2007, approximately 30 million units will be shipped. Equipment compatible with this standard operates in the ISM band. The ISM band is frequency ranges that do not have to be licensed with the FCC for use. This means that operations of 802.11 networks are virtually free, unlike Third Generation (3G) cellular networks that cost operators billions of dollars just to secure the necessary bandwidth for 3G operations. The rapid rise of 802.11 could be attributed to this “free” status which results in a much lower cost of initial investment, roll-out costs, and therefore, a much more rapid rate of investment return (Parrish and Tovar, 2005).

2. Versions

802.11 standards come in 3 flavors: 802.11a, 802.11b and 802.11g. 802.11b provides 11 Mbps of link rate with the 2.4 GHz frequency band, while 802.11a and g provides 54 Mbps of link rate at 2.4 GHz and 5.2 GHz frequency bands respectively. With each new generation of 802.11, the link

rate has increased tremendously. The next generation of 802.11, 802.11n, is expected to reach 1 Gbps.

3. Result

For the military, this enormous wireless link rate and its relatively low cost is indeed too good to be true. Despite all its advantages, 802.11 standard was designed for ad hoc deployment, with nearly no protection from other wireless emitters (especially since it is in the unlicensed band) and no consideration for quality of service. Its main objective was a simple design that would result in very low-cost chipsets. By 2003, the cost of 802.11b chipsets are priced at 4 dollars and 802.11g chipsets are 9 dollars.

With this in mind, it is expected that the market forces will continue to push 802.11 standards along the same direction. That is, since the market is driving the cost lower and lower, then the vendors will make these low-cost chips. Unfortunately, this comes at the cost of quality and security. Despite the interest of the military on 802.11 standards (partly because of its low cost and high link rate), there is very little the military could do to influence the design and/or the market decisions of future 802.11 standards.

B. VULNERABLILITY

1. Security

The potential vulnerability of 802.11 is wireless security, which is of extreme importance to the military, for obvious reasons. The below Figure 3 shows the flow of information an enemy would employ to gain control or shut down an 802.11 network.

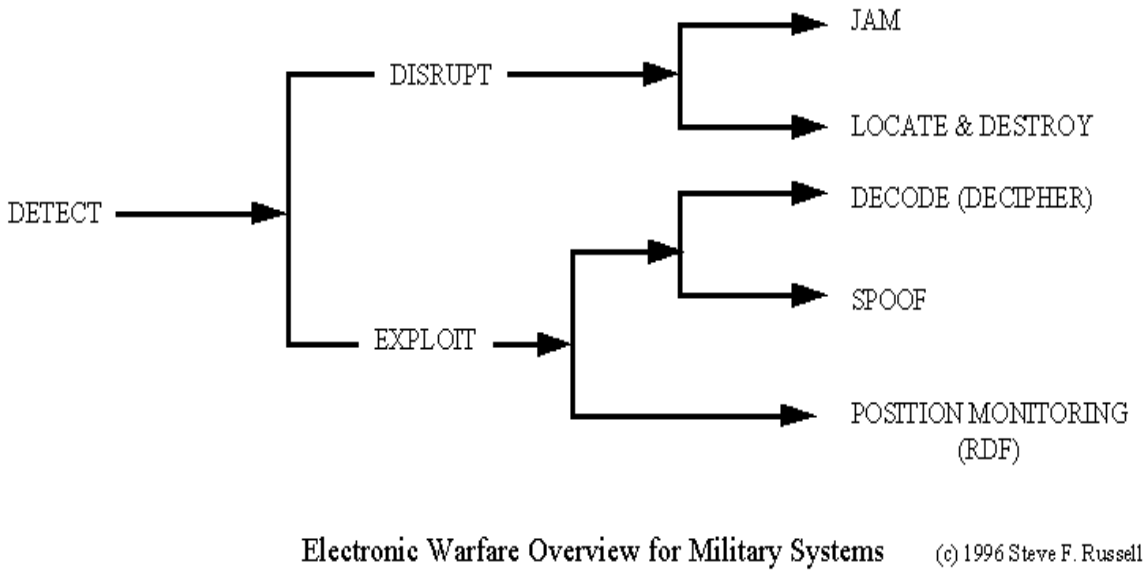

Figure 3: Electronic Warfare Overview for Military Systems. (From: Russell, Steven, F. 1996. "Wireless Channel Security Overview." <http://www.public.iastate.edu/~sfr/wireless/w_tut_1.html> [20 July 2005])

C. POSSIBLE ATTACKS

1. Detect and Exploit

802.11 signals can both be disrupted and exploited. At the heart of this vulnerability is the fact that 802.11 is an open standard – its frequencies, modulation, link layer and media access layer formats are all known – and an enemy could leverage this knowledge to detect such a signal and proceed to leverage advanced digital signal processors and digital signal processing techniques to jam, locate, decode, spoof and position monitor the signal. For a military system, any and all of these options are completely unacceptable.

