NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NETWORK MANAGEMENT SYSTEM FOR TACTICAL MOBILE AD HOC NETWORK SEGMENTS

by

Chad J. Puff

September 2011

Thesis Advisor:	Alex Bordetsky
Second Reader:	John Looney

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** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Network Management System for Tactical Mobile Ad Hoc Network Segments		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Chad J. Puff			
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. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Mobile Ad Hoc Networking (MANET) technologies are highly desirable in tactical environments because they are able to communicate with neighboring devices over one or more hops in order to extend connectivity to areas where a fixed infrastructure is not available or is not possible. There are many factors which can influence the performance and reliability of a MANET. Communications links within the MANET are continuously fluctuating due to device location, power, or environmental factors. Devices within the MANET can enter the network and then disappear due to the devices losing connectivity because of their physical location relative to other nodes within the network. A network management system (NMS) that can provide for MANET administration in both simulation-based and real-time operational environments provides additional value for this network. The objectives for this network management system is to allow users to predict, monitor, and control network behavior; this specifically includes viewing and remotely managing variables such as node status, node location, attached equipment, channel selection, frequencies, error rates, and network utilization.

14. SUBJECT TERMS Network Management System, Tactical Mobile Adhoc Networks, Simple Network Management Protocol			**15. NUMBER OF PAGES** 101
			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** UU

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

NETWORK MANAGEMENT SYSTEM FOR TACTICAL MOBILE AD HOC NETWORK SEGMENTS

Chad J. Puff
Captain, United States Marine Corps
B.A., Washburn University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Author: Chad J. Puff

Approved by: Alex Bordetsky
Thesis Advisor

John Looney
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Mobile Ad Hoc Networking (MANET) technologies are highly desirable in tactical environments because they are able to communicate with neighboring devices over one or more hops in order to extend connectivity to areas where a fixed infrastructure is not available or is not possible. There are many factors that influence the performance and reliability of a MANET: Communications links within the MANET are continuously fluctuating due to device location, power, or environmental factors. Devices within the MANET can enter the network and then disappear due to the devices losing connectivity because of their physical location relative to other nodes within the network. A network management system (NMS) that provides for MANET administration in both simulation-based and real-time operational environments provides additional value for this network. The objectives for this network management system are to allow users to predict, monitor, and control network behavior; this specifically includes viewing and remotely managing variables such as node status, node location, attached equipment, channel selection, frequencies, error rates, and network channel utilization.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AN/PRC	Army/Navy Portable Radio Communication
ANMP	Adhoc Network Management Protocol
C2	Command and Control
CBR	Case-Based Reasoning
CENETIX	Center for Network Innovation and Experimentation
CIRPAS	Center for Interdisciplinary Remotely Piloted Aircraft Studies
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
COC	Combat Operations Center
COI	Conditions of Interest
CONOPS	Concept of Operations
COP	Common Operational Picture
COT	Cursor on Target
CP	Command Post
DoD	Department of Defense
ECO	Enhanced Company Operations
FOB	Forward Operating Base
HPA	High Powered Amplifier
HQMC C4	Headquarter, Marine Corps Command, Control, Communications, and Computers
HTTP	Hypertext Transfer Protocol
I MEF	First Marine Expeditionary Force
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standards Organization
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology

JSON	Java Script Object Notation
Kbps	Kilobits per Second
KML	Keyhole Markup Language
LAN/MAN	Local Area Network Manager
LOS	Line of Sight
MAGTF	Marine Air Ground Task Force
MANET	Mobile Adhoc Network
Mbps	Megabits per Second
MCWL	Marine Corps Warfighting Laboratory
MIB	Management Information Base
MOE	Measures of Effectiveness
MOP	Measures of Performance
MRAP	Mine Resistant Ambush Protected
MUOS	Mobile User Objective System
NCW	Network Centric Warfare
NGC2	Next Generation Command and Control
NLOS	Non-Line of Sight
NMS	Network Management System
NMS-TM	Network Management System Tactical MANET
NOC	Network Operations Center
OID	Object Identifier
OODA	Observe Orient Decide Act
OP	Observation Post
OSI	Open Systems Interconnection
OTAR	Over the Air Rekey
OTAZ	Over the Air Zeroize
PC	Personal Computer
PLI	Position Location Information
QoS	Quality of Service
RF	Radio Frequency

