MODELING THE COMMUNICATIONS CAPABILITIES OF THE INFANTRY SOLDIER

BY
ASHOK DEB
KRISTIN FREBERG
JOHN SURDU
ANDREW HALL
FERNANDO MAYMI

ABSTRACT

The US Army's Land Warrior system provides each soldier in an infantry squad with a wearable personal area network (PAN) consisting of various sensors, a radio system, and a computer system, designed to enhance the individual soldier's awareness of his own situation and that of his squad. Each Land Warrior PAN in turn is a node in an 802.11 wireless local area network (WLAN) that connects him to the rest of his squad. Similar protocols connect the entire platoon and company to enhance total situational awareness. This project contains the modeling for the topology for a voice, video, and data network for Land Warrior 1.0 from squad member to company commander in a light infantry unit. The model focuses on the network connectivity and reliability between network nodes (individual soldiers) to simulate the network load and requirements. The simulation was used to study various topologies, equipment specifications, and network properties. In addition, statistical analysis was conducted on network traffic conducted with Land Warrior simulations to collect data that will assist us in determining expected network loads and variances. Simulations were conducted in OPNET using existing models for SINCGARS radios and the IEEE 802.11 protocol. The model provides a foundation for further discussion and modeling of the total system before it is fielded as part of the Land Warrior project, and provides possible solutions to network problems that may arise through common usage.

1. INTRODUCTION

1.1. Project Summary

The U.S. Army's Land Warrior System provides each soldier in an infantry squad with a wearable personal area network (PAN) consisting of various sensors, a radio system, and a computer system. These are designed to enhance the individual soldier's awareness of his own situation and that of his squad, and his ability to acquire and interpret critical decision-making information.

Each Land Warrior PAN is in turn a node in an Institute for Electrical and Electronics Engineers (IEEE) 802.11 wireless local area network (WLAN) that connects him to the rest of his squad. This WLAN connects the entire platoon and company to enhance total situational awareness.

The purpose of this research was to model the proposed Land Warrior 1.0 WLAN from the member-of-squad (MOS) level to the company command level using OpNet software, using raw data collected during a Land Warrior exercise. No Land Warrior network models existed when the project began.

Using OpNet, the topology for a voice, video, and data network for Land Warrior 1.0 from squad member to company commander in a light infantry unit were modeled. The focus of this research was on the network connectivity and reliability between network nodes (individual soldiers) to simulate the network load and requirements.

Statistical analysis of network traffic during a Land Warrior exercise was conducted to assist us in determining expected network loads and variances. The simulation was then used to conduct a sensitivity analysis on the effect of adding additional soldiers to the simulation and altering the frequency of network traffic generated by our applications between a maximum and a minimum level. To augment existing data samples, additional simulations to determine network traffic levels were conducted using the *Delta Force II: Land Warrior*[1] combat simulation system.

1.2 Problem Statement

Given the dynamics of the light infantry squad, the objective of this project is to model its communications capabilities by accurately characterizing the envisioned network for Land Warrior 1.0 from MOS to company commander.

1.3 Methodology

We divided this project into six phases, outlined as follows:

(1) Designing a baseline model of the Land Warrior 1.0 Network in OpNet. Using OpNet Software, nodes were constructed in the network to represent soldiers in every position from MOS to company commander. The purpose here was to construct a solid foundation that could be modified and refined for further exploration of the Land Warrior 1.0 network's capabilities. Through the process, OpNet capabilities and networking technologies were explored and evaluated.

(2) Analyzing data from the Ft. Polk experiment. During this process, data gathered from an actual simulated mission was analyzed for probability distributions and population parameters that would be used later to enhance the OpNet simulation. Soldiers using the Land Warrior combat system at Ft. Polk, Louisiana, conducted this mission. The data was analyzed using StatFit, a program within the simulation package proModel. When StatFit provided possible populations the data could have been drawn from, the data was compared to these theoretical populations in order to validate the analysis.

(3) Simulating the Land Warrior Network using *Delta Force II: Land Warrior.* In order to further refine the OpNet model, another cheaper, more time-efficient method of determining the amount of network traffic generated by Land Warrior 1.0 applications was deemed necessary. Several scenarios were designed in *Delta Force II: Land Warrior* in which nine selected cadets, acting as the members of a standard infantry squad equipped with Land Warrior, would shoot, move, and communicate using Land Warrior capabilities in order to simulate the Ft. Polk experiment. The simulation kept a log of all messages sent and received by each soldier. Data was captured from this experiment using SnifferPro to sort through the packets and determine what was sent, how often, and by whom.

(4) Analyzing gathered data for distributions and population parameters, and conducting hypothesis tests against data collected at Ft. Polk with actual Land Warrior equipment. This was done to validate the data taken from *Delta Force II: Land Warrior* against the results of the actual scenario. Hypothesis tests were conducted with the null hypothesis

[1] Delta Force II: Land Warrior is a combat simulation software package fielded by NovaLogic in 2000 for the commercial sector.

stating that no difference exists between the expected values for each set of data. The result determines whether or not the data taken from the *Delta Force II: Land Warrior* experiment is valid, and whether or not this software can be useful as a simulation tool for future similar experiments.

(5) Modifying the data distributions of communication sizes and frequencies in the OpNet model in order to create a more accurate model.
In order to more accurately represent the actual Land Warrior capabilities, the model had to send and receive packets at the same rate as the actual system in order to carry the same network load. Data distributions taken from the Delta Force II: Land Warrior experiment and the Ft. Polk experiment were used to modify those in the application profiles of OpNet so that the node applications would send and receive data at the same rate as the actual system.

(6) Verification and validation.
To validate the OpNet model, several simulations were run and the resulting key statistic, the overall network delay time, was analyzed against that gathered from the Ft. Polk data. The purpose here was to determine whether or not the simulations were accurate representations of the existing network. Once that was determined, sensitivity analyses were conducted on the effect of the number of soldiers connected by the network at any given time on the network delay time. Further sensitivity analyses were conducted on changing the maximum and minimum values for the size and frequency of data transmissions.

In short, the goal of this project is to follow the diagram below: to take PM Soldier's concept diagram for the Land Warrior 1.0 WLAN and develop the same network in OpNet software, from the company commander through the company, down to and including the member of each squad. This and other concept slides for the Land Warrior network can be seen in the Concept Slides Appendix.