2. Smart Jamming

It is almost ridiculously easy to interfere with an 802.11 signal, and consequently, jam it. For example, when a 802.11 compliant terminal receives an RTS ("Request to Send") signal, it has to observe radio etiquette and not contend for the wireless channel. This is actually a clever feature of 802.11 to share wireless spectrum and improve the efficiency of channel contention (by reducing collision possibility and in some cases, reduce the hidden node problem). However, an adversary could easily exploit it by continuously sending out an RTS signal. This would case all terminals in the network to fall silent and not send any traffic. And since the network is not being used for sending traffic, it is effectively jammed. Since the RTS signal is sent in the clear and not encrypted, there is very little the military could do to avoid this shortfall.

3. Denial of Service (DoS)

Even with security features such as Wired Equivalent Privacy (WEP) turned on, an adversary could still spoof a genuine user and subvert the authentication process. The adversary need not try anything fanciful in order to bring down the network. All they have to do is to insert false routing table update messages into the network to create a topology oscillation that has two effects:

a) Every packet contains a Time-to-Live (TTL) value. This value determines how many routers the packet is passed through before it is erased. These false messages would be routed around the network for a long time, during which they could cause sufficient network congestion to effectively render the network inoperative.

b) More network routers could flood the network with control packets to discover and establish new routes. This would have the same effect of denying service to legitimate users since these control packets would have priority and would take an extremely long time to pass through.

D. SHORTFALL – CAPACITY AND COVERAGE

1. Multipath

Multipath propagation occurs when an RF signal takes different paths when propagating from a source to a destination node. While the signal is en route, walls, chairs, desks, and other items get in the way and cause the signal to bounce in different directions. A portion of the signal may go directly to the destination, and another part may bounce from a chair to the ceiling, and then to the destination. As a result, some of the signal will encounter delay and travel longer paths to the receiver.

802.11 is vulnerable to multipath. This is because the 802.11b standard is based on Direct Sequence Spread Spectrum (DSSS). Orthogonal Frequency Division Multiplexing (OFDM) is proven to be more resistant to multipath. This is demonstrated amply in the Digital Video Broadcast – Terrestrial (DVB-T) deployment in Singapore where 5 base-stations are used to cover a densely built-up environment like Singapore across an area of 50x40km. As shown in Figure 4 below, the receivers are installed on public buses that ply roads with 12-14 story buildings on both sides of the road. The picture quality for the streaming video is usually good to excellent with occasional poor or stalled video reception when the bus approaches a “deep fade” zone.

Figure 4: DVB-T deployment for mobile reception of TV broadcast. (From: 2004. “Technology in Focus: Digital Video Broadcast - Handheld (DVB-H).” < http://www.ida.gov.sg/idaweb/> [20 June 2005])

2. Frequency Reuse

Early 802.11 products employed static frequency assignments and frequency pre-planning to de-conflict the use of frequencies across different Access Points (AP). If no reuse existed, the AP’s and terminals would interfere with each other across AP coverage cells. The dark overlap regions in Figure 5 represent interference in 802.11-based networks from adjacent cells.

The frequency reuse factor is a figure of merit for network capacity in a network with spectrum resource constraints. The lower the frequency reuse factor, the better is its ability to convert scarce frequency spectrum

resource into network capacity, i.e., more subscribers, or higher data rate per user for same subscribers supported.

Both early and current 802.11 products have a frequency reuse factor much greater than 1. 802.11a & g products have improved frequency reuse factors that are in the range of 4-6. (If the network is designed for higher / peak data rate performance, and operated in an indoor environment where the RF multipath is severe, the reuse factor could be as high as 16-19.)