RFC	Request for Comments
RIMPAC	Rim of the Pacific
RMON	Remote Monitor
SA	Situational Awareness
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
STOM	Ship to Objective Maneuver
TCP	Transmission Control Protocol
TMN	Telephone Management Network
TNT	Tactical Network Topology
UDP	User Datagram Protocol
UFO	UHF Follow-On
UHF	Ultra High Frequency
USB	Universal Serial Bus
VHF	Very High Frequency
VIRT	Valuable Information at the Right Time
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
YAP	Yelp Announcement Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Alex Bordetsky, Mr. Eugene Bourakov, CDR John Looney, and LtCol (retired) Carl Oros. Each of these men has provided me with invaluable insight and guidance throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> A decade into the war in Afghanistan, Army officials continue to grapple with a baffling incongruity: U.S. soldiers have the most sophisticated weaponry and equipment in the world, and yet the enemy can outwit them simply because they have a better means to receive and disseminate information. (Erwin, 2011)

A. NETWORK-CENTRIC WARFARE

The advances of information technology have led to fundamental changes in both society and business. Among these changes has been the shift from platform-based applications to network-based applications that allow information exchanges to occur among a large number of interconnected nodes. The military has gained some insight from these network-based applications and has attempted to apply networking technology to tactical operations in order to achieve Network Centric Warfare (NCW) (Alberts, Garstka, & Stein, 2000). At the core of NCW is the concept that there is value in an organization's ability to share relevant, accurate, and timely information between nodes on its network. Historically, the military has led society in proliferating communications technologies throughout its organizations and enhancing information exchange capabilities, but this may no longer be the case—hence our enemies may have an important advantage that the military needs to mitigate.

1. The Marine Corps Vision for NCW

Part of the Marine Corps' strategic vision is to achieve the capability of network-centric operations by 2025 (United States Marine Corps, 2010). Current operational capabilities fall short of achieving this largely due to the lack of an integrated data network at the company level and below. Network centric operations is supposed to support decision making at all levels (e.g., tactical through strategic) by enabling geographically dispersed military forces to access and share information in near real-time. Implementing an integrated network throughout the tactical level allows small-unit leaders to access and manage information flows necessary to enhance force-wide

situational awareness—a concept that theoretically leads to improved decision making and rapidity of action (Cebrowski & Garstka, 1998).

At the beginning of Operation Iraqi Freedom, VHF and UHF line of sight voice communications were the mainstay of the Marine Corps' communications architecture at the battalion level and below. This resulted in unreliable communications that adversely affected the actions of a Marine Corps battalion during the battle for An Nasiriyah from 20–23 March 2003. Major Rohr described the difficulties of command and control in a chaotic battlefield environment: disrupted communications contributed to incomplete situational awareness that caused tactical friction during this battle because critical information was not able to reliably flow (Rohr, 2006).

The timely flow of information is heavily dependent on a reliable and integrated network. Since the beginning of Operation Iraqi Freedom, the Marine Corps has made substantial investments to deploy communications assets (e.g., wireless mesh networking devices) and information gathering assets (e.g., sensor networks) at the small unit level (Tsirlis, 2008). Despite these efforts, it remains difficult for small-unit leaders to access necessary information, such as intelligence and situational awareness data, due to the many challenges of employing traditional line of sight communications under harsh battlefield conditions.

