NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF NETWORK AND SENSOR PERFORMANCE WITHIN IEEE 802.X WIRELESS MESH NETWORKS IN THE TACTICAL NETWORK TOPOLOGY (TNT)

by

Joseph A. Davis, Sr.

March 2005

Thesis Advisor:	Alexander Bordetsky
Second Reader:	Douglas E. Brinkley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of Network and Sensor Performance within IEEE 802.x Wireless MESH Networks in the Tactical Network Topology (TNT)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Joseph A. Davis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) The objective of this research is to analyze the network performance and sensor functionality, efficacy and usability of IEEE 802.x wireless MESH networks within a DoD Tactical network environment. Multiple sensor configurations operating with wireless MESH network technologies will be researched and analyzed for performance in expeditionary environment situations. Specifically, this thesis will attempt establish the foundation for the development of wireless MESH "network health" models by examining the performance of sensors operating within a MESH network and define which network performance metrics equate to good quality of service. This research will experiment with different application, sensor, and network configurations of currently available COTS components; such as, voice, video and data hardware. This thesis will lay the groundwork for wireless network MESH predictability, which will enable the optimal use of sensors within a tactical network environment.			
14. SUBJECT TERMS Wireless MESH Networking, Ad Hoc Networking, IEEE 802.11, IEEE 802.16, IEEE 802.15.4, Global Information Grid, Wireless, MANET, Sensor Networks, Tactical Network Topology			**15. NUMBER OF PAGES** 69
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ANALYSIS OF NETWORK AND SENSOR PERFORMANCE WITHIN IEEE 802.X WIRELESS MESH NETWORKS IN THE TACTICAL NETWORK TOPOLOGY (TNT)

Joseph A. Davis, Sr.
Lieutenant Commander, Supply Corps, United States Navy
B.B.A., Prairie View A&M University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2005

Author: Joseph A. Davis, Sr.

Approved by: Alexander Bordetsky
Thesis Advisor

Douglas E. Brinkley
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The objective of this research is to analyze the network performance and sensor functionality, efficacy and usability of IEEE 802.x wireless MESH networks within a DoD Tactical network environment. Multiple sensor configurations operating with wireless MESH network technologies will be researched and analyzed for performance in expeditionary environment situations. Specifically, this thesis will attempt establish the foundation for the development of wireless MESH "network health" models by examining the performance of sensors operating within a MESH network and define which network performance metrics equate to good quality of service. This research will experiment with different application, sensor, and network configurations of currently available COTS components; such as, voice, video and data hardware. This thesis will lay the groundwork for wireless network MESH predictability, which will enable the optimal use of sensors within a tactical network environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

ACK	Acknowledge
AODV	Ad Hoc On-demand Distance Vector
AP	Access Point
BRP	Bordercast Routing Protocol
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
DSR	Dynamic Source Routing
ESS	Extended Service Set
GIG	Global Information Grid
GIGA	Global Information Grid Applications
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Server
IPv6	Internet Protocol Version 6
LSP	Link State Packet
MAC	Media Access Control
MCA	Multicriteria analysis
MANET	Mobile Ad Hoc Network
MERCAT	MESH Routing and Capabilities Toolset
MID	Multiple Interface Declaration

MMLDP	Mobile MESH Link Discovery Protocol
MMRP	Mobile MESH Routing Protocol
MobileIP	Mobile Internet Protocol
MPR	Multipoint Relay
NAP	Network Access Points
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OLSR	Optimized Link State Routing
OSI	Open System Interconnection
PCMCIA	Personal Computer Memory Card International Association
PHY	Physical
QoS	Quality-of-Service
RAM	Random Access Memory
RERR	Route Error
RF	Radio frequency
RFC	Requests for Comments
RREP	Route Reply
RREQ	Route Request
SA	Situational Awareness

SNMP	Simple Network Management Protocol
STAN	Surveillance and Target Acquisition Network
SYN	Synchronize
TND	TBRPF Neighbor Discovery
TNT	Tactical Network Topography
TOC	Tactical Operations Center
UGS	Unattended Ground Sensors
UML	Uniform Modeling Language
VoIP	Voice over Internet Protocol
WAP	Wireless Access Point
WDS	Wireless Distribution System
WiFi	Wireless Fidelity

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I want to express my deepest gratitude to my wife and children (Cyndi, Breha, and Anthony) for their understanding and continued support during the course of my studies and thesis work at the Naval Postgraduate School. Secondly, I want to thank my thesis advisor, Professor Alex Bordetsky, for his superb advice and mentorship. Finally, I would like to give special thanks to Douglas Brinkley and Eugene Bourakov for the support they have provided.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

A multipoint-to-multipoint architecture, where every node becomes a router within the network, is a way to enable larger coverage distances with less investment. Wireless MESH networks offer additional capability to traditional networks due to their expandability nature. Because these networks are self-organizing, self-healing and self-balancing, additional MESH nodes and sensors can be seamlessly added to any part of its topology, thus resulting in limitless expansion of MESH networks. The optimal sensor behavior within a network requires a certain level of network performance, and that level of performance equates to premium quality of service (QoS). In order to predict and monitor the performance of wireless MESH sensors in a tactical network environment, I had to analyze and then develop a method of determining the level of network performance required to achieve a given level of sensor performance. In order to make network predictions, we have to be able to measure wireless MESH network performance, and know which variables affect that performance.

B. OBJECTIVES

The objective of this research is to analyze the network and sensor performance, functionality, effectiveness and usability of IEEE 802.x wireless MESH networks within a DoD tactical network environment. Multiple sensor configurations operating with wireless MESH network technologies will be researched and analyzed for performance in expeditionary environment situations. Specifically, this thesis will attempt to define wireless MESH "network health" by examining the performance of sensors operating within a MESH network and what network performance metrics equate to good quality of service. This research will attempt to model the results of experimentation of different application and network configurations of currently available voice, video and data hardware and software wireless MESH networking components. This thesis is intended to lay the groundwork for future modeling and study of mobile ad hoc and wireless MESH networking topics related to the Department of Defense's tactical, expeditionary and Global Information Grid (GIG) environments.

C. RESEARCH QUESTIONS

My primary research question explores network performance required for the optimal operation of sensors in a wireless MESH network within the structure of the Tactical Network Topology (TNT). To resolve this, I initially had to define quality network performance of a wireless MESH network within the framework of a tactical environment. Additionally, I sought to conduct mathematical modeling of network performance resulting from various configurations of commercial-off-the-shelf (COTS) sensors within a tactical wireless MESH network that would result in the best sensor QoS.

D. SCOPE

The scope covers the analysis of the network and sensor performance issues involved in IEEE 802.x standards-based wireless MESH networking solutions. Analyzing configurations of a wireless MESH topology is the initial step in gaining some predictability of network and sensor performance in a tactical MESH network environment. Furthermore, the development of MESH performance metrics will aid in making the TNT more predictable by enabling the possibility of network adjustments prior to losing valuable sensor data, thus increasing the robustness of the tactical network. Numerous local, field, and laboratory experiments using the Tactical Network Topology (TNT) will serve as a foundation for future wireless MESH architecture decisions.

E. METHODOLOGY

My methodology included researching existing network and sensor performance measuring procedures, technologies and theories. I gathered data from various providers of sensor technologies to establish a research baseline for performance measures across multiple operating environments. Additionally, I developed network performance metrics that will support the successful deployment of 802.x wireless MESH sensors in the tactical environment. I then conducted experimentation with sensor configurations to verify vendor data on the efficacy of currently available wireless MESH technologies. The main method of data collection was conducted through Naval Postgraduate School's TNT series of experiments and hands-on testing. Finally, I modeled various MESH sensor configurations that would assist in TNT collaboration and decision-making.

F. ORGANIZATION OF THESIS

The organization of this thesis is as follows:

Chapter II provides an overview of the MESH network and its advantages and constraints. Additionally, I provide a discussion of the QoS of wireless MESH networks.

Chapter III provides an explanation of what makes up a good metric. It also tells what metrics used to forecast TNT network and sensor performance.

Chapter IV discusses the experimental data collection method and the applicable modeling overviews.

Chapter V discusses the experimentation and results of local experiments conducted on the NPS campus and TNT experiments. It examines the experimentation and analysis of different sensor configurations, applications, and MESH protocols affecting wireless MESH network performance. It also analyzes the results of the TNT as it applies to network and sensor performance. Results are analyzed and provide a modeling foundation that will contribute to the optimal performance of the MESH network in a tactical environment. Additionally, it provides some implementation recommendations with regard to planning considerations for TNT.

Chapter VI includes my conclusions on the feasibility and applicability of IEEE 802.x wireless MESH networks within the Tactical Network Topology in light of the current state of technology. Recommendations for future research in this area are also included.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MESH NETWORK HEALTH

A. OVERVIEW OF MESH SENSOR NETWORKS

1. The MESH

A wireless MESH network consists of an ad hoc distribution of wireless nodes. In the MESH, each node constantly communicates its existence, as well as other data, with its neighbors, allowing various algorithms to determine the best way to transmit the information back to the network controller or join point. The purpose of a join point is to connect two different communication mediums in order to provide a reach-back link to the Internet or some other robust communication backbone. All nodes within a wireless MESH act as routers to provide multiple transmission paths from each node to the join point. The MESH can be made infinitely robust by the addition of nodes, which directly affects its scalability.

Various protocols have been designed for wireless MESH communication. There are basically two categories of protocols; proactive and reactive. In proactive routing, all nodes in the network constantly maintain and update tables for routes between certain source-destination pairs, regardless of whether these routes are needed. On the other hand, in a reactive routing protocol, routes are discovered based on the demands of source nodes initiating data for specific destinations. In this case, the routing tables are only updated when a route is requested. This on-demand reactive route discovery often leads to long latency, making it ineffective for real-time applications. As a result, proactive routing protocols can deliver data packets faster than reactive routing one because no discovery time is required. However, the disadvantage of proactive protocols is that the network overhead required to maintain current routing tables takes up valuable bandwidth, thus, reducing the maximum bandwidth available to the sensors in the MESH. As one can see from Figure 1, there are a number of Ad Hoc protocols to choose from.

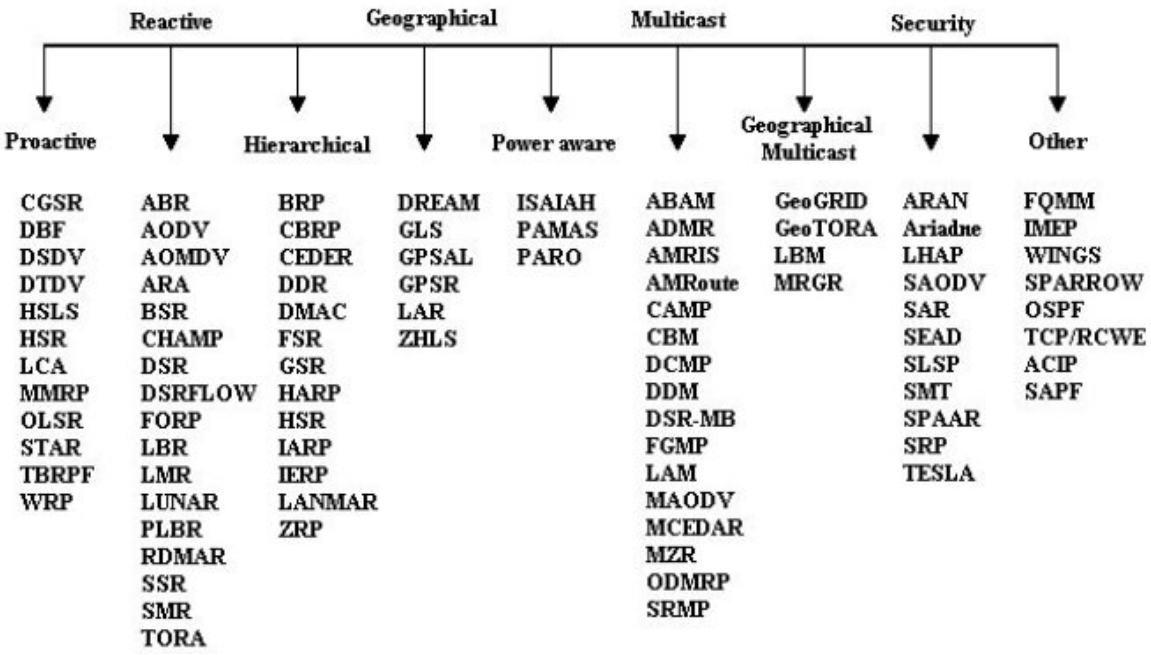

Figure 1. Various Ad Hoc Routing Protocols (From Halvardsson and Lindberg)[1]

In today's military, situational awareness (SA) and ability to effectively communicate is mission essential. Sensor networks with ad-hoc networking capability offer a rapidly deployable, reliable and inexpensive solution to this requirement. In the context of the TNT at NPS, the sensor network, as shown in Figure 2, is a subset of the wireless MESH network, in which the sensors act as nodes of the wireless network. A sensor network is a conglomeration of sensors, in which each is capable of receiving and transmitting information to and from a base station, gateway or data collection point.

[1] Mattias Halvardsson and Patrik Lindberg, "Reliable Group Communication in a Military Mobile Ad hoc Network," Master's Thesis, Vaxjo University, February 2004, p.15.