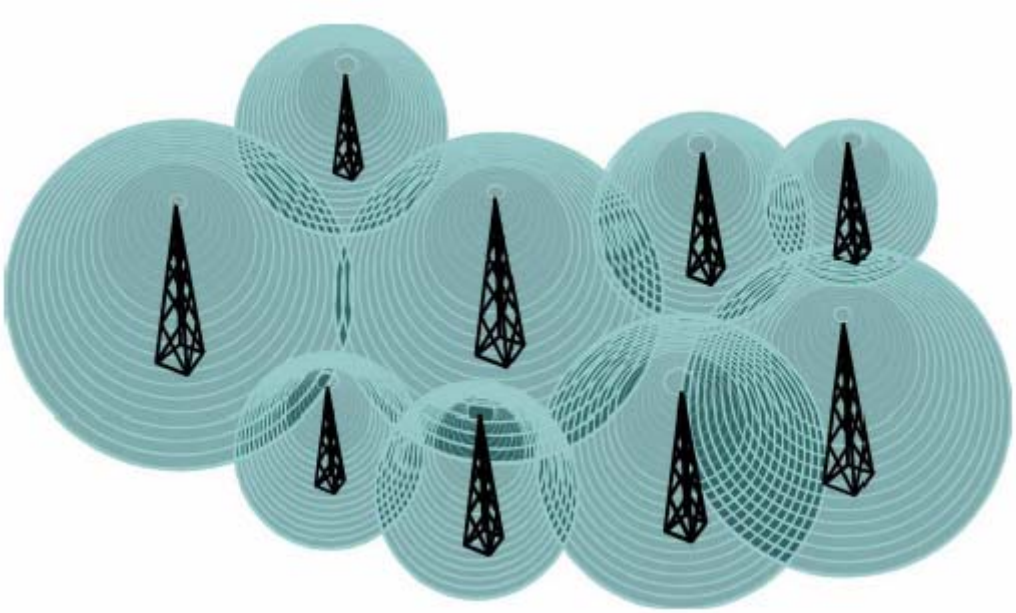

Figure 5: Interference across Cells(From: Kim, J. & Leung, K. (2002). “Frequency Assignment for Multi-Cell IEEE 802.11 Wireless Networks.” AT&T Research.)

3. Frequency

The 802.11 compliant products are usually operated in the ISM band of 2.4 and 5.2 GHz. These frequencies limit its ability to operate extensively in non line-of-sight environments, especially when diffraction of the RF signal due to obstructions are dominant in the degradation of the

RF signal, i.e., operations over a mountain, across a forest of tree canopy, a cluster of buildings etc. Again, the deployment of DVB-T in Singapore within the 600 MHz frequency band demonstrates the tentative advantage of operating in a lower frequency if better range and coverage is desired in an urban environment with many obstructions to clear, line-of-sight signal propagation. For the abovementioned reasons, 802.11 technologies are far from ideal for robust military communications in an urban environment.

V. 802.20 AND TNT

A. BACKGROUND

The Tactical Network Topology (TNT) experiments are carried out each quarter. Experiments were conducted at both Ft Ord's MOUT (Military Operations in an Urban Environment) facility and Camp Roberts near Paso Robles. In the TNT 05-02 phase, there were three separate experiments carried out which focused primarily in integrating connectivity of 802.20 into the existing architecture of TNT. The full description of all three experiments is contained in the Appendix to this thesis.

The purpose of this series of experiments was:

- Operationally test 802.20 while connected to the Tactical Network Topology's infrastructure
- Demonstrate through wall capability of 802.20
- Demonstrate non line-of-sight (NLOS) capabilities of 802.20
- Demonstrate connectivity of mobile users while at speeds in excess of 90 mph

The Cell on Light Truck (COLT) vehicle owned by Flarion Technologies provided network availability. The vehicle is a highly mobile network provider that contains all the elements necessary for a wireless 802.20 network, including: an omni-directional antenna, base station, AAA server and a connection to the backhaul network.

B. MOUT EXPERIMENT

While at the MOUT, mobile-to-mobile through-wall communications with PDA's was successfully demonstrated. A site survey was also conducted to observe Non Line of Sight

(NLOS) behavior. The experiment's purpose was to demonstrate the through-wall capability of 802.20 and its mobility within an urban environment. Since all the buildings in the MOUT are constructed out of cinder blocks, the test of through-wall penetration would be an appropriate scenario for a real-world result.

Figure 6: The MOUT Facility at Fort Ord (From: Parrish & Tovar, 2005)

To begin the experiment, two PDA's were placed in the basements of two different buildings. There was a bullet on the ground in one of the basements. The PDA in that basement was to take a picture of the bullet, and send that, along with an audio warning, to the second PDA, which was in the other basement. This experiment was completed very successfully, with the receiving PDA able to receive the warnings along with the transmitted picture of the bullet without any difficulty.

Figure 7: PDA receiving picture of bullet (From: Parrish & Tovar, 2005)

For the next phase of the experiment, one PDA was placed in a sewer pipe of approximately 30 feet in length that connected two buildings. The sewer pipe was approximately eight feet below the ground in one of the cinder block buildings of the MOUT. The other PDA was outside of the building. Although the connection strength was low between the two PDA's it was still a successful test, as there was quite an impressive barrier separating the two devices.

C. CAMP ROBERTS CAMERA EXPERIMENT

The second experiment was conducted at Camp Roberts. This experiment involved the COLT again, as well as two wireless cameras, one mounted on a tripod on the ground, and another web enabled camera attached to an aerial balloon at approximately 1000 feet of elevation. The purpose of the experiment was to demonstrate the ability of the 802.20 network to capture and send these captured images back to the Tactical Operations Center (TOC). The

measure of success in this experiment was the clarity of the captured images as received by the TOC.

The camera mounted on the aerial balloon was to monitor a certain road, and detect any vehicular traffic on this road. The balloon was approximately 4 miles from the TOC, where the live video feed was viewed. The results were very positive. The received video in the TOC was clear, and observers were able to see a moving vehicle come into the area and leave again.