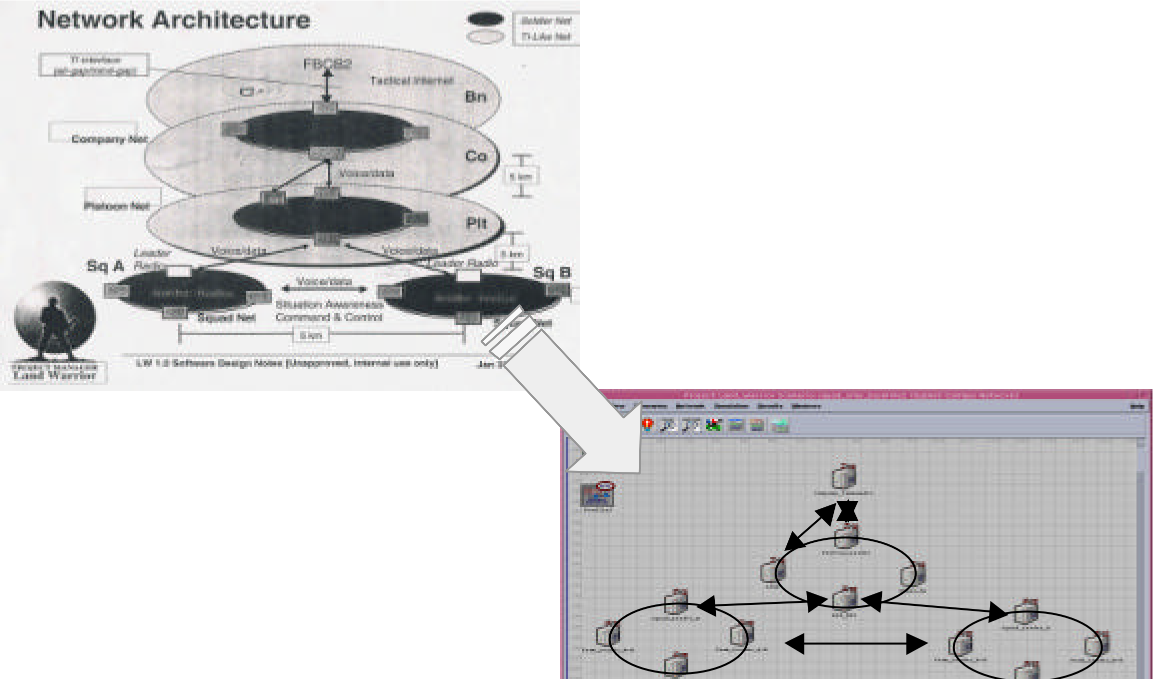


Figure 1.3.1 Progression from Concept Diagram to OpNet Model

2. NETWORKING

2.1 Basics

Wireless Local Area Networks operate similarly to wire networks; however, the data transmission occurs using some radio frequency (RF) technology. The manner in which data is sent poses a problem in reliability and security that is not found in wire transmissions. The three main technologies that handle transmissions in a wireless environment are Direct-Sequence Spread Spectrum (DSSS), Frequency-Hopping Spread Spectrum (FHSS), and Code-Division Multiple Access (CDMA). Spread spectrum (SS) refers to the use of a wide portion of the frequency spectrum. Instead of using a conventional narrowband for transmission, SS uses more bandwidth to spread the signal over a larger range of frequencies. The transmissions are harder to intercept by a third party because of the variable parameters associated with the manner in which the signal is spread. If the intercepting party does not have the exact parameters, then they would only intercept static or background noise.[2]

DSSS communications use a modulated carrier that utilizes a digital code with a code bit rate larger than the information bit rate. The code bits form a redundant bit pattern generated by DSSS that is applied to each bit of information to be transmitted. This bit pattern is the chip or chipping code. The longer the chipping code, the greater the reliability; however, the larger the chipping code, the more bandwidth is required for transmission. The execution of DSSS is fairly straightforward. The binary sequence that is the selected chipping code is applied to the binary sequence of information bits to be transmitted. The first information bit is added modulo-2 (binary addition without the carry) to all the bits in the chipping code. The same is done for the next bit of information to each bit in the chipping code. The resulting transmitted bits should be the number of information bits multiplied by the size of the chipping code. The receiver then mod-2 adds the *n*-bit chipping code to *n*-bit long sequences of the transmitted bits to get the original information with a redundancy of *n*.[3]

The following figure (Figure 2.1.1) is a spectrum analyzer photo of a DSSS signal. The photo shows the most common type of direct sequence modulated spread spectrum signal. The type of carrier and data modulation used can vary the spectral shape somewhat; this particular signal resulted from a binary phase shift keyed (BPSK) signal, the most common type used in direct sequence systems.[4]

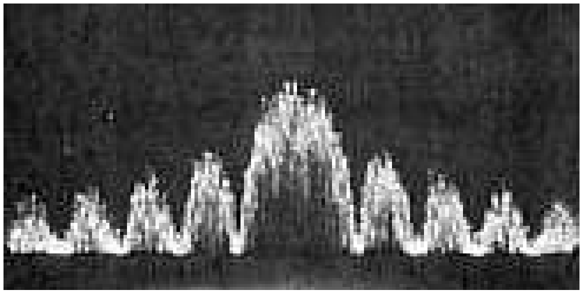


Figure 2.1.1. DSSS Signal Spectrogram.

FHSS uses a narrowband carrier, which is shifted or "hopped" in discrete increments of frequency. The pattern for "hopping" is generated by a code sequence that spreads the signal over the wide frequency band. As an added feature, the frequency hopping code can be designed as to avoid interference from other communication systems in the area. This has the potential to allow multiple networks in the same area using the same bandwidth provided the hopping codes are sufficiently distinct.

The following figure (Figure 2.1.2) is a spectrum analyzer photo of a FHSS signal. The photo shows the flat output of a FHSS system over the band of frequencies used; the bandwidth is simply a function of the

[2] Gil Heal, *Data Over Wireless Network: Bluetooth, WAP, & Wireless LANs* (McGraw-Hill: New York, 2001), 231.

[3] Ibid., 233.

[4] "SSS Online's Spread Spectrum Introduction" [online] http://sss-mag.com/primer.html February 16, 2001.

bandwidth of each hop channel multiplied by the number of frequency slots available.[5]

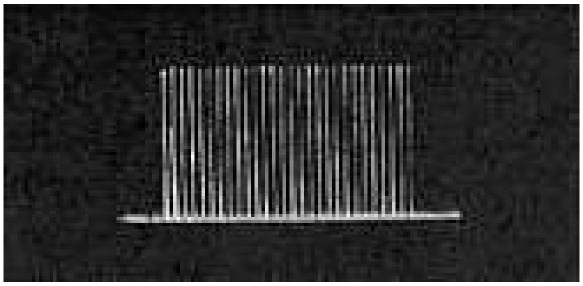


Figure 2.1.2. FHSS Signal Spectrogram.

CDMA is also a direct sequence technique that is similar to DSSS. The spreading sequence is based on a pseudorandom binary sequence called the *pseudonoise digital signal*. This signal is used to modulate the information sequence in a manner like DSSS, which increases the bandwidth requirement. Likewise, the receiver uses the same pseudonoise digital signal to reconstruct the original information sequence. Transmissions with CDMA are time and frequency variable.

This means that transmissions occur at frequency f_1 for a time of t_1 and then move to frequency f_2 for a time of t_2.[6] Currently, CDMA requires 1.23 MHz per channel and is already defined in the United States for the 800- and 1900-MHz frequency bands. In the near future, CDMA2000, which is currently being developed, is expected to use 5 MHz of bandwidth to support 385 Kbps in a mobile environment and 2Mbps from a fixed location.[7]

The figure below (Figure 2.1.3) is an overview of various CDMA technologies currently available and some of their capabilities. The CDMA Development Group (CDG) in particular is working to field new and updated versions of this technology for use in cellular communications.[8]

CCMA, instead of using time or frequency division multiplexing, gives each node its own code that it uses to encode the data bits that it sends. With this methodology, different nodes can transmit simultaneously despite interfering transmissions with other nodes. By this protocol, each bit is multiplied

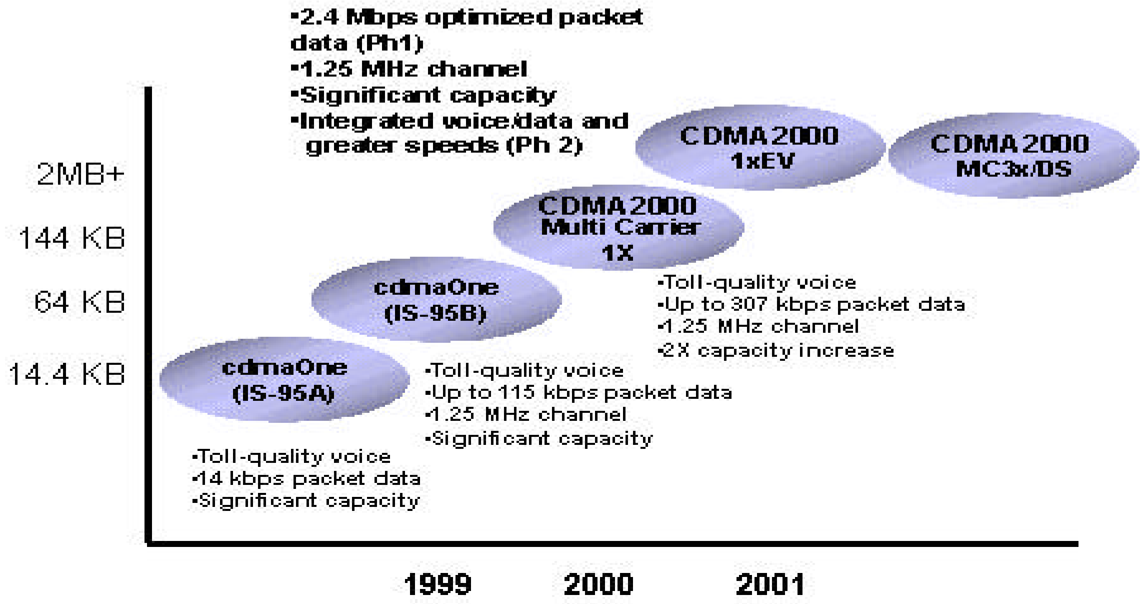


Figure 2.1.3. CDMA Technologies.