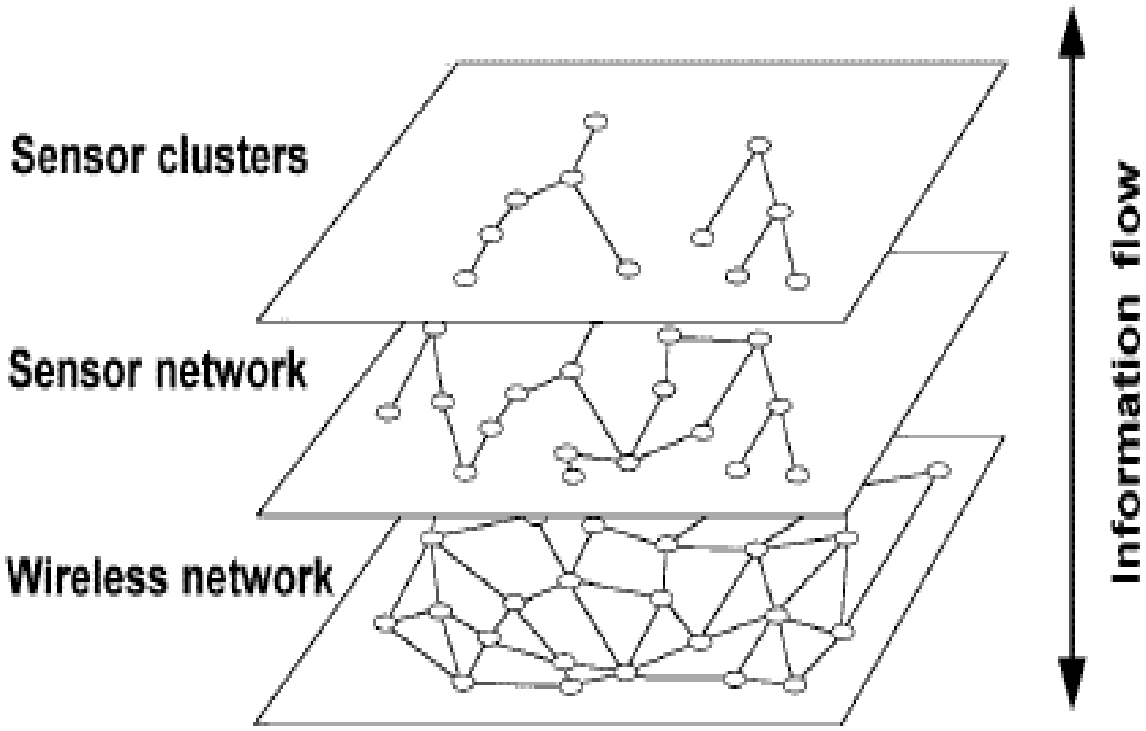

Figure 2. Three conceptual layers in a wireless sensor network (From Distributed Sensor Processing).[2]

To further illustrate this concept, the human body could be thought of as a sensor network. The sensors are the nose, fingers, eyes, ears, and tongue, and the brain is responsible for collecting and processing the data (smell, touch, sight, hearing, and taste) received from its sensors. The nerves within the body represent the medium through which the sensors pass information back to the data collection point (brain). In this example, the efficiency that the brain processes this data is analogous to network performance.

The combination of sensors and wireless technology can provide real-time monitoring, precise location information, and threat data. The fact that sensors are inexpensive and can be deployed in large quantities which require low installation costs

[2] Van Dyck, Robert E. and Miller, Leonard E. Distributed Sensor Processing, "Over An Ad Hoc Wireless Network: Simulation Framework and Performance Criteria," <http://w3.antd.nist.gov/pubs/milcom01.pdf> Last accessed 02 January 2005.

make them a viable SA solution for network centric warfare in a tactical environment.[3] Typical DoD sensor applications include surveillance, security, motion, environmental (chem/bio), and atmospheric. Specific sensors that are used in NPS's TNT will be discussed in later chapters.

2. Advantages of Wireless MESH

There are many attractive features of wireless MESH networks that make them a viable networking solution in a tactical environment. The multi-hop feature of wireless MESHES, which enable all nodes to serve as routers or access points, gives them several advantages over other networking schemes. If the nearest AP or neighbor is congested, a new route is formed to next closest node with the least amount of traffic. This method, known as hopping, is repeated until the data reaches its destination. Wireless MESHES work on the same principle as the Internet, which is just a wired multi-hop network. When email is sent via the Internet, the journey to the recipient involves hops to many servers. The routes are mainly dependent on network traffic density. The email may hop from west to east and then back to west before reaching its final destination in the Midwest. The journey is much longer but more efficient and faster.

One MESH advantage resulting from its multi-hopping phenomena is redundant continuous communication links. Redundancy, in turn, brings priceless reliability and availability that is required in a tactical operation environment. The fact that a wireless MESH gets stronger when more and more nodes are added results in the additional advantages of scalability and robustness. By scalability, I mean the MESH's ability to expand the number of nodes without making major changes to the system or application software. Because a wireless MESH is not dependent on the performance of any one node, it is naturally robust. In MESH architecture, if a node is unable to detect its routing neighbor, data will be routed along an alternative path and MESH network will continue to function.

The final two advantages are two of the most important. The self-forming advantage of a wireless MESH enables quick and easy setup, which is required in a tactical application. Self-forming is made possible by the ad hoc mode, which enables

[3] Innovative Wireless Technologies, "Sensors Networks, wireless sensor network development," <http://www.iwtwireless.com/SensorNetworks.htm>, Accessed 11 November 2004.

every node to form and join the MESH as soon as they have power and a radio signal. Lastly, the self-healing technique of MESHES stands as the most valuable benefit of wireless MESHES. As nodes enter and leave the network, routing tables are continually updated, and routes are recalculated.[4]

3. MESH Constraints

Although wireless MESHES show great potential for use in military tactical environments, there are still many issues facing its eventual DoD GIG implementation. Some of the challenging problems that still need to be addressed are coexistence, interoperability, bandwidth prioritization, security, and quality of service.

In network centric warfare environments, there will potentially be multiple networks on the battlefield within radio range of one another, the MESH network must be able to coexist with surrounding networks with little of no effect on network or sensor performance. To ensure maximum battle readiness, we must develop a way for competing tactical networks to cooperate routinely, with a minimum manual intervention

Another technical obstacle that must be addressed is interoperability. The MESH must be able to interface with numerous devices that have different types of radios. A solution proposed by the Intel Corporation is to put reconfigurable radios at the device level that would allow for adaptation to different wireless environments. This technique would cost a lot less than putting multiple radios each device.[5]

Additionally, bandwidth prioritization also must be addressed. Network transmissions are generated by a variety of applications including; VoIP, video, SA, encryption, and protocols. Each application produces an assortment of data traffic patterns and has different bandwidth requirements. A method needs to be developed to automatically determine which applications have bandwidth priority on the network, and subsequently assign those priorities appropriately.

Finally, the last and maybe most significant wireless MESH constraint, is the matter of security and privacy. If a MESH is to be truly valuable in tactical situations,

[4] Conner, Steven and Gryder, Roxanne, Technology @ Intel Magazine "Building a Wireless World with MESH Networking Technology" <http://www.intel.com/update/contents/nc11032.htm> Last accessed 12 December 2004.

[5] Gelsinger, Pat, Intel, "Catching up with Radio Free Intel," <http://www.intel.com/technology/comms/cn09031.htm> Last accessed 13 January 2005.

security has to become a vital concern and not an afterthought. "Security is a vital part of any wireless network and is an increasingly important issue as adoption of last mile technologies, such as MESH networking, mature and become more widespread," commented Wai Sing Lee, a security consultant at Frost & Sullivan.[6] The MESH security solution must not add unnecessary overhead to a network, in which bandwidth is already at a premium. MESH security has to be both, transparent and ubiquitous, in order for this technology to reach its full potential.

All of the above issues have to be addressed in order for wireless MESH technology to be fully implemented into the network centric warfare arena, which in turn will lead to the highest available QoS for the sensors of the tactical network.

B. MESH QUALITY OF SERVICE

1. Sensor QoS in a MESH Network

QoS is a direct indication of the "Health" of a network. In the context of this thesis, QoS is a collection of procedures and protocols that ensure that a wireless MESH network can provide and maintain the required resources for optimal sensor functionality in the tactical environment. It is essentially a guarantee that at any given time, an application will be able to satisfactorily transmit data in an acceptable time frame without delay, distortion, or loss.[7] The primary mission of QoS is to provide confidence in the ability of a network to deliver predictable results. The ability to consistently provide dependable availability, minimal latency, bandwidth, and packet loss requirements is essential for MESH implementation in the tactical network.

2. QoS is Essential in a Tactical MESH Implementation

Because of the advantages that new technology brings to the battlefield, military personnel have become increasingly dependent on the proper operation of their equipment. As a result of this reliance, it is more important than ever that repair kits, equipment, and even tactical networks function as advertised. Degradation in network performance at the wrong time could result in intolerable consequences when taken in

---

[6] VIA Technologies, INC, "VIA and LocustWorld Secure Wireless MESH Networks with VIA PadLock High-Speed Encryption," <http://www.via.com.tw/en/resources/pressroom/2004_archive/-pr040923lw_secureMESH.jsp> Last accessed 29 November 2004.

[7] Microsoft, "Quality of Service," <http://www.microsoft.com/resources/documentation/-Windows/2000/server/reskit/enus/Default.asp?url=/resources/documentation/windows/2000/server/reskit/en-us/cnet/cndc_qos_WQCI.asp> Last accessed 23 January 2005.

context of a military engagement. QoS has become a key area of research and development in network performance and management. Applications have various requirements for throughput, latency and packet loss. But those such as video, VoIP, SA, and other network customers require a large amount of uninterrupted bandwidth to function properly, and therefore can overload existing network resources. In turn, this will result in overall performance network degradation, which leads to low throughput, excessive latency and high packet loss. Network bandwidth is a critical resource, especially on a wireless sensor MESH tactically deployed as an integral part of the network centric backbone. Accordingly, the use and allotment of bandwidth is of grave consequence to the proper management of the network. Because network resources are so valuable in tactical network applications, the implementation of QoS is vitally important to ensure proper network management of tactical wireless MESHES.

3. QoS Goals in a Wireless Tactical MESH

In any significant network, a network manager is assigned to manage network performance, resources, and costs. In a tactical MESH network, the network management role is equally important, if not more paramount. The technological equipment that is now being produced is very reliable and dependable. More often than not, the proper operation of the equipment depends more on the robustness of the networking infrastructure than the quality of the product. To address the network performance required by deployed sensors in the tactical network, the associated MESH network must be managed to achieve the desired QoS that is demanded by the sensor clusters that the MESH network serves. The resulting QoS-enabled tactical network provides sufficient resource guarantees for congested MESH sensor networks that have high bandwidth, low latency requirements. Therefore, it is vital that a network monitoring system be deployed as part of QoS, to insure that networks are performing at the desired level. The network monitoring system of the tactical wireless MESH network should make every effort to achieve three primary goals of QoS in order to provide reliable network performance for deployed sensors in the field.

The first and overarching goal of tactical wireless MESH QoS is to track the overall health of the network, and identify performance problems of the network. The second goal is to develop a method for the network to discriminate between data packets

and allocate suitable network services based on bandwidth, latency, and packet loss rate. As a consequence of data packet discrimination, QoS can achieve its third goal of prioritizing services resulting in the most efficient use of network bandwidth when servicing deployed resource-demanding sensors. Meeting these primary QoS goals will provide a robust MESH network that guarantees maximum available bandwidth, low latency and low packet-loss of critical sensor data gathered from the tactical environment.

4. Challenges to QoS with Respect to Wireless MESH

There are many similarities between wired and wireless MESH networks, but there are some unique characteristics of a wireless MESH that needs to be addressed in order to implement a successful QoS-enabled sensor MESH network into a tactical environment. The first distinctive characteristic of wireless networks is unstable and irregular signal propagation. This is due to a number of reasons: fading, reflection, and interference due to band bleed, unlicensed bands and inclimate weather. The physical environment has a significant impact on wireless communication.[8] Consequently, link quality between nodes in MESH networks vary over time. This wireless characteristic leads to poor and unreliable network performance, and thus results in a network that is unable to provide QoS to the customers of the network (i.e. sensors). To overcome this wireless challenge, the wireless MESH industry has responded by developing new protocols that operated based on link quality instead of proximity of neighbor nodes. Wired networks don't suffer from this phenomenon because of the stability and solidity of its physical link layer medium (CAT 5).

Another major challenge to the wireless MESH is also one of the major advantages of the MESH; the mobility of its nodes. This is a very taxing characteristic for QoS purposes. Because some of the sensor nodes in the MESH network are mobile, the data paths continually changes. This places a constant drain on the QoS requirements and requires the addition of necessary overhead on the network, which takes up valuable bandwidth. Unlike traditional wired networks that achieve QoS support by managing the network resources and applying admission control to new flows, the wireless MESH is unable to use this wired QoS procedure because it requires a stable and known data path

8 Mobile Computing Group, "QoS in Wireless MESH Networks," <http://www.sce.carleton.ca/wmc/QoSZAP/>, Last accessed 22 October 2004.

in order to maintain network flow control.[9] To overcome the wireless MESH mobility challenge, appropriate and efficient QoS solutions must take node mobility into account during the development of QoS solutions, instead of trying to fit them to the MESH as an afterthought.

[9] Mobile Computing Group, "QoS in Wireless MESH Networks," <http://www.sce.carleton.ca/wmc/QoSZAP/>, Last accessed 22 October 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SELECTION OF MESH NETWORK METRICS

A. ATTRIBUTES OF A GOOD METRIC

A metric is a "meaningful measure of the extent or degree to which an entity possesses or exhibits a particular characteristic."[10] It is designed to objectively measure and provide predictive behavior of desired attributes of a system. Many attributes contribute to a useful metric. There are numerous metrics definitions and purposes, but good performance metrics have several key characteristics in common.