The camera mounted on the tripod was to get a closer view of any vehicles located by the balloon mounted camera. It had a remote control that allowed the user to pan, tilt, and zoom the field of view. It was located approximately one mile from the base station, but was completely NLOS as well. Once again, the resulting picture capture, as you can see below in Figure 8, was successful. The camera was able to follow the vehicle as it progressed down the road, and observers were able to glean much more information about the vehicle than from the balloon-mounted camera.

Figure 8: Captured Image from Tripod-Mounted Camera (From: Parrish & Tovar, 2005)

D. CAMP ROBERTS RUNWAY EXPERIMENT

This experiment was also located at Camp Roberts, but had a different orientation. This time, the ability of the network to handle high speed was tested. The experiment was conducted on a runway. There was a mobile IP camera located at one end of this runway, with a user and laptop at the opposite end. There was another user on the network with a laptop and camera inside a vehicle on the runway. This vehicle would start at the end of the runway with the other user, and drive towards the IP cam at the other end of the runway. At the same time, the two users would engage in a full duplex audio and video conversation via the 802.20 network. The successfulness of this experiment was measured in the ability of the network to rapidly adapt to a high rate of speed of a user, and also in the quality of the video of the IP camera.

Figure 9 below is a screenshot from the laptop of the second user, the one located at one end of the runway. You can see the two videos present on the screen, as well as a diagnostic tool that is monitoring the transmission and receiving rates of the laptop.