[5] Ibid.

[6] Gil Heal, *Data Over Wireless Network: Bluetooth, WAP, & Wireless LANs* (McGraw-Hill: New York, 2001), 117.

[7] Ibid., 141.

[8] "CDMA Development Group Overview" [online] http://www.cdg.org/3GPavilion/overview.asp March 29, 2001.

by a particular code or signal before it is sent. The rate at which the bits are multiplied by the code is called the chipping rate, which must be faster than the transmission rate. The receiving node will also have the sender's code, which is designed in a way to allow the receiver to recover the message out of the aggregate signal sent.[9]

2.2 IEEE 802.11

Institute of Electrical and Electronics Engineers (IEEE) 802.11 protocol is the wireless standards for "over the air" communication between wireless clients that was approved in 1997.[10] This standard is comparable to the IEEE 802.3 standard which specifies Ethernet communications for wired LANs. The IEEE 802.11 standard addresses both the media access control (MAC) and the physical layers of networking to resolve compatibility issues between different manufacturers of wireless equipment.[11] The MAC layer is responsible for maintaining order over the shared medium. The physical layer handles the transmission of data between clients and can either use DSSS, FHSS, or infrared (IR) pulse position modulation. IEEE 802.11 currently has data transmission rates of 1-2 Mbps with future ability of 11 Mbps and operates in the 2.4 – 2.4835 GHz frequency band for spread spectrum, which is an unlicensed band for industrial, scientific, and medical (ISM) applications. IR transmission operates in 300-428,000 GHz and is more secure because it requires direct line-of-sight; however, the line-of-sight requirement makes IR transmission an impossible option for this project.

IEEE 802.11 specifies carrier sense multiple access with collision avoidance (CSMA/CA) protocol. Simply stated, when a client wishes to transmit a packet, it listens to ensure no other client is transmitting; if the channel is clear, the client transmits, and if not it will wait for a randomly determined amount of time (the "back off" factor) and retry. This allows for collision avoidance, not collision detection, which is found in IEEE 802.3. This is because a client transmitting in IEEE 802.11 will drown out any signals arriving with its own transmitting signal.[12]

There are two manners in which to configure a network using IEE 802.11. The first is an "ad-hoc" network, which is when clients are brought together to form a network "on the fly." This is a very mobile configuration because there are no fixed points or a set structure on the network. The added benefit to this is that every client has the ability to communicate with every other client. There are two ways in which order is maintained in the "ad-hoc" network. Spokesman Election Algorithms (SEA) and other similar algorithms designate one client as the master and the other clients in the network as slaves. This provides a hierarchy for information distribution. The other method is to use a broadcast and flooding method to all the clients to determine who is who. The second structure is the infrastructure configuration, which uses fixed network access points within which mobile clients can communicate. The main drawback to this configuration is that the mobile clients must be within range of the predefined, often static, access points in order to communicate with one another.[13]

In regards to this project, IEEE 802.11 has a few significant advantages and disadvantages. The European Telecommunications Standards Institute (ETSI) is considering adopting IEEE 802.11

[9] James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet" New York: Addison Wesley, 2001, 396-398.

[10] Charles Severance, "IEEE 802.11: Wireless is Coming Home," *Computer* (vol. 32, no.11), 126-127.

[11] "IEEE 802 Overview" [online] http://standards.ieee.org/wireless/overview.html December 19, 2000.

[12] D.L. Lough, T.K. Blankenship, K.J. Krizman, "A Short Tutorial on Wireless LANs and IEEE 802.11" [online] http://www.computer.org/students/looking/summer97/ieee802.htmJune 1997.

[13] Ibid.

standards, which would facilitate international interoperability. Interoperability is a future consideration with the increase in combined operations, those that involve more than one allied country. DSSS breaks the spectrum into eleven separate channels. Instead of sending a full power signal through the entire channel, DSSS sends a lower power signal that uses redundant coding so that the receiver can reassemble the data in case of interference. FHSS divides the spectrum into 79 separate 1 MHz wide bands. The communicating devices switch between those different frequencies 50 times per second using a predefined pattern.[14] DSSS transmits over a wider frequency (11 MHz) while FHSS transmits on a narrower band (1 MHz); therefore, DSSS can offer greater transmission speeds over longer distances. The drawback of DSSS is that a wider channel band offers fewer channels and less scalability, meaning that bandwidth goes down as more clients are added to the network.[15] DSSS also uses more power and is more expensive to produce. Power and cost are important considerations, because the client has specified a requirement of a five-kilometer range while operating on a battery.[16]

Other considerations from the military perspective are the reliability of the network given that a client is removed. The IEEE 802.11 standard automatically handles the hand-off required to pass control from one access point to another.[17] As for security, the IEEE 802.11 standard has no special measures in its protocol for added security other than FHSS, so the majority of the security must be handled on the application layer of the network. The main problem with IEEE 802.11, which is common in all wireless protocols, is that since there are no wired connections, an unauthorized person may be able to "spoof" the network. Spoofing is the malicious method by which a person "pretends" to be an authorized user to gain authentication so that they can gain access to the information being sent over the network.

There are two other sub-versions of the IEEE 802.11 standard worth mentioning. The first is IEEE 802.11b which permits devices to connect using either peer-to-peer networks or networks supported by fixed access points around which mobile devices can communicate.[18] The main difference between IEEE 802.11 and IEEE 802.11b is the latter's use of complementary code-keying DSSS, which allows for faster transmissions than those found using regular DSSS in the former.[19] For this reason, IEEE 802.11 is used widely today as the protocol for wireless solutions to LANs using laptops in the home and business.

Another sub-version of IEEE 802.11 is IEEE 802.11a. This protocol supports a chip set that will enable communication on a 5 GHz bandwidth.[20] The implementation cost of this standard is comparable to IEEE 802.11b; however, IEEE 802.11a can provide at least five times the throughput on a cleaner band. The 2.4 GHz band used for IEEE 802.11 has become saturated with increasing applications. The fundamental difference for IEEE 802.11a is that it is based on Orthogonal Frequency Division Multiplexing (OFMD) to modulate the data.[21] OFDM is very robust due to multipath echoes. Each OFDM symbol has 52 subcarriers. The physical layer allows data transfer rates from 6 Mbps to 54 Mbps with a 20 MHz gap between channels. Furthermore,

[14] Charles Severance, "IEEE 802.11: Wireless is Coming Home," *Computer* (vol. 32, no. 11), 126-127.

[15] Ted Lewis, "UbiNet: The Ubiquitous Internet Will Be Wireless," *Computer* (vol. 32, no. 10), 126-128.

[16] Linda D. Paulson, "Exploring the Wireless LANscape," *Computer* (vol. 33, no. 10), 12-16.

[17] Ted Lewis, "UbiNet: The Ubiquitous Internet Will Be Wireless," *Computer* (vol. 32, no. 10), 126-128.

[18] Linda D. Paulson, "Exploring the Wireless LANscape," *Computer* (vol. 33, no. 10), 12-16.