The first characteristic of good metric is that it can be observed and monitored over time. Snapshots of systems simply provide information of what has occurred in the past. In network performance, historical information is useful, but information that gives the capability of prediction and adjustment on-the-fly is much more valuable in network centric applications. Metrics that can be tracked and graphed allow you to see trends, which provide vital visual characterization of network performance. The resultant network depiction makes it easier to forecast network behavior and make adjustments (i.e. sensor locations) to maximize network performance. Another quality of a good metric is that it consistently measures the same item. This is crucial for comparison and trend analysis purposes. Changing what is included in the metric after the outset of data collection invalidates the entire measurement process. For example, throughput measurements must use the same packet size in order to properly analyze bandwidth behavior. The next trait of a good metric is that once it is analyzed, something can be done to change it if necessary. For example, if latency is too high, there needs to be some action that can be taken to change that metric. If not, an out-of-bounds metric simply provides useless data. When a network measure falls outside desired network performance, it should generate an action to remedy the situation. Finally, a good metric is able to be benchmarked amongst similar systems for comparison purposes. For example, the throughput of a wireless MESH can be further analyzed when compared to a wired network throughput.

---

10 DACS, "A History of Software Measurement at Rome Laboratory," <http://www.dacs.dtic.mil/techs/history/His.RL.2.2.html>, Last accessed 12 January 2005.

Valuable network performance metrics are functional, timely and consistent. The QoS of a network is a function of the metric values of that network. As the primary measure of network QoS, metrics provide an indication of how well the system meets customer expectations. Good network performance metrics provide a complete picture of network quality. They enable further network analysis and allow entry into models which result in predictable network behavior and dependable QoS.[11]

B. TNT MESH METRICS

Successful measurement of the general performance of the TNT wireless MESH network was achieved through exhaustive data collection and modeling of QoS indicators. The metrics that provided the best indication of TNT MESH performance were chosen because they potentially offered the best predictability analysis and exhibited most of the characteristics of good metrics pointed out in the previous section. These metrics provide the foundation for the development of tools that will provide an instant dashboard picture of MESH network performance. This result could lead to the development of a tactical MESH plan of action that will facilitate the immediate resolution of MESH performance discrepancies, possible before they occur. The modeling of TNT performance metrics will instantly show network trends that make real time network performance planning possible, and consequently valuably contribute to command and control battle plans for the troops in the field. The metrics that were utilized as input for the modeling that I employed are critical to forecasting the efficiency and effectiveness of tactically deployed wireless MESH networks.

The first metric that I analyzed and used as a basis for MESH network modeling was throughput, which is probably the most essential attribute of the TNT wireless MESH. Video and audio services generally require a significant amount of bandwidth for reliable performance. Providing the optimal amount of throughput directly relates to the performance of multimedia sensors deployed in the field. Consequently, it is easy to see that the primary factor that influences MESH deployment topology is throughput. The next metric that I examined and modeled was packet loss. An increase in packet loss is often an indicator of the degradation of other critical network performance

[11] Sanjiv Bhardwaj, Demand Solutions, "The Performance Metrics Three-Legged Stool," <http://www.demandsolutions.com/pdf/ds_mag/fall_03/metrics.pdf>, Last accessed 22 November 2005.

measurements. Packet loss is usually caused by network traffic congestion. This, in turn, results in overflowing router queues and dropped packets. Since every node is a router in the MESH, this packet loss can be a major QoS problem. Packet loss can also result from bit errors caused by various link imperfections and improperly functioning network equipment.[12] The final metric that I used for contribution to MESH network modeling is the latency. For the purposes of this thesis, latency, delay and response time are essentially the same. Latency is the amount of time it takes for a set amount of data to be transmitted from one point to another. Although there are various types of latency, this thesis will focus on distance latency, because it is the parameter which can be controlled the easiest during network performance experiments. Additionally, distance latency can be affected by manipulating throughput, as opposed to other latency types, because of the various acknowledgements and handshakes associated with them. This metric is critical in one of the most commonly used tactical applications, VoIP. High latency results in more jitter, which is a performance measure of the quality of telephony applications. Using the metrics of throughput, packet loss and latency as the primary criteria for MESH model development will allow the establishment of baselines for predictability analysis of the TNT MESH. The resultant MESH modeling may lead to proper network centric planning, which, in turn, will result in maximum tactical efficiency of deployed MESH networks in the battlefield.

[12] Cottrell, Les, Matthews, Warren and Logg, Connie, Stanford Linear Accelerator Center, "Tutorial on Internet Monitoring & PingER at SLAC," <http://www.slac.stanford.edu/comp/net/wan-mon/tutorial.html>, Last accessed 21 February 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DEVELOPMENT OF MATHEMATICAL MODELS USING MULTICRITERIA ANALYSIS

A. COLLECTION OF OBSERVATIONAL DATA

1. General Data Collection Philosophy

In collecting observational data to be used to construct mathematical models, I needed to focus on the criteria of interest that I wanted to predict and analyze. Several important requirements were emphasized during MESH network performance data captures. Having a very large number of observations was the first requirement for data collection. This is the basis for a high-quality predictive model which provides realistic performance estimates in the post-analysis phase. My general rule of thought was that at least 500 observations were required in order to have a valid experiment. For example, if the condition that I want to predict (e.g. network health) depends on 100 parameters, and I collect only 30, it is very difficult to learn any approximating functions with this amount of inherent error. An additional data collection requirement was to choose consistent network characteristics that I could capture from several different types of experiments for comparison sake. For example, if I asked someone to forward me throughput, latency and packet loss data from an experiment, there would be little confusion about the requirement. In cases where some data was missing, but there were still enough observations to yield a reasonably valid conclusion, statistical imputation algorithms were applied.

2. Data Collection Sources

a. Situational Awareness Database

The first source of data that I collected for MESH network performance modeling purposes was from the SA database that was designed by Eugene Bourakov, a research associate at Naval Postgraduate School in Monterey, CA. The primary purpose of the SA tool is to provide instantaneous shared awareness to various stakeholders at geographically separated sites. Its secondary purpose is to monitor SNMP data and depict throughput and link health of the TNT. The database automatically captures network performance data every five seconds from all sensors and nodes that are connected through its 802.16 (OFDM) backbone. As part of this database, an event log

(Figure 3) was added to help corroborate what was actually happening during the period of time that the evaluated data was captured. Information, such as, range between nodes, the number of MESH nodes, and video/audio quality were used as control variables in MESH network performance modeling efforts. Formerly, we had to depend only on screen captures and photos for post-analysis of experiments.

Figure 3. SA Data collection entry page (From the GIGA Portal Page)

b. IxChariot

The next data capture tool that I used was IxChariot. Developed by Ixia, IxChariot is a traffic pattern analysis and decision support tool emulating real-world application data without the need to install and maintain extensive client/server networks. Incorporating the IxChariot Console, Performance Endpoints, and Application Scanner, the IxChariot family offers thorough application assessment and device testing by emulating hundreds of protocols across thousands of network endpoints. IxChariot provides the ability to predict the expected performance characteristics of any application running on wired and wireless networks. It is operated from a Console program that

creates and runs tests between endpoints on the network, as depicted in Figure 4. Each test uses an application script that, in conjunction with the endpoints, creates the same data flows that actual applications would generate. Upon completion, a summary of the test results is provided that illustrate the maximum, minimum and average throughput, response time, and transaction rates. These tests and data will provide the means for network modeling and drawing conclusions for the link characteristics of the evaluated network.[13]

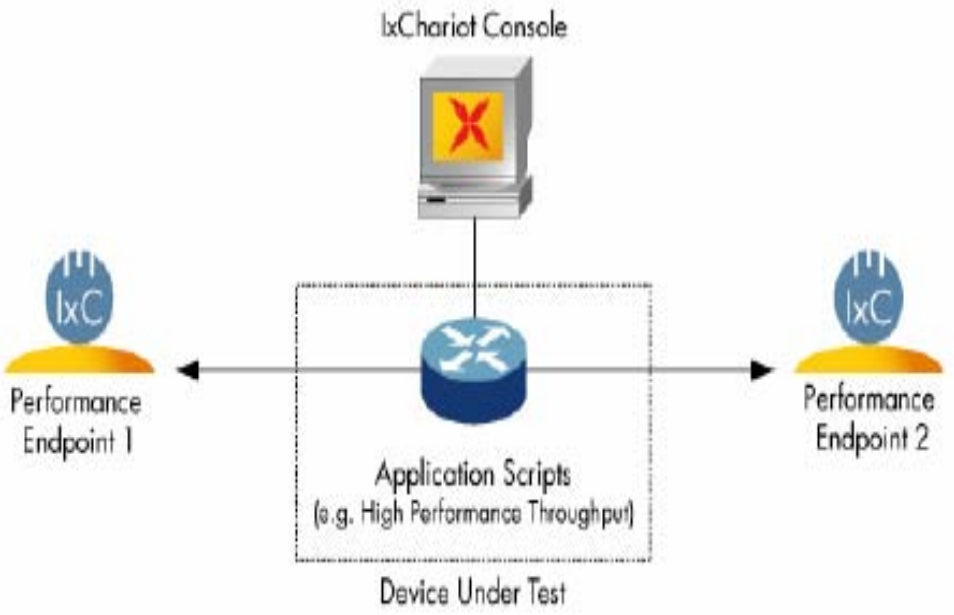

Figure 4. Example of IxChariot test setup (From IxChariot Performance Testing)[14]

c. SolarWinds

SolarWinds is a collection of basic network management tools to handle many aspects of a network. SolarWinds possesses a very robust set of fault and performance monitoring tools. Among the many valuable tools in the SolarWinds suit are Ping, Diagnostic, Trace Route, and IP address Discovery and Management. The main tools that I utilized for data capture were the Network Monitor, SNMP Graph and

[13] Ixia, "Performance Testing IxChariot," <http://www.ixiafederal.net/datasheets/pdfs/-pa_ixchariot.pdf> Last accessed on 21 February 2005.

[14] Ixia, "Performance Testing IxChariot," <http://www.ixiafederal.net/datasheets/pdfs/-pa_ixchariot.pdf> Last accessed on 21 February 2005.

Bandwidth Gauge. The Network Monitor is a fully interactive management application that allows one to monitor selected devices and send alerts on outage conditions. The Real Time Bandwidth Gauge application is a real-time traffic monitor and provides historical graphing, as well. The resulting combination of these tools was a real-time data collection and graphing tool capable of graphing data from any MIB (Management Information Base) simply by selecting the device and the desired OID (Object ID). It monitored parameters such as; throughput, VoIP, latency, packet loss rates, and a great deal more.[15]

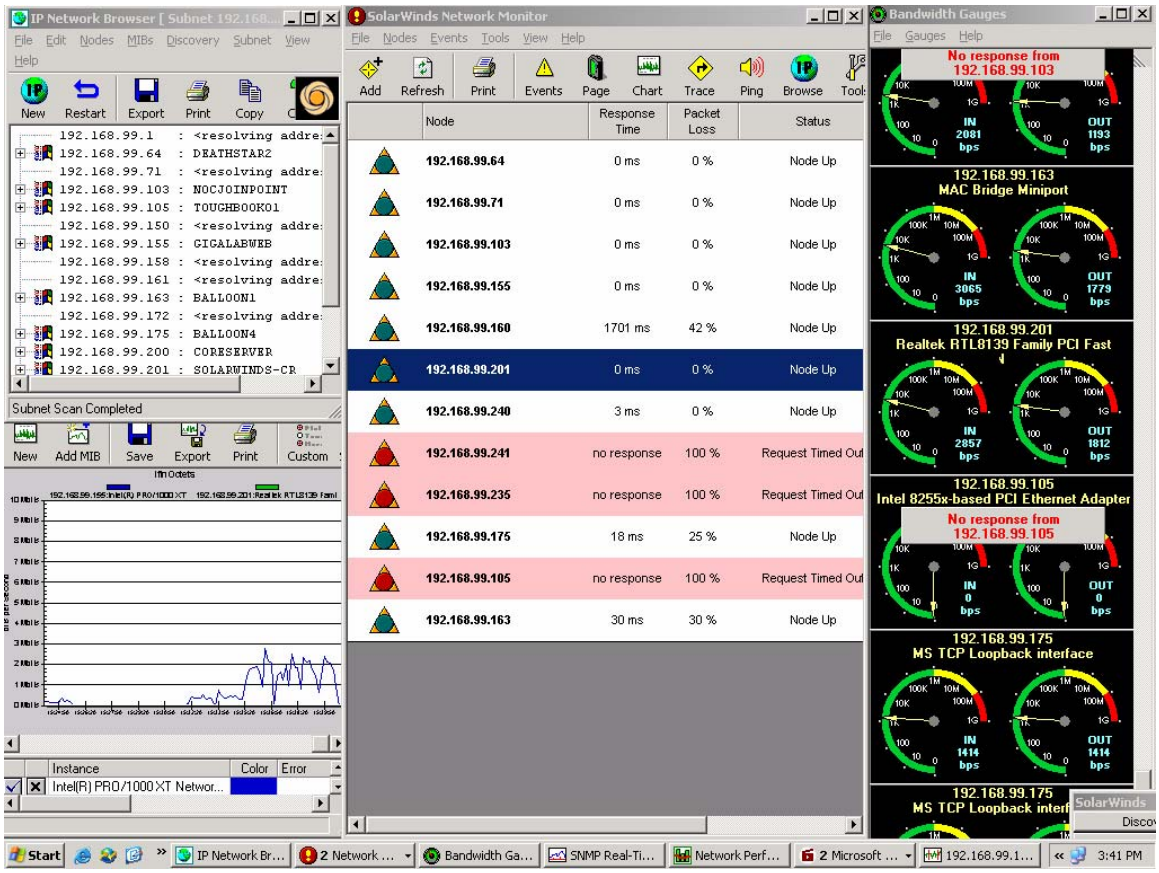

Figure 5. SolarWinds Network Monitoring and Data Capture Screen

15 SolarWinds, "Network Management & Discovery Software," <http://www.solarwinds.net/>, Last accessed 21 February 2005.

B. OVERVIEW OF MULTICRITERIA ANALYSIS

Multicriteria analysis (MCA) is a process and a procedure that provides a list of prioritized options, from the most ideal to the least desired option. In MCA, each option in the criteria set is evaluated, with no option being the obvious solution of choice. Additionally, some horse-trading is frequently required to deduce the most equitable solution.[16] To achieve the most efficient solution, it is vitally important that the criteria are quantifiable and their results measurable for every assessment option. This will result is a foundation of rational comparison of alternatives in a deliberate manner. After deliberate consideration, the most optimal choice is selected as the solution.