2. Infrastructure Requirements for NCW

The concept of NCW requires enterprise network applications and wireless infrastructure for the tactical level architecture to become a reality. Enterprise architecture is the "fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution" (Minoli, 2008). This definition of enterprise architecture indicates that the system design must consider the applications, content, and infrastructure that are supporting the flow of information. In order for a network to be capable of being an enterprise system, heterogeneous components must be able to interconnect. This is not the case with existing communications and sensor networks procured as standalone systems (Erwin, 2011).

a. Grid Computing

Many businesses have shifted their information technology (IT) systems from platform-based standalone systems to a more integrated system designed to allow for the aggregation of geographically distributed computing resources. *Grid computing* is based on the power distribution system that provides consumers with electricity and requires a highly interconnected network infrastructure. The advantage gained from grid computing is that systems can work together so that the total effect is greater than the sum of the individual components (Minoli, 2008). It seems reasonable that the military could achieve similar advantages from deploying a grid-like network infrastructure at the tactical level instead of the status quo of multiple standalone systems. This network must be so reliable so that its availability is as good as other infrastructures such as the electrical grid.

b. Mobile Networks

A second consideration of the more recent changes occurring within the IT field is that it is now common for enterprise networks to include applications that support mobile smart phone devices. The growing popularity of smart phone devices is largely due to consumers finding value in these networks because content, reliability, and connectivity are included in a single mobile device. Modern cellular handsets are at the center of a wave of innovations in the commercial industry that provide consumers with continuous access to information and business intelligence (Traylor, 2009). An example of a military application of this technology is the communications between a patrol leader and the tactical operations center when identifying a suspect as a known person of interest. In the past, this could take several minutes for the patrol leader to describe the individual using voice communications, whereas transmitting a digital photograph could take a matter of seconds (Dixon, 2010). Would it be possible for the military to employ a mobile, wireless broadband network at the tactical level? Would this generate similar value for the warrior as it clearly does for people in society today? How can this tactical network infrastructure be managed in order maximize the value and create opportunities for small-unit leaders to access and share information? Finally, can a network

management system ensure the availability of the network, so that it becomes as reliable as other infrastructures to which consumers are accustomed?

B. VALUE OF INFORMATION

Further study of those questions requires an operational definition of value. Business operations generally think of value as the ability to generate profits. Modern organizations seek to improve their ability to adapt to changing environmental circumstances by using IT systems to make better decisions more rapidly. This enhanced information processing capability allows these organizations to achieve better results and obtain a competitive advantage. The goal of applying IT systems to military operations should be the same as commercial organizations, i.e., maximize the ratio of value added to cost (Hayes-Roth, 2005).

1. Information Value

A measure of the value added to military operations could be how the information contributes to mission accomplishment. Air Force pilot John Boyd is famous for introducing the cycle of information processing and decision making referred to as the Observe-Orient-Decide-Act (OODA) loop (Coram, 2002). Organizations that operate this loop faster than their competitors have an advantage. Superior information processing contributes to "having an accurate understanding of what is happening around you and what is likely to happen in the near future" (Situational Awareness, 2011). Situational awareness leads to a competitive advantage because it allows one side the opportunity to control the operational tempo. In this context, the value of the information is not simply the result of the raw data collected, but the ability to process this data and transmit only the relevant and timely information to the correct nodes that need this information to achieve situational awareness. With this advantage, those nodes (e.g., tactical commanders) are able to plan and be proactive instead of just responding to the things that are happening around them.

2. Network Value

Networks can create value by allowing the rapid sharing of information. Ideas applied from the field of economics help to better understand the value created by a network. Networks are composed of links that connect nodes, and the structure of a network requires many components to provision enterprise services. These components must be interoperable to create a network infrastructure. The value of the network infrastructure derives from its ability to efficiently produce interconnectedness and its ability to support the consumption of information (Economides, 1996).

In other words, the value of a network derives from connectivity or from content. There is some debate over which of these factors is most significant. In certain types of networks, connectivity is the dominating factor that leads to increasing the network's value. An example of this is e-mail: e-mail has value because it provides access to people instead of access to information. On the other hand, broadcast networks such as cable television or mass media have value based more on content rather than connectivity (Odlyzko, 2001).

a. Models of Network Value

There are at least four ways to model the value of a network depending on the type of network that is being evaluated (Table 1).