[19] Ibid.

[20] Patrick Mannion, "Radiata Rolls 5-GHz Wireless LAN Chip Set, As IEEE 802 Meets," *EE Times*, July 10, 2000.

[21] Summary Report of the November 1999 meeting of IEEE 802.11 [online], http://grouper.ieee.org/groups/802/11/Reports/Summary-report-99-Nov-meeting.html, November 1999.

the multirate mechanism of the media access control layer ensures that all devices are communicating at the best rate possible for that particular channel.[22]

2.3 Bluetooth

Bluetooth is a developing wireless technology that has a lot of potential. Bluetooth supports ad hoc networking, which, as stated before, is a network system that forms spontaneously.[23] The network model for Bluetooth is a peer-to-peer, which is based on the proximity of the networking. When two Bluetooth devices come within range of each other, a connection is automatically made.

Bluetooth uses FHSS over 79 1-MHz-wide channels. This standard transmits on the license-free 2.4 GHz ISM band. The FCC part 15.247 regulations restrict the maximum peak output power of the radiator to 1 watt (30 dBm), which would provide a range of over 100 meters.[24] The transmit power and receiver sensitivity design decisions for Bluetooth led to reduced cost and lower power requirements than IEEE 802.11. An IEEE 802.11 network uses more power and has a higher sensitivity level, meaning that a comparable Bluetooth radio can be manufactured cheaper than an 802.11 radio.[25]

Bluetooth has a power saving feature called adaptive transmission power. This allows the slaves to inform the master when the transmission power is not adequate so that the master can adjust the transmission power. This is done via the received signal strength indicator (RSSI). The RSSI can adjust the transmission power if it is too strong or too weak so that only the required power needed is used. This obviously saves power, which is important for a system operating on battery; additionally, this ensures that the range of the network does not overextend, which allows for easier eavesdropping and network spoofing.[26]

Bluetooth uses a piconet topology. A piconet is a master device that is connected to slave devices, which are in proximity. In order to communicate, all of the devices in the piconet must be synchronized with the master device. When there are two or more piconets within the same proximity, a scatternet is formed. The two piconets can stay independent if the two master devices are synchronized with their respective piconets and have different frequency hopping patterns.[27]

When two devices establish a Bluetooth link, one acts in the role of the master and the other occupies the role of the slave. The master does not have any additional privileges or authority; instead, it regulates the synchronization of the FHSS between the two devices. The master determines the frequency hopping pattern and the phase for the hopping sequence. It hops pseudo-randomly at 1,600 hops per second. Bluetooth supports both synchronous and asynchronous communication. Synchronous bands will deliver high quality voice transmissions in excess of 1 Mbps, while asynchronous bands will send data at a rate of 700 Kbps.[28] A master can communicate with up to 7 active slaves and maintain a connection with up to 255 parked slaves. The main strength of Bluetooth is that it is optimized for short-range communication, lower power consumptions, and low cost.[29] Its short range is, however, a disadvantage, along with the communication loss that results from sustained motion. Bluetooth may be practical for turning the Land Warrior PAN into a wireless network, but not for operating the entire Land Warrior 1.0 network.

[22] Ibid.
[23] Chatschik Bisdikian, Brent A. Miller, *Bluetooth Revealed* (Prentice Hall PTR: Upper Saddle River, 2001), 44.
[24] Ibid, 80.
[25] Ibid, 82.
[26] Ibid, 24.
[27] Ibid, 26.
[28] Art Wittmann, "Brush Up On Bluetooth," [online] http://networkcomution.com/1013/1013colwittmann.html June 28, 1999.
[29] Chatschik Bisdikian, Brent A. Miller, *Bluetooth Revealed* (Prentice Hall PTR: Upper Saddle River, 2001), 20.

2.4 SINCGARS

The Single Channel Ground and Airborne Radio System (SINCGARS) was designed to provide VHF-FM (30-88 MHz) combat net radio communication with frequency hopping capabilities and digital data transmission capabilities. It was given a modular design in order to make it compatible with the maximum number of existing ground and airborne communications systems. Both the manpack and vehicle configurations use a common Receiver-Transmitter (RT) unit in order to communicate. This system operates between 30 and 88 MHz over 2320 channels, and purportedly is designed to withstand even the pressures of a nuclear environment.[30]

Security for SINCGARS transmissions is provided by the VINSON device, which provides encrypted high-frequency protection, although a system integral to the SINCGARS radio itself is in production. Electric Counter Countermeasure (ECCM) capabilities allow the SINCGARS radio to operate in a number of hostile environments, including nuclear and chemical conditions. It provides a Combat Net Radio (CNR) that is highly secure, very reliable according to testing, and easily maintained. It is capable of handling both voice and data transmissions, and is continually being modified in order to reduce weight and size.[31]

SINCGARS radios offer "improved data capability, improved forward error correction for low speed data modes, and a Global Positioning System interface and Internet Controller, which allows SINCGARS to interface with EPLRS and Battlefield Functional Area host computers." So far, 136,000 of these radios have been tested and fielded to Army units, and are in continual improvement and revision.[32]

3. LAND WARRIOR

3.1 Concept

The purpose behind the Land Warrior fighting system is to integrate the capabilities of an infantry soldier into a war-fighting system that maximizes a soldier's abilities in close combat. Land Warrior is designed to be a Soldier System, which includes everything that is "worn, carried, or consumed by individuals in a tactical environment."[33] It enhances not only the abilities of the individual soldier in terms of combat effectiveness, situational awareness, lethality, mobility, and survivability, but enhances the overall effectiveness of the entire infantry unit, from individual soldier to fighting line company. As mentioned previously, concept designs for the Land Warrior project and network can be found in the Concept Slides Appendix.

Land Warrior was designed with the Army's Force XXI vision in mind, providing to the Army infantry forces that have greater effectiveness in the aforementioned areas of lethality, mobility, and survivability. This contributes to a more lethal force that will be more effective in exploiting both tactical and strategic objectives. These objectives are referenced in greater detail in the 1998 Army Modernization Plan, Annex B, and the 1998 Defense Planning Guidance FY 2000-2005, with respect to the Force XXI vision and the overarching concept behind the Army After Next proposal.[34]

The Land Warrior 1.0 network contributes to the overall Land Warrior combat system by providing both individual soldiers and command echelons with essential situational awareness tools and improved communications capabilities. The system requires this network to provide reliable information to the individual soldier and the ability to share this information across units all

[30] John Pike, "Single Channel Ground and Airborne Radio System," [online] http://www.fas.org/man/dod-101/sys/land/sincgars.htm, March 19, 1999.
[31] Ibid.
[32] Ibid.

[33] PM Soldier, "Land Warrior Operational Requirements Document" (3 August 1999), 1.
[34] Ibid.

the way to battalion command facilities. This capability improves command and control functions and maintains mission focus throughout the unit.[35]

Under current communications systems, infantry soldiers have only limited access to information and data regarding their unit's status in an engagement, pertinent weather data, updated maneuver and fire information, and other information essential to their ability to make decisions on the battlefield. In order to have complete situational awareness, a soldier must have timely, relevant, and accurate information available to him at all times. This allows infantry commanders and leaders to make more informed and quicker decisions, improve force protection within their units, and increase their effectiveness in accomplishing their missions.[36] A concept diagram of the Land Warrior system as it will look eventually with all technological changes implemented is shown below.[37]

3.2 Integration

In order for the Land Warrior system to improve a soldier's ability to shoot, move, and communicate, there must be a reliable secure network connecting each soldier to the rest of his unit, and connecting that unit to higher echelons of command and control. The purpose of this project is to model this network. Our collected and analyzed data and the OpNet software package will enable simulation of the actual network and assist in determining whether or not it meets the specifications of the Land Warrior system. It also enables the early identification of problem areas that could potentially occur in the Land Warrior 1.0 network, and possibly present solutions as well. It accomplishes this in a much cheaper and more time-efficient manner than running a full simulation such as that conducted with real soldiers and real equipment at Ft. Polk.