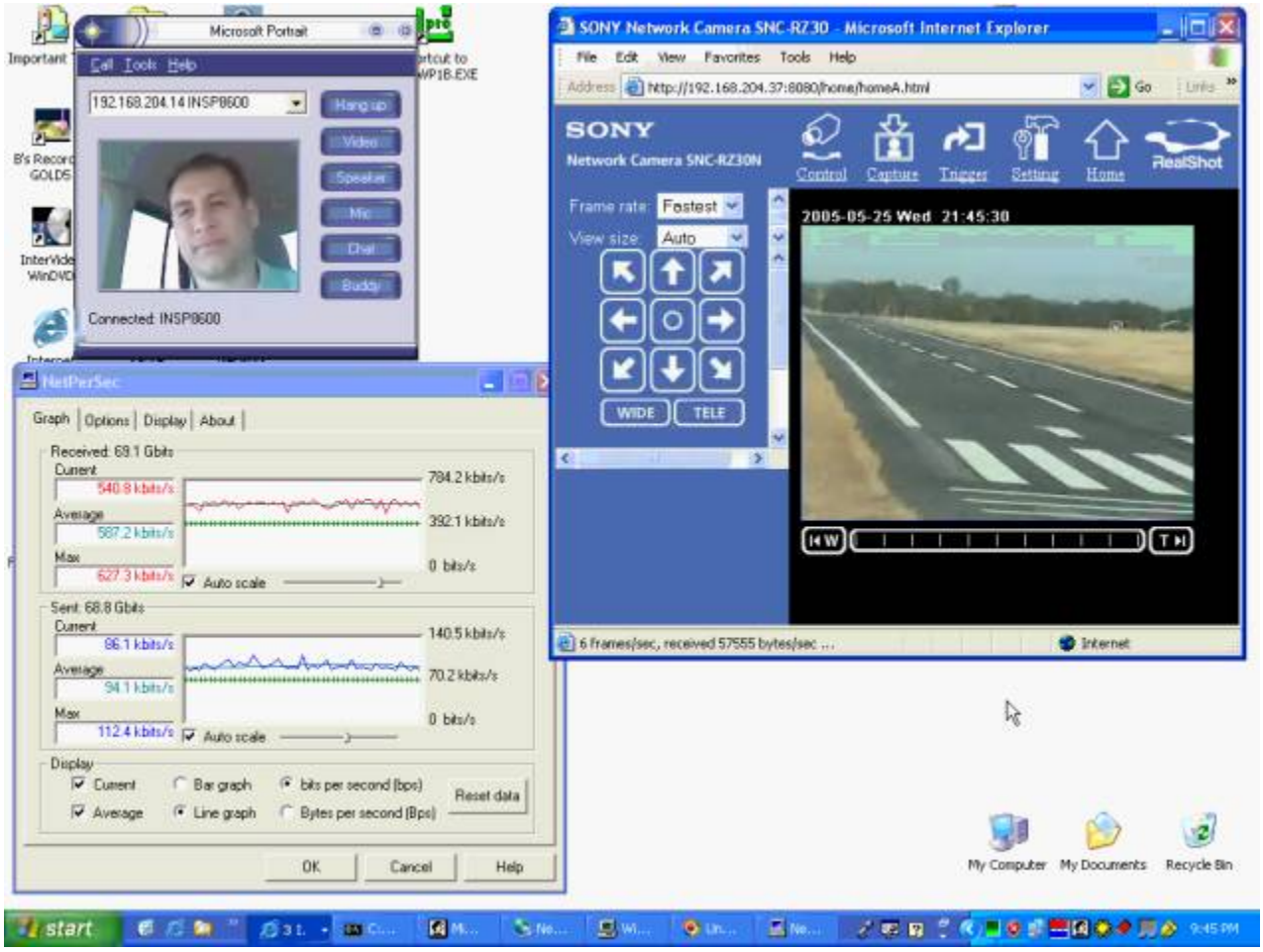

Figure 9: Screenshot of Laptop Located at one end of Runway (From: Parrish & Tovar, 2005)

From the diagnostic tool, called NetPerSec, one can see that the average receiving rate is 587.2 Kbps, and the average transmission rate is 94.1 Kbps. Since this is

while maintaining two video links, one that is full duplex audio and video, these results are extremely good.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. OVERVIEW

Given the ever-increasing pace of technological advances it becomes clear that 802.11 will no longer continue to offer a satisfactory level of service to military forces worldwide. Especially in today's modern Network-Centric military, where mission success depends upon wireless network connections, this thesis has shown that 802.20 simply offers a more viable solution that 802.11.

B. KEY COMPONENTS

1. Security

The wireless networking aspect that the military is most concerned about is wireless security. 802.11 was just not created with security in mind. On the contrary, it was created for the purpose of sharing information between wireless devices; security on 802.11 came to be almost as an afterthought. For military missions to be successful, a certain element of stealth has to be present. If the enemy is able to monitor wireless communications, and even worse, intercept wireless communications, then mission success gets less and less probable.

802.20 has the added advantage of being developed at the present time. The developers are aware of the 802.11 vulnerabilities and available exploits, so 802.20 is already more secure than 802.11 already, even though it is not actually official as of yet. Of course, add to that

the additional layers of security (as discussed in this thesis) that are included in the 802.20 protocols, and the resulting level of security in 802.20 is vastly superior to 802.11.

Technology has allowed the military forces to act and respond to any given threat quickly due to faster and wider bandwidth for communications. This wider connectivity allows the military to expand their command and control networks to span a much farther area of responsibility than for which they have previously been utilized. While this enables the forces to have a drastically higher combat effectiveness, as shown previously in this thesis, this also puts a vast amount of sensitive data on these command and control networks. If the networks were compromised and this valuable data and information were to get to the enemy, then mission effectiveness and the lives of the soldiers would be at risk. Since 802.20 brings with it a much more solid and secure infrastructure than 802.11, security wise, it is the obvious choice.

2. Mobility

As previously mentioned, 802.20 incorporates high-speed handoff into its requisites. Flarion specifies speeds of up to 250 kilometers per hour. This means that platforms traveling at speeds at or below this mark could still employ 802.20 without getting messy with the handoffs between cells. This has huge advantages over 802.11, which does not support mobility much at all. Ships, ground forces, and aircraft, all moving at relatively high speeds could still manage to communicate using any variety of methods available. This enables these groups of platforms

to remain on the network, feeding information into the Common Operating Picture and contributing to the overall objective of Network Centric Warfare. Since 802.11 does not support this high-speed mobility, this would be an enormous advantage to NCW, enabling more platforms to be linked together over the same network.

This added mobility associated with 802.20 equipment and networks greatly adds to the war fighting capabilities of any given force structure. 802.20 is focused on full mobility as a differentiator. In addition, 802.20 is designed to operate in small portions of the spectrum. Spectrum lower on the band is the most ideal for wide area and mobile networks but is largely used up, except for small portions. The 802.20 standard uses those small pieces of spectrum lower on the band. This use of frequency portions is part of what allows 802.20 to provide such mobility in its networks. This added mobility is what will allow various military platforms to stay connected on the same network even at high speeds.

3. Frequency / Through-Wall Capability

Flarion's 802.20 equipment operates at 700 MHz. 802.11 technologies operate at 2.4 GHz and 5 GHz. This lower frequency opens up many options in the Network Centric Warfare arena. Since it operates at a lower frequency, it has a much better penetrating range. Recall the discussion presented in the earlier section with the connectivity in the concrete sewer at the MOUT facility at Fort Ord. The two PDA's were still connected even with so much concrete and earth separating them. This through-wall capability is unique to 802.20. 802.11 has limited

through-wall capability, since it operates at a much higher frequency. This higher frequency is unaffected with LOS transmissions where there are few barriers. However, with 802.20, since it operates at a much lower frequency, the transmissions attain the through-wall capability that can prove to be extremely useful in combat situations. Maintaining connectivity throughout a period of time is extremely useful, especially in combat situations, where instantaneous reports often mean the difference between life and death. Having this connectivity would vastly increase the military's range and power, as well as make it safer for the end user.