Mathematical program models that have the ability to consider numerous objectives simultaneously are very valuable devices and proficient in figuring out the best solution from a multitude of conflicting options. The goal of MCA in this thesis is to provide TNT MESH stakeholders with a predictability tool for MESH network performance within the TNT. Consequently, we will have the ability to predict, in advance, network risks and vulnerabilities which will facilitate making the best possible network centric decisions regarding the topological deployment of wireless MESH sensors in tactical environments.

This overview is meant to be only a basic description of MCA. The purpose of MCA in the context of this thesis was to use it as a tool to test hypotheses of experiments. Further details concerning multicriteria analysis are beyond the scope of this thesis.

C. MULTICRITERIA ANALYSIS OF A MATHEMATICAL MODEL

1. Determination of the Pareto Optimal Set

Multicriteria analysis was founded on the thinking of Vilfredo Pareto (1848--1923). He was an Italian classical thinker, expert in both economics and sociology. He was the first to make the distinction between cardinal and ordinal utility. He also presented the idea that one can handle the analysis of economic equilibrium with ordinal utility. Pareto's work on the foundation of what today is called welfare economics is another example of his impact on later generations. However, what most people know

16 "DTLR multi-criteria analysis manual," <http://www.odpm.gov.uk/stellent/-groups/odpm_about/documents/pdf/odpm_about_pdf_608524.pdf>, Last accessed 23 January 2005

about his works is the "Pareto-optimum."[17] According to Ameya Kamerkar and Yugendra Bhide, “a point is said to be Pareto optimal if, at that point any attempt of improvement in one of the objective functions from its current value would cause at least one of the other objective functions to deteriorate from its current.”[18] Pareto optimal designs cannot be improved in more than one criterion simultaneously. An example of this type of solution is depicted in Figure 6. Improvement in one criteria leads to deterioration in the others. For example, when choosing to purchase an automobile, a buyer desires the largest car with the best gas mileage. In this example, size and gas mileage are the criteria of concern. The point at which he is equally satisfied with both the vehicle size and the gas mileage is considered to be a Pareto optimal solution. Getting a larger vehicle decreases gas mileage and getting better gas mileage decreases the acceptable vehicle size.

[17] Aspers, Patrik, “Crossing the Boundary of Economics and Sociology: The Case of Vilfredo Pareto,” <http://www.findarticles.com/p/-articles/mi_m0254/is_2_60/-ai_75451916>, Last accessed 1 March 2005.

[18] Aspers, Patrik, “Crossing the Boundary of Economics and Sociology: The Case of Vilfredo Pareto,” <http://www.findarticles.com/p/-articles/mi_m0254/is_2_60/-ai_75451916>, Last accessed 1 March 2005.

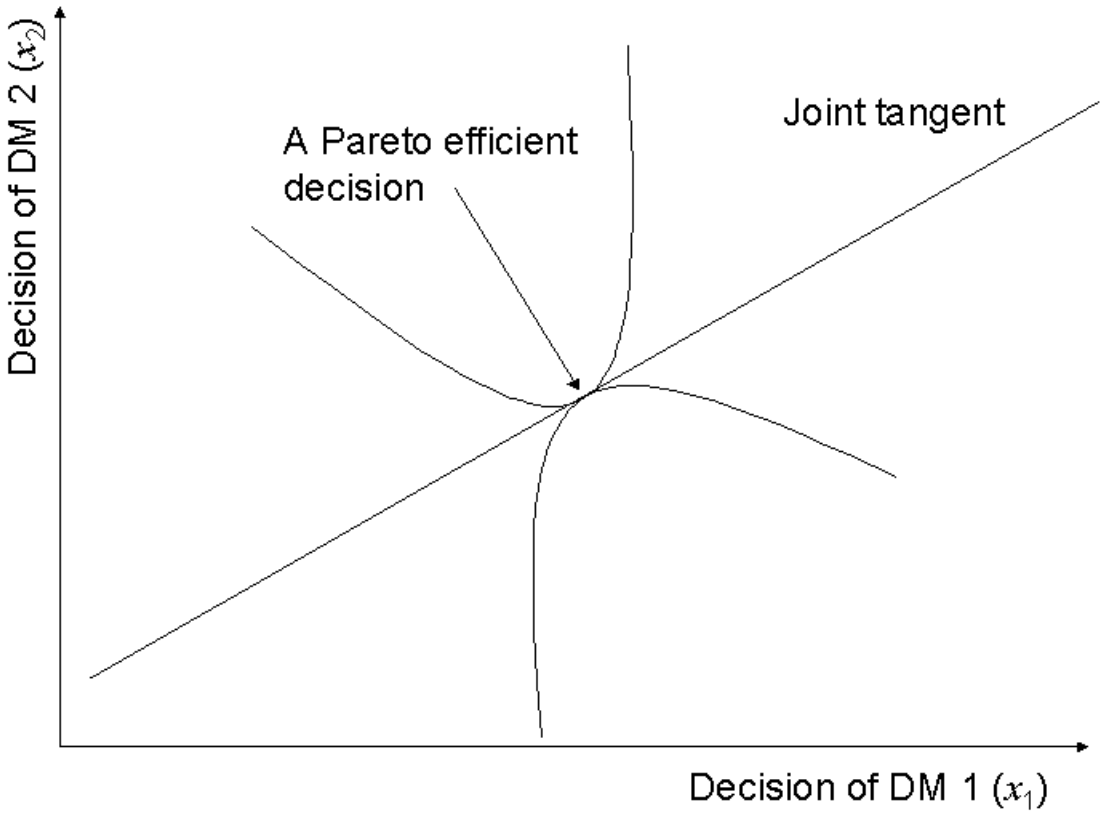

Figure 6. Example of a Pareto Optimal Design (From SAL Research) [19]

When examining a set of Pareto solutions, we know what can and cannot be achieved and consequently, we are able to choose the most preferable option of the set because there are no better solutions. We generally have to compromise and trade between criteria in order to get a solution that satisfies most of what is needed. In order to get the most out of Pareto optimal design solutions, the key decision makers must be knowledgeable about what is desired, what is needed, and what is acceptable. This will enable them to know how recognize Pareto optimal solutions when presented with them. They must also understand that a Pareto approach is by design a negotiation process, which is a necessary condition that allows the mitigation of risks and best solution.

[19] Systems Analysis Laboratories, "Dynamic games, large scale systems and optimization," <http://www.sal.hut.fi/Reasearch/index1.html>, Last accessed 1 March 2005.

2. Development of Mathematical Models

A model is a representation of the structure of some entity, process, or event in the world. Much of the facts and comprehension that we have learned about the world has been because of models. One of the main purposes of models is prediction and control of the environment in which we live. The particular model that I used in this thesis work was that of a symbolic nature, consisting of mathematical approximation equations.

The goal of the mathematical models was to construct functions based on observational MESH network performance data. I was interested to see if these functions depended on parameters, namely, throughput, latency and packet loss. My goal was to obtain performance estimates for these functions on data not employed for construction of these functions. In other words, I wanted see if the mathematical models could produce functions that could be used to predict future MESH network performance in tactical deployment situations.

Various types of learning algorithms can be used to construct functions. If the criterion is continuous, which was the case for the data that I collected, algorithms for multiple regression were used. Examples of these types of regression algorithms are:

1. Regression by neural networks[20]
2. Support Vector Machine (SVM) based regression[21]
3. Multiple linear regression[22]

Each of these of these regression algorithms were used in the mathematical models used in my experiments. They can be applied to a variety of data types and are robust enough for dozens or up to thousands of observations. Additionally, these algorithms have each of the following required characteristics:

1. is multivariate – works with multiple variables

---

[20] Wasserman, P. D., "Advanced Methods in Neural Computing ," New York: Van Nostrand Reinhold, pp. 155-61, 1993.

[21] Ronan Collobert, et al. "SVMTorch: Support Vector Machines for Large-Scale Regression Problems," Journal of Machine Learning Research, 1(Feb): 143-160, 2001

[22] Chatterjee, S. and A. S. Hadi. Influential Observations, High Leverage Points, and Outliers in Linear Regression. Statistical Science, 1986. pp. 379-416.

2. can reconstruct highly nonlinear criteria functions
3. handles very large number of parameters
4. can obtain good results even with a relatively small number of observations
5. is not sensitive to noise

I strived to compare the true and reconstructed mathematical models and find out whether the most important dependencies between parameters and criteria and between criteria were preserved or not. This could also be an indicator of the quality of the reconstructed model. Therefore, to evaluate the quality of the models, I used the following four statistical measures of error:

1. mean absolute error
2. mean relative error
3. mean squared error
4. R-squared

The goal of the results were to show that in addition to accurate reconstruction of the mathematical model, dependencies between criteria and parameters were preserved, which is essential for multicriteria analysis.

In using the MCA approach to develop mathematical models for TNT MESH network performance predictability, I hope to lay the groundwork for the development of a robust MESH modeling tool that can be used for network centric planning, as well as, a wireless MESH network performance forecasting tool.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. EXPERIMENTATION AND RESULTS

A. NPS GIGALAB EXPERIMENTS

I performed several discrete experiments at NPS to investigate MESH network performance characteristics. These experiments were usually limited in scope with the goals of observing specific attributes of network performance, comparing protocol features and manipulating configurations within the MESH. I also observed the effective ranges of nodes within the MESH in order to maximize performance. The specific purpose for my last experiment was to test the data capture capability of the SA application (Figure 7) and then secondarily analyze those network performance results. This experiment was also used to establish a network performance baseline for the follow on TNT experiment.

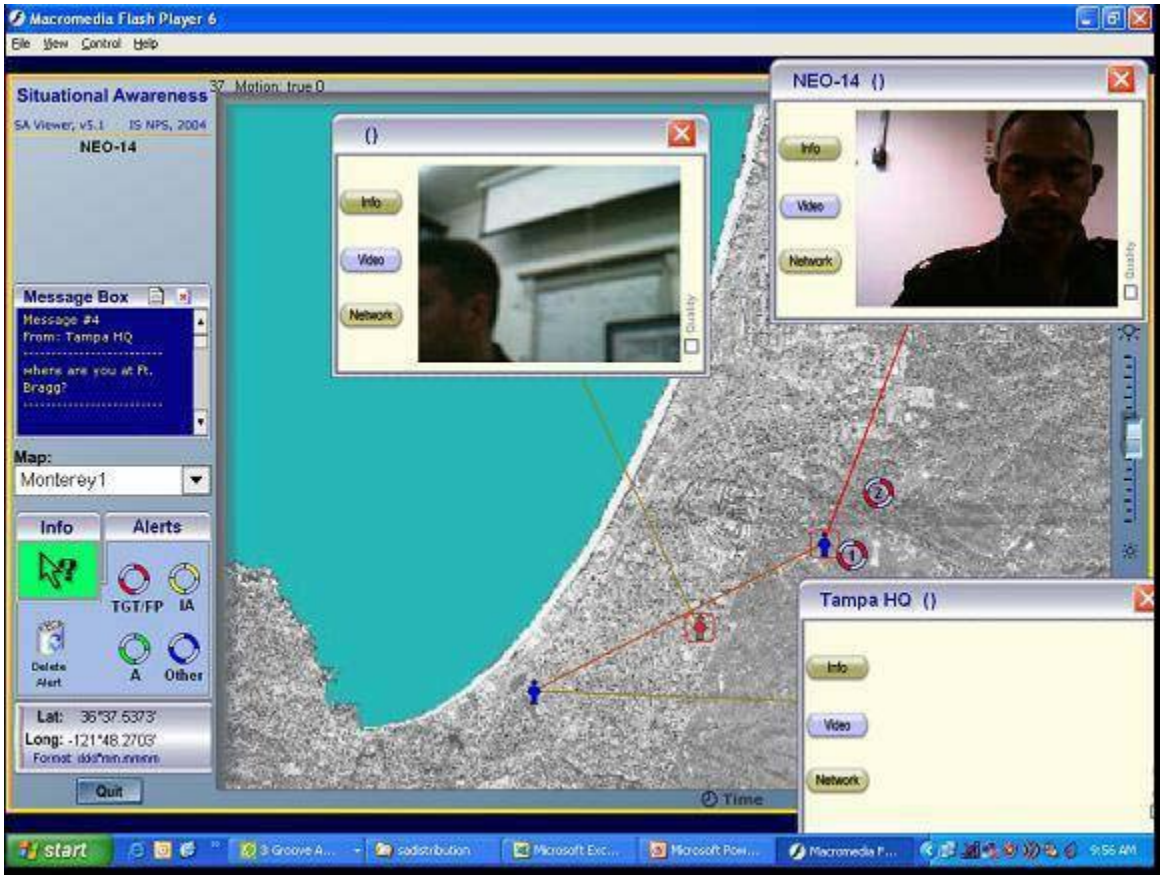

Figure 7. Screen capture of NPS SA application

1. Experiment Scenario

I set up a single cluster of 802.11 wireless MESH nodes in the courtyard of the NPS quadrant with the join point located in the GIGALAB to provide delivery of video and voice applications across the tactical network via the OFDM backbone (see Figure 8). The performance of the MESH network was captured via the Situational Awareness (SA) application and monitored by SolarWinds. Several control variables were altered to observe the resultant effect on network performance.