[35] Ibid., 2.
[36] Ibid., 13.
[37] PM Soldier, "Land Warrior Press Packet," January 2001.

4. ANALYSIS OF DATA

4.1 Data Collection

The network data upon which the OpNet model would be based was taken from a Land Warrior 1.0 exercise conducted at Ft. Polk, Louisiana. A platoon of infantry soldiers from the 82nd Airborne Division at Ft. Bragg jumped into Ft. Polk on a night mission, fully equipped with Land Warrior technology, with a mission to perform an airborne insertion, conduct movement to contact, and eliminate any enemy forces they might encounter using Land Warrior technologies. They successfully inserted into the objective, conducted their mission, and utilized Land Warrior communication systems to enhance their situational awareness and their ability to communicate with one another.[38]

Data from this experiment was collected over a period of five hours, from approximately 0300 to 0800, during the time between the platoon's landing and assaulting across the objective. The network data provided was then analyzed through the use of a Java application, to break it down into lines of data that could be further manipulated for experimentation and simulation purposes.

4.2 Analysis of Data

The data captured from the Ft. Polk experiment consisted of several key statistics regarding frequency of message data and types of messages sent, which would be used in the OpNet simulation model. Over three hundred thousand lines of data were retrieved, consisting of a timestamp of the time the data was sent, the size of the file, the IP addresses of the sender and receiver, and the type of data being transmitted.

A Java application was used to sift through the raw network traffic data and identify packets that fell into one of four categories: Active Soldier packets, voice over Internet Protocol (VOIP) packets, Email packets, and map overlay packets. Active Soldier packets contain the position location data (from GPS) about each soldier equipped with Land Warrior. VOIP packets are the most common, and they carry voice transmissions between soldiers. Email packets are used to send requests for artillery fire, requests for medic, situation reports, and other messages. Overlay packets are used to transmit graphical information to be displayed on other soldiers' map displays. This Java application identified the various packets and put them into a comma-delimited text file that could be read into Microsoft Excel[39] for further analysis.

Microsoft Excel was able to transform these text files into columns of data that could be sorted and filtered using various macros. Using these macros, the data categories were sorted by time in order to determine Interarrival times (IATs) and the size of the sent files. Further macros pulled sections of data into StatFit. This data package was selected because it provided the top six possible populations (distribution types with parameters, e.g. Gamma with ? = 2 and ? = 3, etc.) from which our data could be a sample, and the percent likelihood that our data came from those populations. This feature of the

[38] Land Warrior's effectiveness in enhancing situational awareness was revealed when a soldier was able to take out an opposing force (OPFOR) sniper solely through the use of his Land Warrior equipment. He sighted an approaching soldier through his night vision technology, consulted his overlay map, noted the position of each of the members of his unit, and realized that the approaching soldier's position did not correspond to any of their positions. He realized that the approaching soldier was OPFOR and took him out. Land Warrior's ability to provide this information prevented a possible fratricide.

[39] Microsoft Excel is a spreadsheet data package fielded in 1998 for Windows by Microsoft, Inc.

program enabled the consideration of multiple populations, some being more practical for simulation than others. Additionally, these distributions were tested using probability plots in Minitab 13[40] to ensure their goodness of fit.

The following statistics and distributions were retrieved from the Ft. Polk data:

?? VOIP IATs: Exponential [? = 112.537]
?? VOIP Sizes: Lognormal [min = 64, ? = 118.041, ? = 27.4399]
?? GPS IATs: Weibull [min = 56, ? = 2.73, ? = 12]
?? GPS Sizes: Lognormal [min = 64, ? = 187.682, ? = 4.371]
?? Email IATs: Exponential [? = 11.486]
?? Email Sizes: Lognormal [min = 202, ? = 205.057, ? = 8.4649]
?? Overlay IATs: Lognormal [min = 0, ? = 233.813, ? = 4.282]
?? Overlay Sizes: Lognormal [min = 88, ? = 113.6, ? = 5.908]

When these data sets were run through Minitab probability plot analyses, they returned graphs showing that each of these distributions were satisfactory fits for the data samples. Any error in these graphs can be the result of any number of outside factors that were not taken into account during this experiment, e.g. soldier discipline or lack thereof over the VOIP system, etc.

In order to conduct further tests on this analysis, a Kolmogorov-Smirnov (KS) test, a chi-squared test, and an Anderson-Darling test were performed between simulated values generated by the theoretical distribution and those data points actually provided to determine whether or not there was a significant disparity between the two sets of data. The tests were conducted again using StatFit.

A KS test is based on the largest deviation between the theoretical and simulated data points. This test is based on a null hypothesis of no significant difference between the theoretical distribution and the given sample that is being tested. As the number of data in the sample becomes larger, the given sample should become a better approximation to the theoretical data given that our null hypothesis is true.[41]

A chi-squared test uses a sample statistic that determines the sum of the squared error terms, which are given by the difference between the observed and expected value divided by the expected value. The chi-squared test is a less powerful test than the Kolmogorov-Smirnov test and can only be used to look at large sample sizes. Since the data in this experiment numbers in the thousands, far above the forty or so data points a chi-squared test needs to be effective, the chi-squared test can be used here.[42]

An Anderson-Darling test compares the fit of a cumulative distribution function to an expected cumulative distribution function. The goodness-of-fit test is very skewed and while the associated critical points have been tabulated both through simulation and through theoretical approximation, the test is usually highly effective in the lower tails of the distribution, though it loses its effectiveness in the large curve.[43]

The KS test is the most powerful test of the three. The probability of committing a Type-II error, or accepting the null hypothesis when it is actually false, determines the power of the test. The probability of committing a Type-II error is represented by ?, and the power of the test can be determined by 1-?. The probability of rejecting the null hypothesis when it is actually true is therefore much lower with a KS test than with any of the other tests. All three tests are readily available in StatFit, so all were used. The

[40] Minitab 13 is a statistics analysis software package fielded in 2001 for Windows by Minitab Inc.

[41] Jerry Banks, John S. Carson, Barry L. Nelson, *Discrete Event System Simulation* (Prentice Hall: Upper Saddle River, NJ, 1999), 299.

[42] Ibid., 303.

[43] David Giles, "A Saddle-point Approximation to the Distribution Function of the Anderson-Darling Statistic," [online] http://ideas.uqam.ca/ideas/data/Papers/vicvicewp0005.html, 28 April 2000.

results as determined by StatFit are shown in the following table:

Sample Data Set	Distribution Name	p.d.f Form in StatFit	Parameter s	Key Statistics	Test Statistics	Sample Statistics	Accept / Reject
VOIP IATs	Exponential	$f(x) ?? \frac{1}{?} ?e^{?\frac{?(x? \min)}{?}?}$	? = 112.537	? = .004247, ? = 3.274	Chi^2 = 16.9 KS = 0.0618 And. = 2.49	Chi^2 = 283 KS = 0.826 And. = 983	All Reject
VOIP Sizes	Lognormal	$f(x) ?? \frac{1}{(x? \min)?\sqrt{2?x?^2}} ?e^{\frac{(?\ln(x? \min)??)}{2?^2}}$	min = 64 ? = 3.84 ? = 0.693	? = 118.041, ? = 27.4399	Chi^2 = 36.4 KS = 0.31 And. = 2.49	Chi^2 = 671 KS = 0.0158 And. = 121	All Reject
GPS IATs	Weibull	$f(x) ?? \frac{?}{?} ?\frac{x? \min}{?}?^{??1} e^{??\frac{(x? \min)}{?}??}$	min = 56 ? = 2.73 ? = 12	? = 66.4 ? = 4.022	Chi^2 = 9.49 KS = 0.172 And. = 2.49	Chi^2 = 9.17 KS = 0.155 And. = 2.17	Accept
GPS Sizes	Lognormal	$f(x) ?? \frac{1}{(x? \min)?\sqrt{2?x?^2}} ?e^{\frac{(?\ln(x? \min)??)}{2?^2}}$	min = 64 ? = 4.81 ? = 0.107	? = 187.682 ? = 4.371	Chi^2 = 26.3 KS = 0.0292 And. = 2.49	Chi^2 = 126 KS = 0.428 And. = 34	All Reject
Email IATs	Exponential	$f(x) ?? \frac{1}{?} ?e^{?\frac{?(x? \min)}{?}?}$	min = 102 ? = 11.486	? = .0833 ? =132.87	Chi^2 = 12.6 KS = 0.104 And. = 2.49	Chi^2 = 140 KS = 0.366 And. = 22.8	All Reject
Email Sizes	Lognormal	$f(x) ?? \frac{1}{(x? \min)?\sqrt{2?x?^2}} ?e^{\frac{(?\ln(x? \min)??)}{2?^2}}$	min = 202 ? = 2 ? = 1.21	? = 204.178 ? = 7.165	Chi^2 = 12.6 KS = 0.103 And. = 2.49	Chi^2 = 737 KS = 0.834 And. = 289	All Reject
Overlay IATs	Lognormal	$f(x) ?? \frac{1}{(x? \min)?\sqrt{2?x?^2}} ?e^{\frac{(?\ln(x? \min)??)}{2?^2}}$	min = 0 ? = -1.4 ? = 1.29	? = 1.2725 ? = 5.908	Chi^2 = 21 KS = 0.0456 And. = 2.49	Chi^2 = 191 KS = 0.273 And. = 197	All Reject
Overlay Sizes	Lognormal	$f(x) ?? \frac{1}{(x? \min)?\sqrt{2?x?^2}} ?e^{\frac{(?\ln(x? \min)??)}{2?^2}}$	min = 88 ? = 4.98 ? = 0.0974	? = 233.811 ? = 4.304	Chi^2 = 37.7 KS = 0.0153 And. = 2.49	Chi^2 = 481 KS = 0.417 And. = 210	All Reject

Table 4.2.1. Data Distribution and Hypothesis Tests.

As shown by the previous table, seven out of the eight distributions provided were not statistically similar enough to the actual data to pass the three types of tests. The distributions shown in this table, however, are those that had the lowest difference between the test statistic and the statistic derived from the data given. Since most test statistics are determined by factoring the sample size somehow into their denominators, and the sample sizes being utilized were in the thousands, the test statistics were abnormally small. Because of this, the data parameters given by StatFit are assumed to be maximum likelihood estimators and, until further data can be collected and the distributions modified, will be utilized in simulation.

As useful as these distributions will be, in order to improve the effectiveness of the model, more data must be collected and analyzed more thoroughly. In order to make this data more robust, it is suggested that another means of finding data, lest costly and less time-consuming than the Ft. Polk experiment, be employed. Exploring these options led to the discovery of the Delta Force II: Land Warrior simulation package, which will be discussed in detail in the following section.

5. EXPERIMENT

5.1 Overview

The data gathered from Ft. Polk provided much of the information needed to identify population probability distributions and refine the OpNet model. As mentioned previously, the data given by the Ft. Polk experiment did not match any known distribution with statistical accuracy. Because of this, it became necessary to collect more data. This project's scope and resources required a means of collecting data that would be more cost- and time-efficient than the Ft. Polk experiment.

Finally, the *Delta Force II: Land Warrior* combat simulation system came up in discussions and became a viable option for collecting data regarding network traffic, as simulated by the game. By analyzing statistics gathered from this simulated network traffic, the existing data distributions could be refined and perhaps a statistical match could be found for the given samples. These refined data distributions would allow the OpNet simulation to more accurately approximate the existing Land Warrior 1.0 model.

Delta Force II: Land Warrior is a simulation system that is based on the first-person shooter genre video game of the same name fielded by NovaLogic for the public market. The version utilized for this experiment, however, was modifiable so that individuals could run completely interactive missions using all of the currently developed Land Warrior technology in a simulated environment.[44] The United States Military Academy Department of Military Instruction provided nine networked workstations equipped with *Delta Force II: Land Warrior* technology and a series of scenarios that would allow the collection of further network data.

Nine volunteers from the United States Corps of Cadets acted as the squad throughout the experiment. They were trained in the use of *Delta Force II: Land Warrior* software and worked at interacting with each other using the networked workstations, with each member of the squad holding a specific position with specific capabilities, e.g. Alpha Team Leader, Grenadier B, and so forth. In doing so, they approximated an actual infantry squad with Land Warrior capabilities.

The following were identified as key statistics necessary for the model:

?? Interarrival time between transmissions from all (in seconds)

?? Size of sent messages (in bytes)

?? Type of files or messages sent (voice, video, data, etc.)

In order to obtain these statistics, SnifferPro[45] software was utilized on a laptop attached to the simulation machines to filter out selected packets of information. SnifferPro is a software package designed to filter packets of data and search only for those packets specified in a search program. Using SnifferPro, a large amount of network clutter that would otherwise bias the data could be ignored. This software program was designed to filter out packets with a timestamp, and to show the approximate size of the message, who sent the message, and who received it.

5.2 Assumptions

The Land Warrior 1.0 network model as portrayed by *Delta Force II: Land Warrior* required the following assumptions for the experiment:

?? The network modeled here involves only a single squad.

?? The *Delta Force II: Land Warrior* combat simulation package is not capable of simulating every capability of the current Land Warrior network. For instance, it is not possible to send voice data over the system, and it is not possible to send video imaging. Message data only can be sent.

[44] "Land Warrior Game Info," [online] http://www.landwarrior.org/land_warrior/ November 9, 2000.

[45] SnifferPro is a network analysis package fielded in 2000 by Network Associates.

?? The *Delta Force II: Land Warrior* combat simulation package will not take into account the degradation of signal over the distances shown in the proposed network architecture, nor will it take into account the degradation of signal caused by vegetation or terrain.

?? The *Delta Force II: Land Warrior* combat simulation package simulates a self-healing network; no members in the squad will be disconnected from the network if the squad leader is killed in the combat scenario, and it must be assumed that this happens because the network has "healed" itself.

?? The nine cadets chosen to play *Delta Force II: Land Warrior* have limited knowledge of infantry tactics and doctrine. They will perform according to the guidelines given to them by the experiment controllers, not necessarily those guidelines given by FM 7-8 and official infantry combat standing operating procedures.

5.3 Designing the Experiment

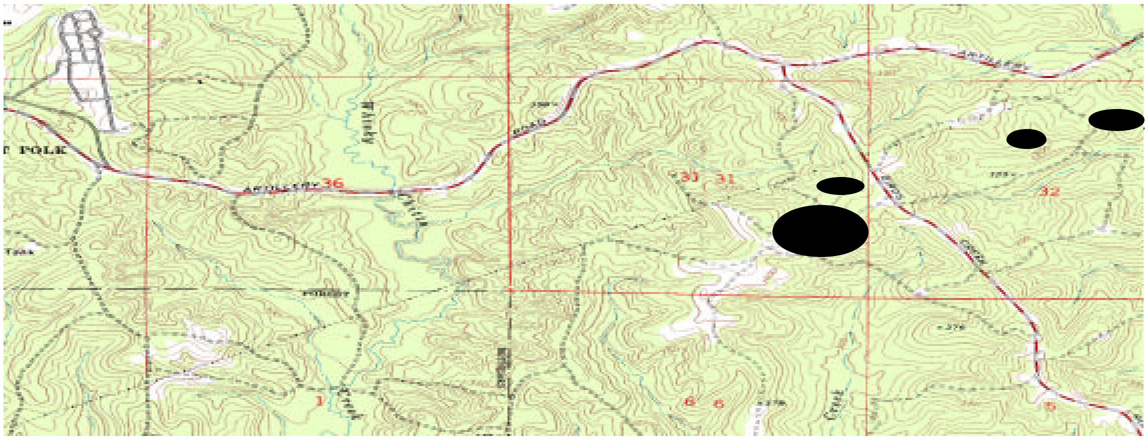
In order to collect data from the Land Warrior experiment, "packet sniffers" were placed on the computers' simulated network to monitor its behavior. These were designed to filter out all information save the key statistics previously identified, in order to make data analysis more efficient. SnifferPro was the software used in this experiment. It is a leading-edge technology that allows network managers to analyze network activity and effectively troubleshoot potential problems on a variety of networks and servers. It can capture data traveling through a network, as in this experiment, or it can measure network capacity needs and analyze the impact of adding new applications.[46] SnifferPro was loaded up onto a laptop and attached to the *Delta Force II: Land Warrior* simulation network to monitor network activity during the experiment.