APPENDIX

Naval Postgraduate School Field Experiment TNT 05-02 (802.20)

SCENARIO: ON-THE-MOVE NETWORK PERFORMANCE AT MOUT FACILITY

Assumption

Future SOF and Marine Corp operations will require the use of an on-the-move network between multiple, dissimilar manned and unmanned assets to include air to provide situational awareness and enhanced warfighting capabilities. These assets could include UAVs (micro, small, tactical, strategic), manned and unmanned aircraft, and squad personnel with advanced video/audio capabilities. Some assets might be permanent while others may rapidly join and leave the area. Network mobility is a necessity driven by target mobility. An integrated network for all assets and the TOC is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of UAVs and other assets utilizing a minimum number of operating personnel.

Basic Requirements

- Local C3I using multiple assets with rapidly changing participants and network node locations
- Network that permits control of multiple assets as well as rapid insertion of new assets
- Situational awareness and common operational picture

Experiment/Demonstration Technologies

- "On-the-move" network.
- Local and remote location SA from multiple assets

Capabilities/Assets

- All 802.20 tactical equipment connected to 802.20/OFDM network

- TOC and MV and experimenter with SA

Experiment Variables

State Variables

- Time and space variations of network node locations
- Distance of nodes beyond FOV of TOC

Environmental Variables

- Weather
- Wireless traffic (UWB, non 802.20)

Measures of Performance

- Ability of network to rapidly adapt to number of nodes, location of nodes, and rate-of-change of location
- Quality and effectiveness of operating team communications and information flow
- Reliability and quality of asset video
- Reliability and "usability" of SA at local TOC and MV

Scenario 16-18 May

To be tested is the networks ability to provide "through-wall" user access in an urban area utilizing the Military Operations in an Urban Terrain (MOUT) facility located at Fort Ord.

Network availability will be provided by the Cell on Light Truck (COLT) vehicle provided by Flarion Technologies. The vehicle is a highly mobile network provider which contains all elements necessary for a wireless 802.20 network to include: omni-directional antenna, basestation, AAA server and a connection to the backhaul network.

Network availability and capability will then be tested throughout the MOUT facility beginning at the buildings closest to the COLT vehicle and moving outward.

Network availability will be tested in a highly mobile environment throughout the facility. Experimenters will rapidly enter and exit the MOUT buildings utilizing a vehicle to traverse the facility and will determine connectivity as a result of speed and distance from the

base station. The COLT location will be pre-entered on a map and its logical area of coverage will be discerned prior to the experiment. MUST BE AT LEAST 1.5 LINES AT TOP

EVENT 1

Experimenters will establish a working 802.16 link into the MOUT facility, connecting to a pre-existing antenna on R32. This link will require a line of sight shot from R32 to a ridgeline above the MOUT facility. At the ridgeline, experimenters will need two AN-50s, a generator, one sectional antenna pointed at R32 and an omni antenna to connect to the MOUT facility. Placing an Omni antenna at the building nearest to the 802.20 COLT vehicle will complete the link. This Omni will be connected to an AN-50 placed inside the COLT vehicle. Once connected, experimenters will ensure “plug and play” connectivity between 802.16 and 802.20. From the 802.20 side of the network, experimenters will ping servers located at NPS and will utilize VOIP to communicate on the NPS infrastructure.

EVENT 2

Experimenters will utilize a Sony Pan-Tilt-Zoom camera located in the MOUT facility and will continue to access and move the camera using the 802.20 network from a mobile laptop. Testing will be done throughout the facility and again via vehicular travel in and around the MOUT facility until connectivity is lost. Network capability will be demonstrated by the ability to view the video stream from the Internet camera at given distances with varying terrain.

EVENT 3

Experimenters will traverse the MOUT facility utilizing handheld PDA’s connected to the 802.20 network. They will use Microsoft Portrait to communicate with each other in and around the buildings. Network capability will be demonstrated by the ability for the experimenters to communicate effectively. Testing will specifically be done at two points of interest as identified by SOCOM. The first location will be inside a basement and the second will be inside a “mock” prison cell well within a windowless MOUT building.

EVENT 4

Experimenters will drive rapidly through the facility and surrounding terrain utilizing a laptop connected to the 802.20 network. Measures of performance will be measured using FMDM, Netpersec and Miperf. Network connectivity will be measured in relation to distance and speed.

19 MAY THROUGH WALL PENETRATION ALONGSIDE UWB

Through wall penetration tests will be conducted utilizing UWB. Experimenters will conduct through wall tests of network access in conjunction with UWB tests. FMDM, Miperf and Netpersec will be utilized to measure performance and Microsoft Portrait will be utilized to demonstrate network capabilities. The user’s ability to maintain connectivity while maneuvering in and around the MOUT facility will be noted. A repeat of the above events may be conducted to provide necessary data.