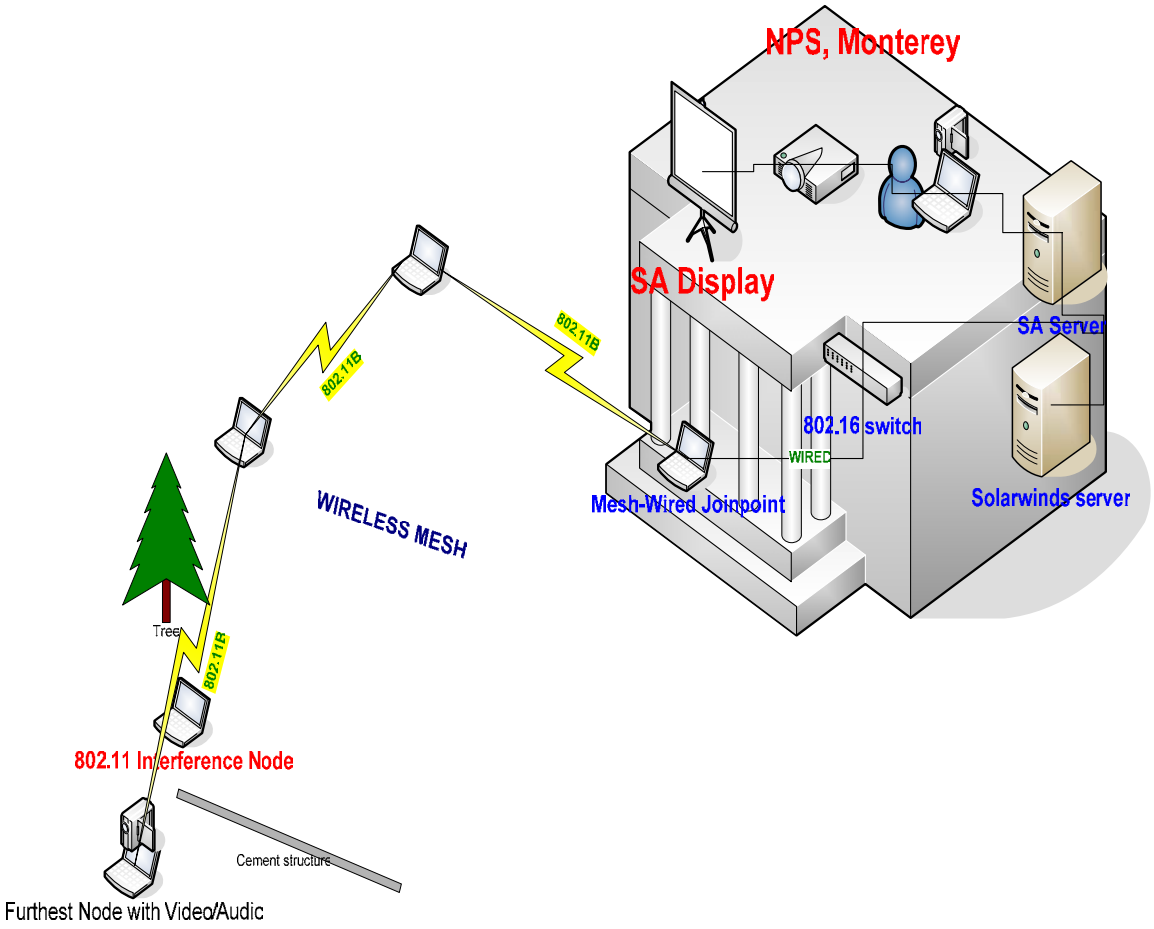

Figure 8. Wireless MESH Schematic

The basic scenario was to set up two wireless MESH nodes outside in the NPS quadrant initially at low transmission power as depicted in Figure 9. I gradually increased the range between the two nodes until MESH connectivity was lost. The

distance between the nodes was measured at that point and entered into the SA database entry log. The procedure was then repeated at full power.

Figure 9. MESH layout at the NPS Quad

Transmission power was again decreased and an additional node was added between the two existing nodes to re-establish MESH connectivity. The video was then started on furthest node. Video quality was noted and annotated in the SA database for post-experiment analysis. The power was again increased and the nodes were separated to ensure hopping. Once more, video quality was noted and annotated in the SA database. At that time, audio was started on furthest node, and the quality was noted and annotated in the SA database. Then, another node was added at full power to increase the robustness of the MESH.

The next control variables that were altered were those that produced interference. To introduce interference into the experiment, I maneuvered nodes behind various physical structures to observe network connectivity and performance of the MESH. The structure type was annotated into the entry log and the network performance was capture in the SA database. To imitate wireless communication interference, I maneuvered a wireless laptop associated to the NPS wireless intranet throughout the MESH. Network performance and connectivity was again noted and recorded. Specific details concerning the experiment are as follows:

2. Equipment Used

- Two Way Radios
- MESH Laptops (3)
  - Dell Latitude X300, 1.40 GHz Pentium M, 648 MB RAM, Wireless ORiNOCO 802.11 Client PCMCIA NIC
- Join point
  - Dell Latitude X300, 1.40 GHz Pentium M, 648 MB RAM, Wireless ORiNOCO 802.11 Client PCMCIA NIC
- Interference Laptop
  - Dell Latitude X300, 1.40 GHz Pentium M, 648 MB RAM, Wireless ORiNOCO 802.11 Client PCMCIA NIC
- SA And SolarWinds Servers
- OFDM Switch –Provided Connection To 802.16 Backbone
- Video Camera – Veo Mobile Connect
- Standard Computer Audio Microphone

3. Communication Mediums

- 802.11B
- 802.16/
- Wire – Standard CAT5 Cable

4. Control Variables

- Number Of Nodes
- Transmission Power
- Position Of Nodes
- Background Noise (Wireless Traffic/Interference)

- Physical Structures

5. Measures of Performance

- Bandwidth/Throughput
- Packet Loss
- Latency
- Video Quality (Frame Rate, Resolution)
- Voice Quality

6. Protocols Used

The Optimized Link State Routing (OLSR) protocol is a relatively easy proactive ad hoc MESH protocol to use. The specific version of the protocol that I used for this particular experiment was OLSR 4.7. This release featured a windows graphics user interface (GUI), displayed in Figure 10, a wireless LAN interface and some of bug fixes from previous versions. OLSR is table-driven and uses the link-state scheme to distribute topology information. As a proactive routing protocol, it maintains a full and current routing table, whether the routing information is requested or not. The optimization of the protocol is realized by a Multi-Point Relaying (MPR) procedure that is used for message flooding.[23] MPR reduces the number of duplicate retransmissions while forwarding broadcast packets, thereby preserving bandwidth by reducing required protocol overhead. Packet retransmission reduction is achieved by reducing the number of nodes that retransmit packets from all nodes to a subset of nodes.

The updated table data is based on received control message traffic. OLSR defines three basic types of control messages:

HELLO – HELLO messages are transmitted to all neighbors and are used for neighbor sensing and MPR calculation.

TC – Topology Control messages are the link state signaling conducted by OLSR, and are optimized using MPR.

[23] OLSR Homepage, "Ad-hoc and OLSR," <http://www.olsr.org/index.cgi?action=adhoc> Last accessed 1 March 2005.

MID - Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. All IP addresses used by each node are listed.[24]

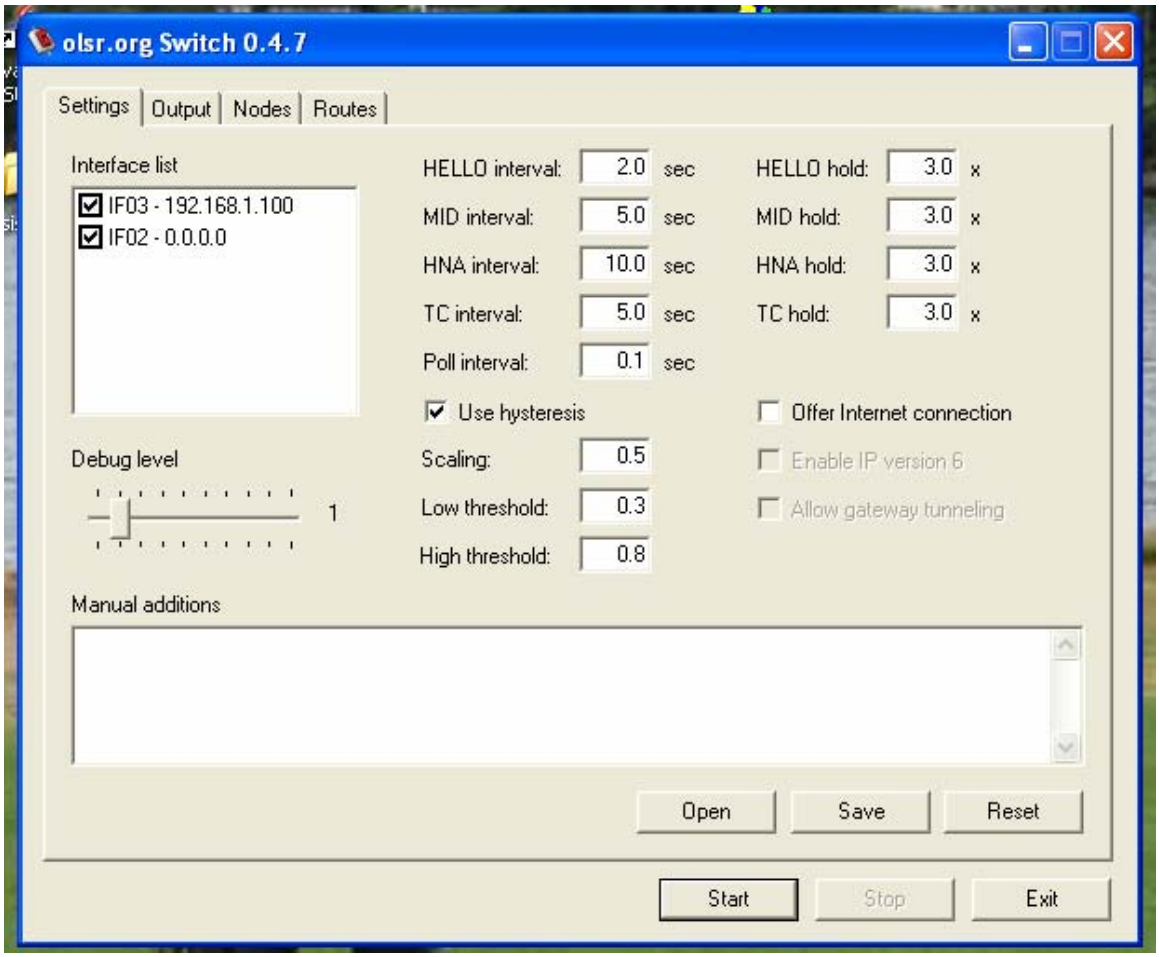

Figure 10. Screenshot of OLSR 4.7 GUI

At the conclusion of the experiment, a data collection of the experiment was conducted from the SA server database and analyzed.

7. Results

As stated before, the primary goal of this experiment was to test the data capturing capability of the SA database, developed by Eugene Bourakov. The experiment proved successful and captured the MESH network performance data of

[24] Andreas Tonnesen, "Implementing and extending the Optimized Link State Routing Protocol," UniK University Graduate Center, University of Oslo, 1 August 2004, p. 8.

concern, namely: throughput, packet loss and latency. The SA entry log also proved to be a valuable addition. It provided additional capability to specifically timestamp the control variables that were used to manipulate the experiment. I was able to tell exactly when nodes were added, range increased, interference introduced and so on. This was a significant value-added tool, especially for the much more complex TNT experiments in the future.

B. TNT 02 EXPERIMENT

1. TNT 02 Overview

NPS's Tactical Network Topology (TNT 02) was conducted 22 February – 08 March, 2005, at Camp Roberts and Monterey, CA. This quarter, the field experiments focused on a multitude of high-level complex tasks as a stepping stone to achieve the ultimate goal of tactical networking interoperability to establish and improve situational awareness in the battlefield arena. To illustrate the complexity of the TNT experimental evolution, below are some of the experiments that were conducted in TNT 02:

- Persistent Air-Based Surveillance
- MESH Topology with Fixed Assets
- Physical Link Variation
- MESH with Mobile Node
- Propagating UAV Control through MESH and SATCOM
- MESH Network Vulnerability Assessment
- Tacticomp MESH Software Evaluation
- Covert MESH Networks
- Information Sharing and Collaborative Action
- 802.16/OFDM Airborne Node with MESH to Tacticomp and SATCOM Reachback
- Light Reconnaissance Vehicle
- Mobile NOC/TOC with Fixed Ground Sensors
- Above and Below Water Situational Awareness for Submerged Diver
- Multi-path Networks

As one can see in Figure 11 below, the TNT is a very complex network. The performance of the MESH network is critical to its successful operation and testing.

Therefore, it is critical to develop and maintain a MESH that is capable of providing a level of QoS that can ensure a robust network.