To explore the capabilities of the Land Warrior network, the volunteers followed specific scenarios designed to help them generate accurate network traffic data. The scenarios were designed to run anywhere from twenty minutes to a full hour, depending on the squad's ability to react to each portion of the simulation. On a simulated layout of Ft. Polk, the squad of game players initiated the simulation after an airborne insertion, moved through a series of checkpoints, and assaulted a small village where a SCUD missile launch platform had been emplaced. Their mission was to check in at each of the checkpoints with situation reports (SITREPs), engage any snipers they might see, call for fire on the SCUD launch platform, and eliminate any security force they might engage within the village itself. If casualties were taken, they were to call for a medic. During the simulation, the players sent in periodic situation reports and checked in at each of the checkpoints, shown on the following map.

Between Checkpoint 1 and Checkpoint 2, the players engaged a pair of snipers and were forced to call for the platoon medic. Continuing on, the players progressed through the last checkpoint and arrived at the village outskirts, where they were engaged by heavy fire from the opposing force (OPFOR) team within the village. There, they successfully called for fire on the SCUD missile launch platform and eliminated the OPFOR security team. This scenario was run twice, and each time took roughly forty minutes to complete.

The variety inherent to the system and in the players enabled the use of all facets of the Land Warrior technology programmed into the *Delta Force II: Land Warrior* software. Unfortunately, not all existing Land Warrior technologies were present in the software, and not every kind of file supported by the network could be simulated. There were no video still capabilities, for example, and no voice data transference was performed. The volunteers performed actions as directed by the experiment controllers to generate data.

[46] "Expert Intelligence for Advanced Network Management," [on-line], http://www.snifferpro.co.uk/pro98/Default.htm, March 12, 2001.



5.4 Data Collection

SnifferPro managed to collect a large amount of data from this experiment. Unfortunately, none of this data could be used to refine the OpNet model. The data generated by the *Delta Force II: Land Warrior* simulation system was not in the form of Land Warrior packets but in game packets. The game packets reflected instantaneous transfer of information and continuously updated GPS locator packets rather than the delayed intermittent packets and information sent across the real Land Warrior network.

While this data was not useful for the OpNet model, it could be useful for later experiments if *Delta Force II: Land Warrior* is modified with the distributions gathered from the actual data to generate Land Warrior packets. Once further experimentation is done to refine the statistical analysis of the actual data, if *Delta Force II: Land Warrior* is modified to more accurately reflect the network's transference of data and modified to include all other omitted applications, it could be a powerful resource for troubleshooting the Land Warrior system. It is a far more cost- and time-efficient method of testing and experimenting than operations such as that conducted at Ft. Polk.

PM Soldier should take a look at making the *Delta Force II: Land Warrior* game into a more robust and accurate piece of software to simulate the system. While the data is not accurate, this experiment proved that SnifferPro could collect packet data from the network and sort it into information that could be used.

6. OPNET PROCEDURES

6.1 OpNet Model Development

In order to develop the Land Warrior 1.0 WLAN in OpNet, the following steps were taken. All of the elements in the model are wireless LAN servers (mobile) from the wireless palette in OpNet. To modify the properties, select "edit attributes." The main point of interest here is to assign the application profiles of each element. Application profiles are developed in the Profiles icon. By editing this, the number of rows can be adjusted to add new profiles, as was done with this model, and add applications that are to be associated with each profile.

The major scenarios worked with in this design are a platoon, a platoon with only two squads, a company, and a company with only two platoons. The profiles developed for these scenarios were profiles for the company commander, the two platoon leaders, the squad leaders, the team leaders, and member of squad. The commanders and leaders in the platoon were given two profiles to allow for the two nets they will utilize, one to their level and higher, and one to their level and lower.

For simulating, OpNet provides global statistics to analyze. The user must also provide the time he or she wishes to run the simulation, the seed, and the statistics he or she wants to collect. The results will be displayed and can be exported into Excel for analysis, as was performed here.

6.2 Data Collection

The simulations conducted in OpNet used existing software models for SINCGARS radios and the IEEE 802.11 protocol for communication. The model was created from the squad up, beginning with a squad leader and two team leaders on a network, expanding to a full squad, enlarging that squad to three squads and a platoon leader, and finally creating two more platoons and a company commander.

New tasks, applications, and overall profiles for each of the soldier-nodes were created within the model to generate the proper amount of network traffic. The profiles are assigned to each soldier-node, and each profile contains a number of applications. Each application contains a given number of tasks, and the tasks themselves are composed of attributes, one of which is the frequency and size of messages sent. Using the new data distributions and parameters, the tasks in the profiles were modified to more accurately represent the traffic generated by applications over the Land Warrior 1.0 WLAN. The purpose of making modifications and running the simulation was to generate information statistically similar to that produced by the Ft. Polk experiment.

6.3 Sensitivity Analysis

A 2^k Factorial Design will be used to conduct a sensitivity analysis on the OpNet model. In order to analyze the effect of a single factor on the model, it would be a simple matter of adjusting that factor and performing a confidence interval on the results. In order to better understand the behavior of the network, multiple factors must be adjusted. This factors that will most likely affect this network are the addition of more soldiers to the network, and adjusting several of the data distributions from their mean value to their maximum value to determine the effect this has on the network load. The purpose in doing this is determining what the critical levels are that may cause the network to keep from functioning. In order to conduct this experiment, the unit examined was a platoon with three complete squads. It took approximately five hours to run four simulations to collect an hour's worth of data for each one.

Since there are *k* amount of factors in this design, and it is necessary to know how each factor individually affects the outcome as well as whether or not these factors interact with each other, a 2^k factorial design will be conducted. This requires that two levels are chosen for each factor, a maximum and a minimum value, and a simulation will be run with every possible combination of the factors. A table will be developed showing these combinations, and each factor will be assigned a plus sign (+) where the factor is at its maximum level, and a minus sign (-) where the factor is at its minimum.[47]

The factors to be investigated will be the frequency of the messages sent over the network for email, overlay, and voice data. The size of each sent message can be assumed to be relatively constant, so the size will not be varied for sensitivity analysis. Additionally, GPS interarrival times are relatively constant as well, with a mean time of about one minute. These times will not be varied for sensitivity analysis. It can be assumed that these variances will be accounted for when the platoon sizes are varied.

This leaves the interarrival times of email, map overlays, and voice over Internet protocol to be analyzed. These three factors will provide eight data points for analysis. For the response values, the maximum net delay and maximum throughput will be used in each case. Most statisticians would argue that at least 30

[47] Averil M. Law, W. David Kelton, *Simulation Modeling and Analysis* (McGraw-Hill: Boston, 2000), 626.

simulation results are needed for each alternative in order to create an accurate result; however, since the parameters being used are based on guesswork, this would only create a false sense of accuracy.[48] Because of this and other time constraints, only a single statistic was taken for each of the eight scenarios. In the future, more work should be done gathering this data and checking it for accuracy and sensitivity, but only after the parameters have been refined. The simulation values used in this analysis were determined by analyzing the three-squad platoon model using a seed of 128.