Naval Postgraduate School Field Experiment TNT 05-02 (802.20)

SCENARIO: ON-THE-MOVE NETWORK PERFORMANCE AT CAMP ROBERTS

Assumption

Future SOF and Marine Corp operations will require the use of an on-the-move network between multiple, dissimilar manned and unmanned assets to include air to provide situational awareness and enhanced warfighting capabilities. These assets could include UAVs (micro, small, tactical, strategic), manned and unmanned aircraft, and squad personnel with advanced video/audio capabilities. Some assets might be permanent while others may rapidly join and leave the area. Network mobility is a necessity driven by target mobility. An integrated network for all assets and the TOC is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of UAVs and other assets utilizing a minimum number of operating personnel.

Basic Requirements

- Local C3I using multiple assets with rapidly changing participants and network node locations
- Network that permits control of multiple assets as well as rapid insertion of new assets
- Situational awareness and common operational picture

Experiment/Demonstration Technologies

- “On-the-move” network.
- Local and remote location SA from multiple assets

Capabilities/Assets

- All 802.20 tactical equipment connected to 802.20/OFDM network
- TOC and MV and experimenter with SA

Experiment Variables

State Variables

- Time and space variations of network node locations
- Distance of nodes beyond FOV of TOC

Environmental Variables

- Weather
- Wireless traffic (UWB, non 802.20)

Measures of Performance

- Ability of network to rapidly adapt to number of nodes, location of nodes, and rate-of-change of location
- Quality and effectiveness of operating team communications and information flow
- Reliability and quality of asset video

Scenario

26 May

To be tested is the networks “range” ability to provide user access in an area of varying geography and vegetation utilizing Camp Roberts.

Network availability will be provided by the Cell on Light Truck (COLT) vehicle provided by Flarion Technologies. The vehicle is a highly mobile network provider which contains all elements necessary for a wireless 802.20 network to include: omni-directional antenna, basestation, AAA server and a connection to the backhaul network.

Network availability and capability will then be tested throughout Camp Roberts starting at the COLT vehicle and moving outward until connectivity is lost.

Network availability will be tested in a highly mobile environment throughout the base. Experimenters will rapidly enter and exit the network utilizing a vehicle to traverse the facility and will determine connectivity as a result of speed and distance from the base station. The COLT location will be pre-entered on a map and its logical area of coverage will be discerned prior to the experiment.

EVENT 1

Experimenter will enter the network by placing a network card into his laptop and proceed to utilize Miperf to flood the network and receive packet throughput information. Testing and recording will be done utilizing Flarion's Mobile Diagnostic Monitor to record all pertinent information to include; SNR, throughput, GPS data, etc. Experimenter will then proceed around Camp Roberts via vehicle to ascertain geographical limits of the COLT 802.20 network.

EVENT 2

Experimenter will enter the network via network card and proceed to utilize a Sony Pan-tilt-zoom camera attached to the network via a Personal Access Device (PAD). Network capability will be determined via the ability to receive quality video and audio while traversing the camp. The physical limits from Event 1 will be used to determine vehicular path.

EVENT 3

Experimenters will traverse Camp Roberts utilizing handheld PDA's connected to the 802.20 network. They will use Microsoft Portrait to communicate with each other in and around the facility. Network capability will be demonstrated by the ability of the experimenters to communicate effectively. Physical limits from Event 1 will be used to determine experimenter's locations. The experimenters should be at the two furthest locations possible for transmission.

EVENT 4

Experimenters will drive rapidly through the facility utilizing a laptop connected to the 802.20 network. Measures of performance will be measured using FMDM, Netpersec and Miperf. Network connectivity will be measured in relation to distance and speed. Experimenters will simulate a rapid military movement utilizing solely the 802.20 network for communications. Experimenters will utilize Camp Roberts airfield to make a high speed run and demonstrate networks ability to stream video and voice without any apparent degradation in quality at speeds in excess of 90mph (90mph is the claimed speed threshold of

the forthcoming 802.16e standard, 802.20 has been successfully tested at speeds of up to 300mph).

EVENT 5

Experimenters will demonstrate the ease of denying user access. Experimenters will have three laptops accessing the network. They will randomly pick one network card to have been compromised and will notify the COLT at which point network access will be denied. All three laptops will be downloading information. To be noted is the networks ability (time) to end the transmission.

The above experiments will not highlight the capability of the technology to seamlessly handoff between two base stations. Once more than one base station has been acquired, this can be demonstrated.

Naval Postgraduate School Field Experiment TNT 05-02 (802.20)

TNT CAMP ROBERTS FIELD DEMONSTRATION

Assumption

Special Operations Forces lack critical capabilities to effectively conduct network-centric operations in urban and near-urban environments. Shortfalls include availability of shared situational awareness, high bandwidth and persistent communications at tactical level, ability to identify and track enemy personnel and equipment, collaborative tools and visualization to more effectively conduct highly coordinated combined U.S. and coalition activities. Secure communications at the tactical level are needed.