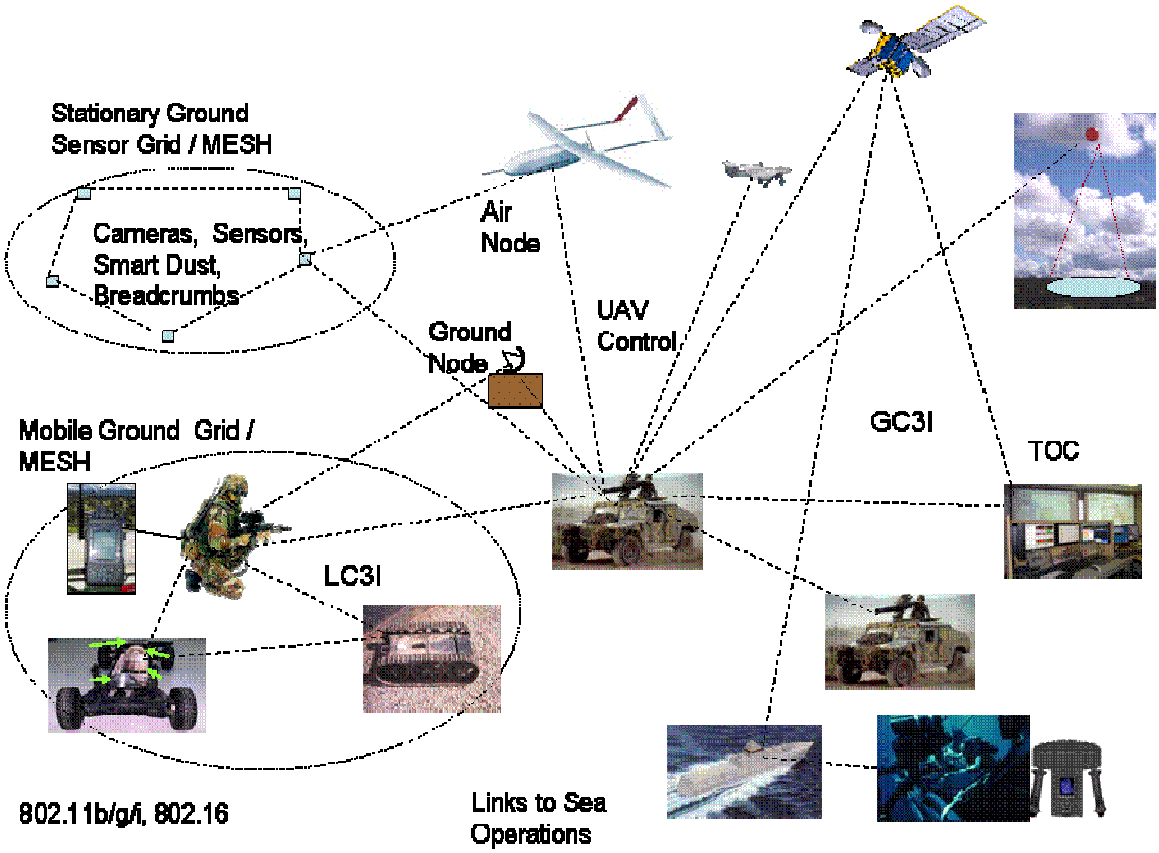

Figure 11. NPS Tactical Network Topography

2. Scenarios

The basic premise of TNT 02 was that future SOF and Marine Corp operations will utilize multiple, dissimilar manned and unmanned air assets to provide situational awareness and enhanced war fighting capabilities. These assets could include tethered balloons/aerostats, UAVs, manned and unmanned airships, and manned aircraft. Some assets are permanent while others may rapidly join and leave the area. Network mobility will be 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 unmanned vehicles and other assets utilizing a minimum number of operating personnel.

3. Objectives

My objective within the TNT 02 experiment was to monitor and capture network performance data for multicriteria analysis in an effort to develop mathematical models. These models will then be used as a foundation for the development of future MESH network predictability tools for deployment and planning purposes of the TNT at NPS.

4. Hypotheses

My primary hypothesis was that there would be statistical relationship between throughput, latency, and packet loss criteria. My derivative hypothesis was that a MESH predictability mathematical model could be constructed from their statistical relationship.

5. Experiment Setup

- Tethered balloons #1, #2, and #3 with light-weight 802.11b payloads and video cameras were deployed for the purpose of persistent surveillance to 2,000 feet above ground level (AGL) approximately 2, 3 and 5 km from the Tactical Operations Center respectively.
- Remote motion detector put within 20' of roadway and pan-tilt-zoom camera deployed on West Perimeter Road, west of FP21, ~5.5 km from TOC. Camera and sensor are non-line-of-sight (NLOS) with any airborne network node, including B#3. MESH Dynamics multi-radio MESH nodes were used for access point to TOC via balloon #3.
- Smart Rock with Iridium-based motion detector located at same location as above detector and camera, but on opposite side of roadway.
- Three cameras with PDA/GlobalStar deployed between field of view (FOV) of remote video camera and FOV of balloon #3 on West Perimeter Road.
- TOC and Light Reconnaissance Vehicle (LRV) SA application tracks and displays all assets and video.
- Pelican, TERN UAV, and NPS small UAV standby to intercept red team intruder. All flights within FOV of 60 degree sector antenna at TOC to maintain MESH connectivity.
- Video and text messaging at TOC provided to Tampa, Ft. Bragg, Lawrence Livermore National Laboratory (LLNL), Ft. Meade, and Office of Force Transformation (OFT).
- LRV maneuvers through MESH cloud with the goal of maintaining MESH connectivity.

Various scenarios were run using multiple configurations of the assets above to test the TNT MESH connectivity and network performance. During the experiments, I used the SA database, SolarWinds, and IxChariot applications to capture valuable MESH network QoS data for throughput, latency and packet loss metrics.

6. Results

The results of my thesis were based off of data captured from 802.11 wireless MESH operations during the TNT 02 experiment conducted February through March 2005. I was assisted in the data analysis phase of my thesis by Roman Statnikov, a Research Assistant at NPS, Monterey and Alexander Statnikov, a student at Vanderbilt University.

a. Multicriteria Analysis

First, I had to establish dependency from the data, and then optimize the criteria. As a rule, criteria should depend on parameters. My goal was to maximize information content in order to produce robust regression models for the chosen criteria.

My primary parameter in the TNT 02 experiment was distance or range between nodes in the MESH. I intended to vary distance between objects and measure criteria (throughput, latency, and packet loss) for each value of the distance. If I could produce data for a very large number of different values of the distance (say, hundreds), I could develop regression models of the criteria of interest provided that distance was indeed significant. One major data gathering obstacle of TNT 02 was that I did not have sole control over most of the parameters due to the shear complexity of the experiment. As a result, even though the range between the nodes was varied from time to time, typically many different values of criteria corresponded to the same range. Thus, I concluded that the criteria depended not exclusively on range, but on other parameters as well. So, I chose to use some criteria as parameters. For example, I tested regression models for different criteria as a function of the others. If it proved interesting, I could utilize the current dataset to build regression models of latency, throughput, and packet size as functions of the remaining three (or less) criteria.

As a result of MCA, the following findings were revealed. Using both multiple linear and generalized neural networks regression, it became very apparent that there is a dependency relationship between packet loss and throughput. Figure 12 shows

the results of the multiple linear regression tests, which demonstrate a correlation between these two criteria. An R-squared value of 0.803057 means that there is an 80% chance that packet loss and throughput show a relationship. A high R-squared value along with a low mean relative error (uncertainty) of 24% shows strong evidence of data correlation. An additional data test using multiple linear regression (Figure 13), also supports that evidence with an R-squared of 78%.

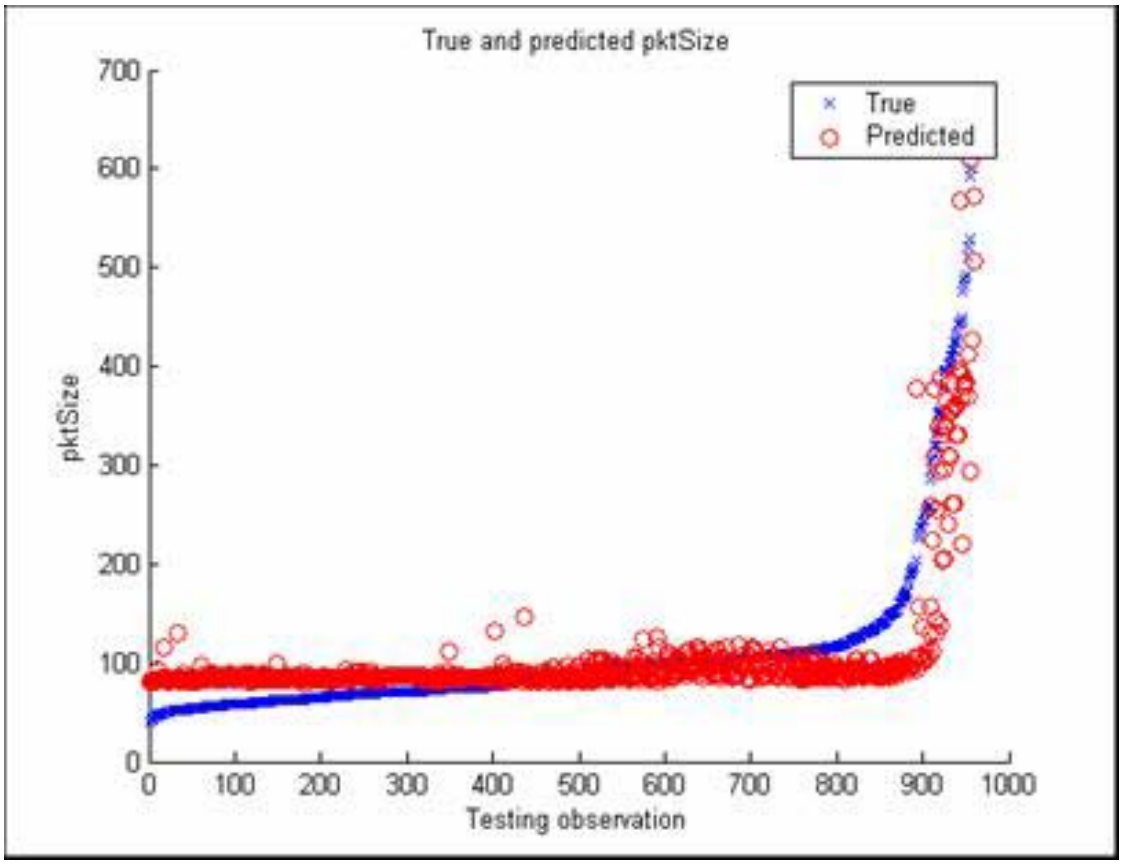

Figure 12. Prediction of Packet Size as a function of Throughput using Multiple Linear Regression

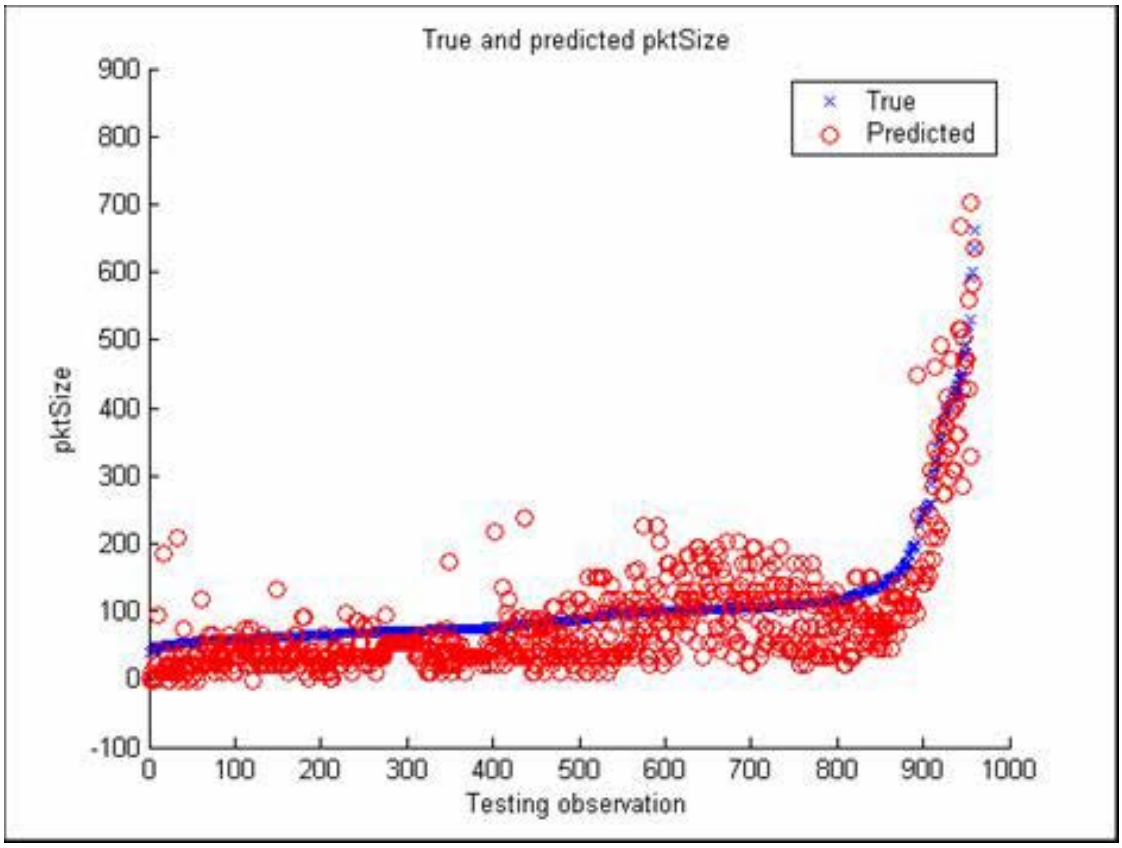

Figure 13. Prediction of Packet Size as a function of Throughput using Generalized Neural Networks linear regression

b. Functional Modeling Analysis

To further investigate the relationship between throughput and packet loss, I developed the scatter plot in Figure 14. An R-squared value of 86% provided even more tangible proof of the relationship between packet loss and throughput, especially given that it was substantiated by a different tool. Based on the previous findings, I constructed a mathematical model shown in Figure 15. It is a mathematical representation of the relationship between throughput and packet loss. The result was a logarithmic equation that showed throughput as a function of packet loss. An R-squared of 94%, provides confidence in this result. The ability to plug one criterion into an equation model and obtain another could become a very valuable tool in the future.

The next potential relationship that I investigated was the criteria of throughput with range as its parameter. I wanted to see if I could construct a mathematical modeling equation for a relationship that is generally accepted as fact.