Network delay and network throughput were designated as the response values, by which the overall effectiveness of the network will be measured. To obtain response values, the network simulation in OpNet was altered and run several times to obtain a mean value for both the network delay and the network throughput. The positive or negative designation was multiplied by the corresponding design point response, not shown on the table, to determine the effect of each factor on the network. For example, the following equation represents the effect of Factor 1, the unit size, on the network:

$$e_1 ?? \frac{?R_1 ? R_2 ? R_3 ? R_4 ? R_5 ? R_6 ? R_7 ? R_8}{2^k}$$

The resulting e_j value is defined as "the difference between the average response when factor j is at its '+' level and the average response when it is at its '-' level."[49] In essence, the process takes the dot product of the factor column with the response column. The result is a mean error value resulting from the lack of or the presence of the factor being analyzed. With this in mind, the simulation was repeated several times, with minimum values for each factor defined as the mean of each distribution, and maximum values for each IAT defined above.

Factors					
	Factor 1	Factor 2	Factor 3		
Design Points	Email IATs	Overlay IATs	Voice IATs	Net Delay	Through put
	Avg / Max	Avg / Max	Avg / Max		
1	-1	-1	-1	0.00654	7412.67
2	1	-1	-1	0.00703	8594.44
3	-1	1	-1	0.00654	7412.67
4	1	1	-1	0.00703	8594.44
5	-1	-1	1	0.00623	8058.89
6	1	-1	1	0.00817	9100.89
7	-1	1	1	0.00623	8058.89
8	1	1	1	0.00817	9100.89

Table 6.2.1. Design of Experiments.

Factor effects were computed as shown in the following table:

Factor	Effect 1 (Delay)	Effect 2 (Throughput)
e1 (Email)	-0.0005425	1111.885
e2 (Overlay)	0	0
e3 (Voice)	0.00205	576.335

Table 6.2.2. Factor Effects Chart.

When an effect shown in the table has a positive value, that means it increases the effect by a positive value of that amount; conversely, when the effect has a negative value, that means it decreases the effect by that amount. These results show the average difference made by the addition of the particular factor being analyzed. For this experiment, negative values are preferable for Delay, which means that the factor is decreasing the network delay when it is added. The factors being added to the network will only serve to increase delay and increase throughput, however. The negative value that the email interarrival times returned is not significant enough to be considered in this case; it is simply assumed that email does not have a significant effect on the delay. Since there are

[48] Ibid., 348.

[49] Ibid., 627.

no interaction effects designated, they will not be analyzed in detail here.

None of the factors examined in this experiment have a significant effect at the platoon level on message delay time measured in seconds. It has been determined that a delay time of more than 3 milliseconds is perceptible by human senses; nothing even approaching this can be seen here on the platoon level. When this factor is analyzed on the company or even the battalion level, however, this may change and there may be serious effects. This will be discussed under future work.

Out of the three factors examined, email has the most significant effect on measured throughput, increasing our measurement on average by 1111.885 bytes. Voice Over Internet Protocol has the second highest effect on the throughput, an effect of 576.335 bytes. These are the largest producers of network traffic; apparently in this simulation, the overlay option was not utilized enough to produce a significant effect on the network. This again may change on the company and battalion levels, and will also be examined in future work.

This experiment determined which factors had a significant effect on the network, but in order to gain a precise understanding of the manner in which these factors affect it, or to determine a mathematical relationship between factors, further experiments must be run on different sizes of units. The most useful part of this analysis is its ability to determine which factors have the worst impact on the network, and to determine whether or not that factor causes the network to cease functioning effectively and methods perhaps of reducing that factor's impact on the network. By adjusting these values, it is possible to determine the sensitivity of the network to different ranges of these factors. Expanding this experiment to utilizing more platoons and a broader range of frequency in transmissions, the capabilities of the network can be further explored.

Examples of the sensitivity of the network to information sent over time can be found in the Graphs Appendix. These graphs show the amount of load, throughput, and delay over time for each of the platoon simulations run.

7. CONCLUSION

7.1 Conclusion

The scope of this project included developing, from the ground up, a model using OpNet software of the Land Warrior 1.0 WLAN from the MOS level to the company commander so that it could be used for network analysis. The design team tasked to this project succeeded in creating a base model in OpNet with all the appropriate nodes from the MOS level to the company commander, as shown by the Project Concept Diagram included in the Land Warrior section and in the Concept Slides Appendix.

Data from the real Land Warrior network was captured and analyzed to further refine the base OpNet model. While the distributions derived from this data are maximum likelihood estimations, hypothesis testing showed them to be flawed still, and determined that more data should be taken to improve the distributions. Methods for improving this data were identified as conducting further experiments with the actual equipment, like the experiment conducted at Ft. Polk, or modifying *Delta Force II: Land Warrior* into a simulation system capable of accurately representing the Land Warrior network. With more data, the model can be made even more accurate.

Preliminary simulations were run using the OpNet model and a full platoon with three complete squads. Effects of three different factors on the network were examined, and it was determined that none of these factors had significant effect on network delay at the platoon level, but both email and VOIP had a significant effect on throughput. Through further simulations and sensitivity analysis, mathematical relationships between the factors and the results can be determined. This can be accomplished in future work.

The design team met its goal of developing a foundation network design that can be further modified and refined, as shown in the next section.

7.2 Future Work

The work here accurately models the Land Warrior 1.0 WLAN and provides a foundation for further studies of the total system before it is fielded as a part of the Land Warrior project in 2010. The model, however, still can be greatly modified before it can finally be considered complete and fully accurate.

The scope of this project was to lay the foundation work for future research and more detailed analysis. The current model only has four main scenarios; future scenarios would include a battalion-sized task force of different company size and composition for use in conducting sensitivity analysis and testing.

The individual profiles in this model currently account for the two command nets on which the platoon leader, squad leader, and team leader will communicate. The model should be expanded to include such considerations for the company commander and the amount of traffic that will be coming down from the battalion commander. Although the company commander is the last command element in Land Warrior 1.0, he or she will be receiving communications traffic from the battalion commander, and this will affect the company commander's communications profile.

The model currently has updated distributions for voice, overlay, and email transmissions that are the same for all elements. However, all of these elements are designed to be different based on position (e.g. the CO's distributions will likely be different from the SL's distributions when broken down further). This data needs to be collected in further experimentation to determine how different these distributions are.

As mentioned previously, one of the problems concerning data generation in the modeling process was using an FTP server in OpNet. The server was configured with a get / total ratio of zero so that it only sent information according to the distributions determined for overlays, voice over IP, GPS updates, and email messages. Ideally, there should be a custom application that uses a custom server to generate the appropriate data for the different types of data sent. This was the original modeling effort; however, difficulties in creating a data source in OpNet forced modeling to continue through different means of implementation. This does not devalue the current model; it only reduces the robustness being sought. Conquering this problem in OpNet is one of the first tasks for follow-up work regarding this project.

Hypothesis tests regarding the accuracy of the data generated by the OpNet model need to be conducted as well. A full level sensitivity analysis was not conducted due to time requirements for running a simulation of merit at the company level. More data needs to be taken to make the data distributions more robust and refine their parameters further. This must be done once the OpNet model is further refined.

Future research will include using a more powerful processing machine to generate the data for analysis, in a more realistic time that allows for multiple iterations. Many more iterations are necessary to ensure confidence in the simulation results. More data will be collected and more detailed analysis will be performed. Additionally, the use of Bluetooth as a protocol will be examined, as well as the Mesh Radio technology, and these technologies will be compared to determine the best protocol for Land Warrior 1.0.

The model in its current state is a solid foundation for future adaptation and refinement, to be conducted in following semesters by successive design teams. As the model grows more and more robust and more closely approximates the actual network, it can be a very useful tool for network analysis and will aid in the production of a Land Warrior 1.0 network that will exceed the Army's expectations in providing situational awareness to soldiers in the field.