Basic Requirements

- Maintain local C3I and global C3I for experiment team.
- GC3I connectivity required from experimenters to TOC.

Experiment/Demonstration Technologies

- Web enabled cameras attached to 802.20 network.
- Effective video transmission with reach back to TOC
- Short haul wireless network: 802.20

Capabilities and Network Building Blocks

A web-enabled camera attached to the 802.20 network will be installed and launched via an aerial balloon. Connectivity will be established and maintained throughout demonstration to include sending suitable footage of the demonstration back to the TOC. Balloon will be located at a distance of 4 miles from the TOC at an elevation of 1000ft.

A second web enabled pan-tilt-zoom camera will be mounted on a tripod and placed on a secluded road between COLT and the aerial balloon. The camera will be utilized to alert the TOC of approaching traffic during the overall demonstration.

Flarion 700 MHz network via COLT

FLARION Network Card in the pad and a 3db gain omni-antenna.

Experiment Variables

State Variables

- Distance between COLT and cameras
- “Visibility” between COLT and cameras (LOS, OLOS, NLOS)
- Distance between cameras and TOC/Command Post
- “Visibility” between cameras and TOC/Command Post

Environmental Variables

- Weather
- Background wireless traffic

Measures of Performance

- 802.20/OFDM mesh networks performance (throughput, packet loss, latency) as function of distance and “visibility.”

Experiments 25 May.

0900: Re-establish connectivity to both cameras utilized in setup of the prior day. Camera is to be connected constantly throughout the demonstration with picture stability and quality used as a visual measure of effectiveness of the experiment given the terrain of the area, cameras optical capabilities and distance between network components.

LIST OF REFERENCES

Alberts, D.S., Garstka, J.J., & Stein, F.P. (1999). "Network Centric Warfare: Developing and Leveraging Information Superiority." 2nd Edition. *C4ISR Cooperative Research Program (CCRP)*.

Alberts, D.S., Garstka, J.J. (1999). "Information Superiority & Network Centric Warfare.." Briefing Slides from: "The Information Warfare Site." http://eee.iwar.org.uk/iwar/resources/info-superiority1999. Accessed 25 July 2005.

Cebrowski, A.K. & Garstka, J.J. (January 1998). "Network-centric warfare: Its origin and future." *United States Naval Institute Proceedings*, 124(1).

Clark, Thea & Moon, Terry. (1999). "Assessing the Military Worth of C4ISR Information." *7th International Command and Control Research and Technology Symposium*.

Hayes, Richard E. and others. (Sep, 2003). "Headquarters Effectiveness Assessment Tool (HEAT)." Evidence Based Research, Inc.

Kim, J. & Leung, K. (2002). "Frequency Assignment for Multi-Cell IEEE 802.11 Wireless Networks." AT&T Research.

Lander, Michael T. "Flash-OFDM Technical Update," *Signals Ahead*, Vol 2, No.3, 7 Feb 2005.

Lim, Soon-Chia. (2004). "Network Centric Warfare: A Command and Control Perspective." Naval Postgraduate School.

Logan, B.C. (2003). "Technical Referene Model for Network Centric Operations." Crosstalk-The Journal of Defense Software Engineering.

Parrish, Bill & Tovar, Daniel. (2005). “Tactical Wireless Networking In Coalition Environments: Implementing an IEEE 802.20 Wireless End-User Network utilizing FLASH-OFDM to Provide a Secure Mobile Extension to Existing WAN. Naval Postgraduate School.

Power, Willam V., (2004). “Drive Testing Nextel’s Flarion Trial in Raleigh,” Baird US Equity Research Report.

Russell, Steven F. “Wireless Channel Security Tutorial.” http://www.public.iastate.edu/~sfr/wireless/w_tut_1.html. Accessed 25 July 2005.

U.S. Joint Chiefs of Staff. (2000). “Joint Vision 2020.” Washington, D.C.

“802.20 Working Group.” http://grouper.ieee.org/groups/802/20/. Accessed 25 June 2005.

“The Infocomm Development Authority of Singapore.” http://www.ida.gov.sg/idaweb/. Accessed 20 June 2005.

Flarion Technologies, Inc., (2003). “Quality of Service (QoS) over an IP-Friendly Air link,” Bedminster, NJ.

Flarion Technologies, Inc., (2003). “End-to-End Security across a Mobile Broadband Network.” Bedminster, NJ.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Jacob Huffaker
   US Navy
   Pensacola, FL

4. Dan C. Boger
   Naval Postgraduate School
   Monterey, CA

5. Alex Bordetsky
   Naval Postgraduate School
   Monterey, CA