Model	**Equation**	**Use**
Sarnoff's Law	$V = N$	Simple broadcast networks
Metcalfe's Law	$V = N^2 - N$	Networks where all connections are of equal value
Reed's Law	$V = 2^N - N - 1$	Used to show that group forming networks create value much more rapidly than shown by Metcalfe's Law
Zipf's Law	$V = N \log(N)$	Shows that most valuable connections are made first

Table 1. Four models of network value (After Briscoe, Odlyzko, & Tilly, 2006)

Sarnoff's Law states that the value of a network is directly proportional to the number of nodes on the network. According to Sarnoff's Law, the value of a

broadcast network is a linear function in which the value (V) is proportional to the total number of nodes (N) on the network. The second model, known as Metcalfe's Law, states that the value of a network increases with the square of the number of nodes that it connects. Because Metcalf's Law assumes that all potential links in a network are equal; it may result in an over estimate of network's value if all nodes are not equal. Zipf's Law estimates the value of networks where all connections are not of equal value and it accepts that the first connections made were the most valuable. A final model, known as Reed's Law, accounts for certain networks being able to form groups that share content specific to the group (Briscoe, Odlyzko, & Tilly, 2006). Figure 1 shows a graphical representation of how the network value increases as node density increases in each of these four cases.

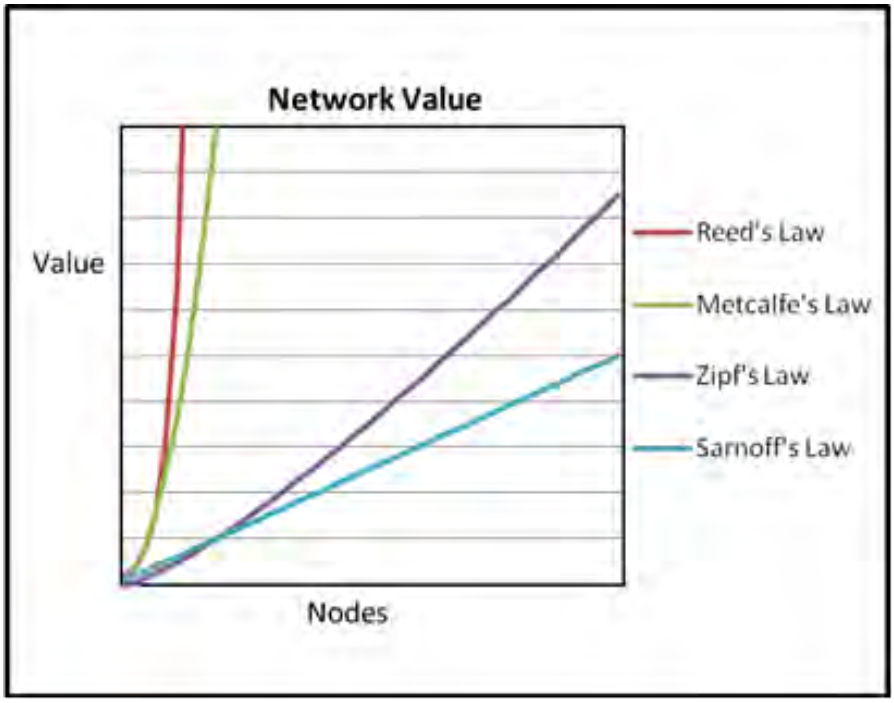


Figure 1 Graphical representation of network value models (After Briscoe, Odlyzko, & Tilly, 2006)

Content also determines how each of the four models can illustrate the value of the network. The first types of networks used in support of tactical military operations were broadcast networks based upon netted voice communications over single

channel radios. Sarnoff's Law could measure the value of these early tactical networks. As data networks became more common at the tactical levels, the value resulted from the network's ability to provide connectivity to applications such as tactical chat or to transmit imagery of the battlefield to a limited number of users. Any member of the unit could collect and transmit valuable information and contribute to an overall situational awareness. Here Metcalfe's Law seems to apply; however, further analysis reveals that the accessibility does not ensure timely processing of the most important information. The fact that most of the value will come from the most critical nodes reveals that Zipf's Law is a more accurate representation of the network's value. According to Zipf's Law these critical nodes account for approximately two-thirds of the network's total value. The remaining one-third of the network's value is derived from the remaining nodes (Briscoe, Odlyzko, & Tilly, 2006).