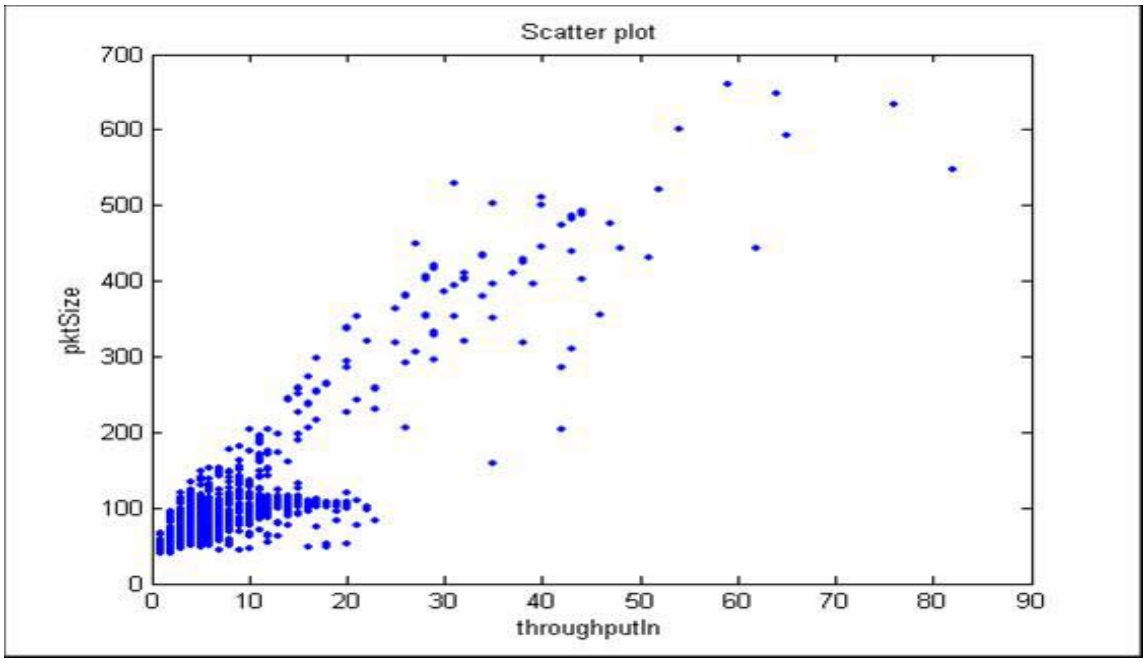

Figure 14. Comparison of Throughput and Packet Size

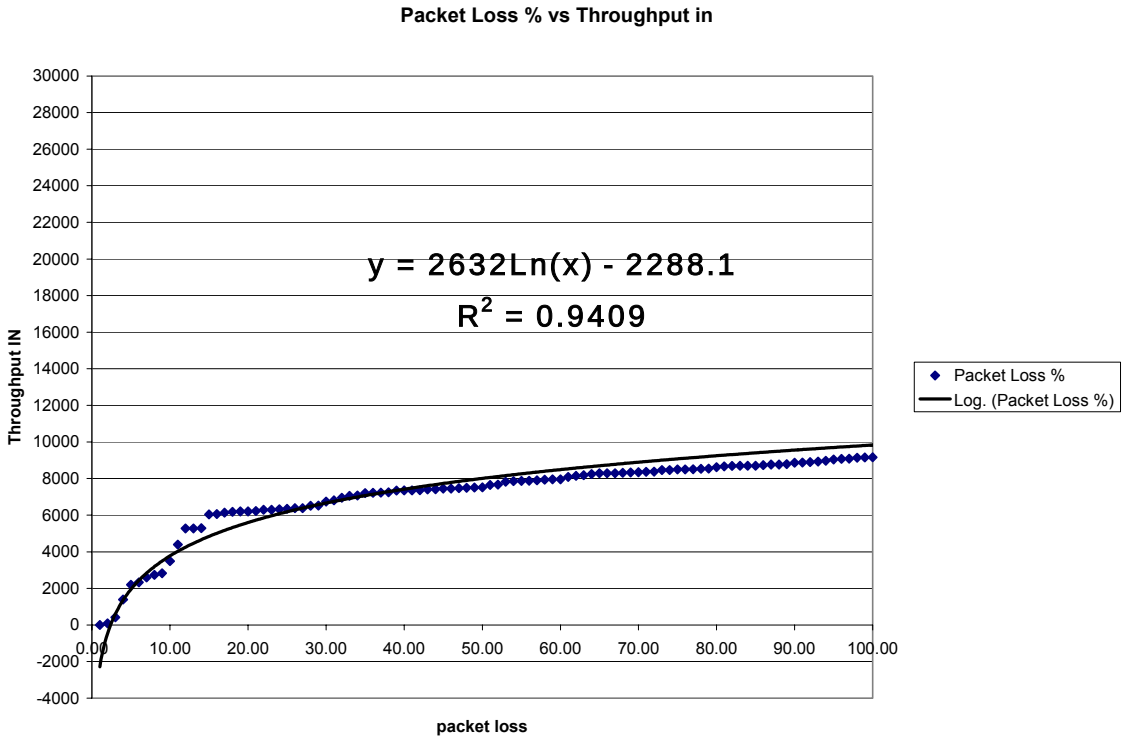

Figure 15. Graph of Throughput vs. Packet Loss Functional Model

Indeed, Figure 16 below shows an R-squared that indicates nearly 100% correlation between throughput and range. In this case, the ability to prove something that is already known is significant, because it validates my mathematical modeling process.

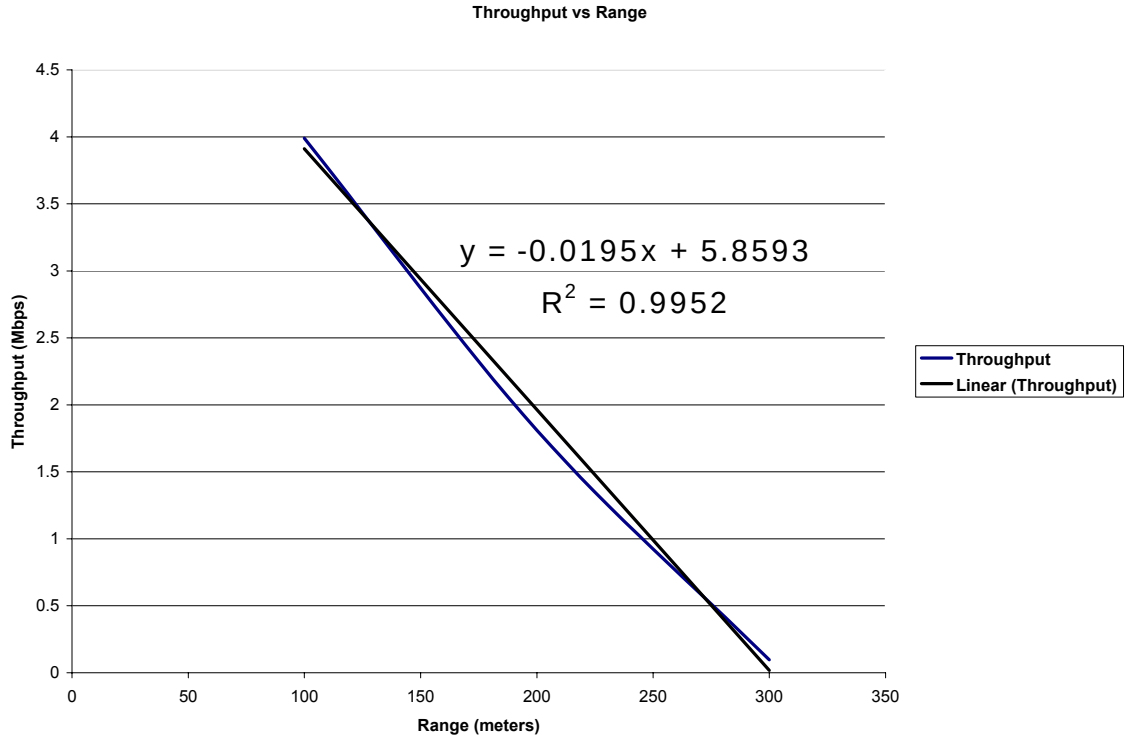

Figure 16. Graph of Throughput vs. Range Functional Model

As you can see below, I continued to use this now proven method to develop additional equations on MESH network performance criteria and parameters. Each seemed to have different relationships (i.e. exponential, linear, logarithmic), but they all had relatively smooth curves and high correlation. Figure 17 illustrates latency as a function of range and shows that, for that particular 802.11 MESH cluster, one can predict that latency will skyrocket when the range between the nodes approaches 200 meters. By performing a simple ping exercise to obtain latency figures, one can use the equation shown in Figure 18 to forecast the amount of throughput that will be available for use when the MESH network in deployed. Once again, this is critical information when planning to deploy tactical units in a potential battlefield.

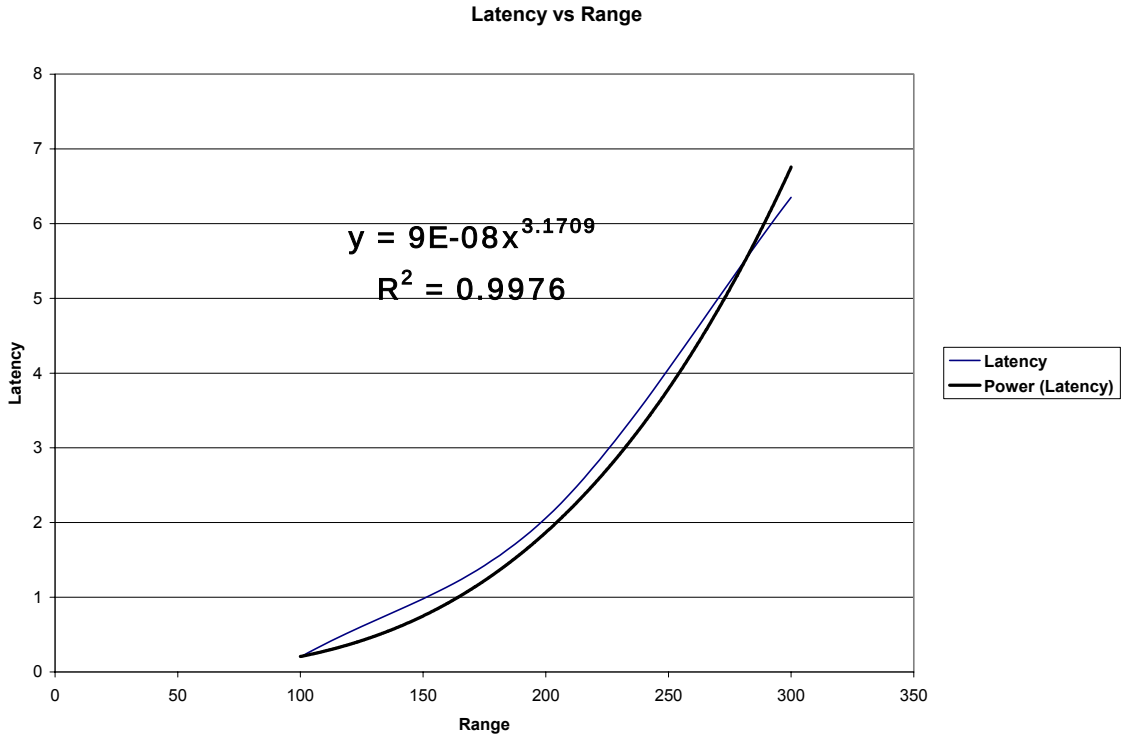

Figure 17. Graph of Throughput vs. Range Functional Model

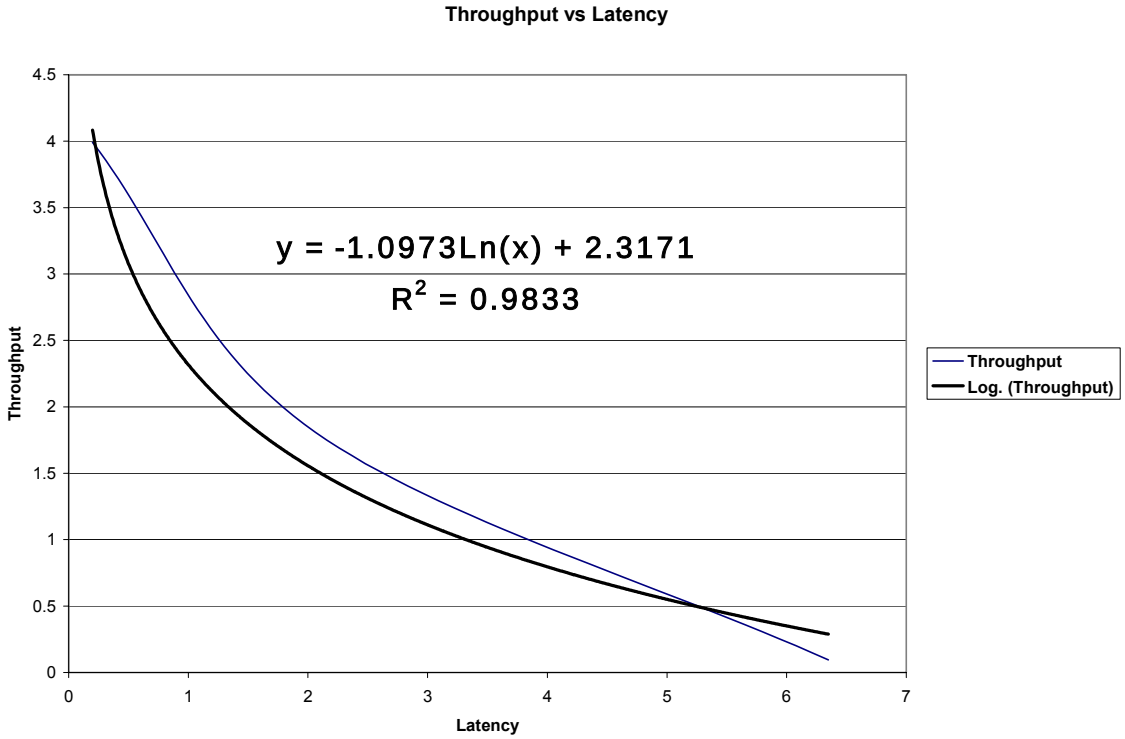

Figure 18. Graph of Throughput vs. Latency Functional Model

7. Conclusions

My experimentation results demonstrate the tremendous potential of having MESH network predictability tools at one's disposal for both planning and deployment purposes. One modeling application already in use in the TNT experiments is the OPNET modeling application. In the near future, mathematical predictability modeling equations could serve as an input to OPNET in an effort to produce better simulations of the genuine real world network behavior of the TNT. The major limitation of my TNT research was the fact that I did not have explicit control of all of the variables of the experiments. This should definitely be a focus area for upcoming MESH experiments in order to produce a really robust regression model.

V. CONCLUSION

A. CURRENT STATE OF TECHNOLOGY

In order to achieve the most effective military collaboration and self-synchronization, there has to be a dramatic increase in the ability to share tactical information between the tactical operating center (TOC) and the battlefield. In present tactical collaboration solutions, limited information is exchanged between armed forces in the battlefield. Verbal communications still remain the main source of data sharing. Extended-range transmissions are usually point-to-point, requiring high broadcast power, leaving communication vulnerable to it to enemy detection and single point of failure. Most tactical situations of today necessitate a collaborative solution that enable Combatant Commanders to maintain a current visual tactical picture at all times and the ability to constantly communicate their intent and update rules of engagement as the situation dictates. In current situational environments, every squadron or individual soldier is a sensor and has constant access to all sensory data in the tactical environment. As shown in Figure 19, each soldier continuously provides information about his tactical situation, resulting in superior collaboration between soldiers over an extended geographical range.

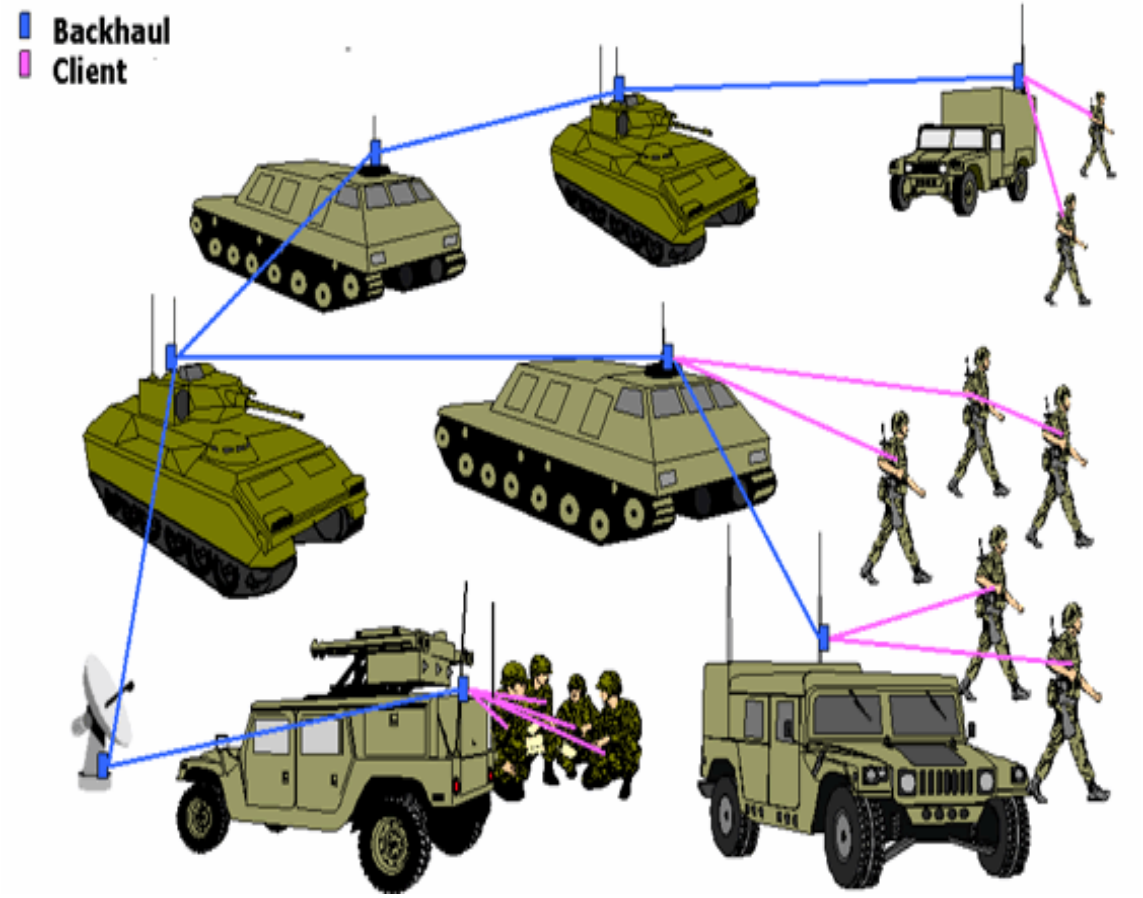

Figure 19. Soldiers as part of sensor clusters (From Structured MESH advantages)[25]

Wireless MESH networks provide the QoS required for the most efficient and effective sensor performance needed in today's tactical situations by providing the networking requirements necessary optimal operation of tactical sensors. Two such sensor requirements are adaptability and expandability (a.k.a. scalability). Because no global synchronization is required, a MESH can be assembled on the fly in any tactical situation. As nodes are added, the traffic routing options between nodes exponentially increase, resulting in a stronger MESH.[26] When nodes are added or removed, the network updates its routing tables and dynamically reconfigures its ever-changing virtual topology. The inherent mobility of a wireless MESH network satisfies one of the most

[25] MESHDynamics, "Why Structured MESH is Different." <http://www.MESHdynamics.com/WhyStructuredMESH.html>, Last accessed 15 February 2005.

[26] Lizhi, Charlie, Zhong, Jan, Rabaey, Chunlong, Guo, Rahul, Shah, "Data Link Layer Design for Wireless Sensor Networks," <http://bwrc.eecs.berkeley.edu/People/-Grad_Students/czhong/documents/milcom_2001_final.pdf#search='SENSOR%20NETWORKS%20IN%20MILLITARY%20APPLICATIONS'>, Last accessed 11 December 2005.

important tactical sensor requirements. The fact that data collection remains uninterrupted while wireless sensors are on the move is an invaluable tactical advantage of the MESH. One cannot overlook the reliability that a MESH provides due to its self-healing nature. The result is that there is no single point of failure in a true MESH because it simply reroutes the network traffic when communication with a neighboring node is lost. Although secure data transmissions of MESH networking have not been seriously addressed yet, the short data communication links reduces the possibility of being detected by the enemy, thus inherently providing some low scale security. Finally, the low power requirements of the MESH satisfy the tactical sensor requirement of power efficiency. Low power requirements of sensors are directly related to sensor size and the amount of bandwidth required from the MESH, affecting MESH QoS and sensor deployability. As computer processors develop and become more complex, further research and improvement is this area will be needed in order to maximize the benefits of the MESH sensor network.

A tactical networking solution that satisfies most or all of these sensor requirements will result in very robust system that can be implemented in any tactical environment and also vitally provide collaborative situation awareness needed by both, the Commanders and troops in the field today. Wireless MESH networks not only answer the mail, but are the best solution available at this time to expand dependable network centric warfare to the battlefield.

B. CONCLUSIONS

There are limitless opportunities for future MESH implementations. Wireless MESH networks offer added capacity to wired networks because of their natural ability to rapidly expand. While still in its infancy state, too much time is spent trying to determine why the MESH is not working. In order to guarantee an acceptable level of QoS, the MESH has to become more predictable in nature. The optimal performance of sensors within a tactical network requires a certain level of network performance, and that level of performance equates to premium QoS. In order to make network predictions, we have to be able to measure wireless MESH network performance, and know which variables affect that performance.

My research has shown that there are dependencies within MESH network performance criteria. Based on this relationship, I demonstrated the possibility of constructing mathematical models using network performance criteria, such as throughput, latency, and packet loss. As the maturity and stability of MESH technology increases, it will become easier to accumulate reliable data and perform network predictability analysis. The more dependable the MESH network, the better QoS that it can provide to its sensor clusters the resultant enhancement of its forecast ability.

C. RECOMMENDATIONS FOR FUTURE RESEARCH

In my opinion, future research should focus on three areas. First, continuing the development of predictability analysis because it is critical for the robust operation of MESH networks in the battlefield. Next, the development of predictability analysis will lead to higher and more stable QoS standards of MESH networks. Lastly, the development and implementation of secure MESH protocols are essential to the MESH ever being seriously considered for tactical deployment support for out troops.

SELECTED BIBLIOGRAPHY

Andreas Tonnesen, "Implementing and extending the Optimized Link State Routing Protocol," UniK University Graduate Center, University of Oslo, 1 August 2004.

Aspers, Patrik, "Crossing the Boundary of Economics and Sociology: The Case of Vilfredo Pareto," <http://www.findarticles.com/p/-articles/mi_m0254/is_2_60/-ai_75451916>, Last accessed 1 March 2005.

Chatterjee, S. and A. S. Hadi. Influential Observations, "High Leverage Points, and Outliers in Linear Regression." Statistical Science, 1986.

Conner, Steven and Gryder, Roxanne, Technology @ Intel Magazine "Building a Wireless World with MESH Networking Technology" <http://www.intel.com/update/contents/nc11032.htm> Last accessed 12 December 2004.

Cottrell, Les, Matthews, Warren and Logg, Connie, Stanford Linear Accelerator Center, "Tutorial on Internet Monitoring & PingER at SLAC," <http://www.slac.stanford.edu/comp/net/wan-mon/tutorial.html>, Last accessed 21 February 2005.

DACS, "A History of Software Measurement at Rome Laboratory," <http://www.dacs.dtic.mil/techs/history/His.RL.2.2.html>, Last accessed 12 January 2005.

"DTLR multi-criteria analysis manual," <http://www.odpm.gov.uk/stellent/-groups/odpm_about/documents/pdf/odpm_about_pdf_608524.pdf>, Last accessed 23 January 2005.

Gelsinger, Pat, Intel, "Catching up with Radio Free Intel," <http://www.intel.com/technology/comms/cn09031.htm> Last accessed 13 January 2005.

Innovative Wireless Technologies, "Sensors Networks, wireless sensor network development," <http://www.iwtwireless.com/SensorNetworks.htm>, Accessed 11 November 2004.

Ixia, "Performance Testing IxChariot," <http://www.ixiafederal.net/datasheets/pdfs/-pa_ixchariot.pdf> Last accessed on 21 February 2005.

Lizhi, Charlie, Zhong, Jan, Rabaey, Chunlong, Guo, Rahul, Shah, "Data Link Layer Design for Wireless Sensor Networks," <http://bwrc.eecs.berkeley.edu/People/-Grad_Students/czhong/documents/milcom_2001_final.pdf#search='SENSOR%20NETWORKS%20IN%20MILLITARY%20APPLICATIONS'>, Last accessed 11 December 2005.

Mattias Halvardsson and Patrik Lindberg, “Reliable Group Communication in a Military Mobile Ad hoc Network,” Master’s Thesis, Vaxjo University, February 2004, 15.

MESHDynamics, “Why Structured MESH is Different.” <http://www.MESHdynamics.com/WhyStructuredMESH.html>, Last accessed 15 February 2005.

Microsoft, “Quality of Service,” <http://www.microsoft.com/resources/documentation/-Windows/2000/server/reskit/enus/Default.asp?url=/resources/documentation/-windows/2000/server/reskit/en-us/cnet/cndc_qos_WQCI.asp> Last accessed 23 January 2005.

Mobile Computing Group, “QoS in Wireless MESH Networks,” <http://www.sce.carleton.ca/wmc/QoSZAP/>, Last accessed 22 October 2004.

OLSR Homepage, “Ad-hoc and OLSR,” <http://www.olsr.org/index.cgi?action=adhoc> Last accessed 1 March 2005.

Ronan Collobert, et al. “SVMTorch: Support Vector Machines for Large-Scale Regression Problems,” Journal of Machine Learning Research, 1(Feb): 2001.

Sanjiv Bhardwaj, Demand Solutions, “The Performance Metrics Three-Legged Stool,” <http://www.demandsolutions.com/pdf/ds_mag/fall_03/metrics.pdf>, Last accessed 22 November 2005.

SolarWinds, “Network Management & Discovery Software,” <http://www.solarwinds.net/>, Last accessed 21 February 2005.

Systems Analysis Laboratories, “Dynamic games, large scale systems and optimization,” <http://www.sal.hut.fi/Reasearch/index1.html>, Last accessed 1 March 2005.

Technologies, INC, “VIA and LocustWorld Secure Wireless MESH Networks with VIA PadLock High-Speed Encryption,” <http://www.via.com.tw/en/-resources/pressroom/2004_archive/pr040923lw_secureMESH.jsp> Last accessed 29 November 2004.

Van Dyck, Robert E. and Miller, Leonard E. Distributed Sensor Processing, “Over An Ad Hoc Wireless Network: Simulation Framework and Performance Criteria,” <http://w3.antd.nist.gov/pubs/milcom01.pdf> Last accessed 02 January 2005.

VIA Technologies, INC, “VIA and LocustWorld Secure Wireless MESH Networks with VIA PadLock High-Speed Encryption,” <http://www.via.com.tw/en/-resources/pressroom/2004_archive/pr040923lw_secureMESH.jsp> Last accessed 29 November 2004.

Wasserman, P. D., “Advanced Methods in Neural Computing,” New York: Van Nostrand Reinhold, 1993.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, California

4. Douglas E. Brinkley
   Naval Postgraduate School
   Monterey, California

5. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Joseph A. Davis
   Naval Postgraduate School
   Monterey, California