Although deployed units have numerous sensors and network equipment at their disposal, these systems exist as "point-to-point" links, which limits their usefulness. According to senior Army officials, soldiers at the tactical level often complain about living off of the information grid (Erwin, 2011). This indicates that soldiers at the tactical level desire a network that can connect anyone to the information grid. Allowing these soldiers to form groups makes Reed's Law apropos and there is additional value added to tactical networks (Reed, 1999).

Adhering to lessons learned from society shows the value of networks is greater when the network supports the ability to form groups and transmit group specific information. The rapid increase in value observed with social network applications such as Facebook™ or MySpace™ is such an illustration. These applications have changed the way networks are valued because now both connectivity and content are equal factors. Each node in *group forming networks* is able to select other nodes that it communicates with and subscribe to specific content. The result is that the network's value increases exponentially as node density is increased, which is described by Reed's Law.

b. Using a Network Management System to Create Added Value

The management system that is used to support the tactical network must be able to create and maintain a grid-like infrastructure that is capable of allowing a similar convergence of content and connectivity as is available in commercial smart phone networks. The development of such an infrastructure maximizes the value of this network. This infrastructure likely includes interconnected and heterogeneous links such as commercial and military satellites, 802.16 WiMAX,[1] 802.11 WLAN,[2] mobile ad hoc networking, and ultra wideband devices. This requires a network management system capable of maintaining this infrastructure under the most difficult and extreme conditions that tactical units encounter.

Tactical units are required to operate with a great amount of geographic dispersion in harsh conditions, both environmental and enemy induced, where access to fixed infrastructure is not available. These units must be able to rapidly deploy the required infrastructure capable of supporting beyond line of sight communications in order to interconnect the operations center, the small-unit leaders, and the associated sensor equipment deployed within the area of operations (Kutsor, 2010). Providing a fully integrated network to the edges at the tactical level likely requires coupling ultra wideband networking devices with the information gathering sensor equipment, and then interconnecting these sensor nodes to a mobile ad hoc network backbone. That network is capable of overcoming the challenges faced under those extreme environmental conditions by creating a self-healing, self-forming infrastructure that is able to penetrate thick foliage or the dense materials of modern urban structures.

Ultimately, the value of this sensor grid network depends on the total number of devices that can be interconnected in order to provide small-unit leaders with high bandwidth connectivity so that they can share information and gain timely situational awareness relevant to their area of operations. Providing broadband access on

[1] Worldwide Interoperability for Microwave Access (WiMAX) is a telecommunications protocol that provides fixed and mobile wireless broadband network access.

[2] Wireless Local Area Networking (WLAN) is a communications standard for connecting electronic devices through an access point.

the battlefield and smartphones updated with new mobile applications has become a top priority for senior Army and Marine Corps officials (Erwin, 2010). The ability to maintain these types of tactical networks with high node density under harsh conditions will require a robust network management system that is able to minimize service disruptions within the sensor grid network. The ultimate goal of the network management system is to maximize the network's value even under the most extreme conditions.

C. SUMMARY

The goal of this thesis is to describe the value of the tactical Mobile Adhoc Network (MANET) and how a network management system will enhance this value. The next two chapters of this thesis provide an overview of the basic concepts of the network management protocols and standards that apply, and describe the quality attribute characteristics of the tactical MANET. The final three chapters describe field research conducted and recommendations regarding the appropriate variables to incorporate into the network management system. The final chapter provides additional incremental improvements available to the tactical MANET network management system in order to move closer toward the ultimate end state of a tactical network consisting of autonomous self-managing nodes.

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORK MANAGEMENT

This chapter provides a detailed explanation of how the vision of network-centric warfare leads to a superior information position resulting in a competitive advantage and dominance over our adversaries. The foundation of the network-centric enterprise is the information infrastructure that allows information sharing among geographically dispersed forces. This network-centric enterprise requires an entirely new communications protocol that researchers at the Naval Postgraduate School have described as being the *8th layer* of the OSI Model.[3] This chapter describes all of the building blocks of the 8th layer protocol. One of the most fundamental architectural elements of the 8th layer is the *hypernode* or autonomous network element that is capable of adapting its behavior and performance based on changing environmental conditions. Other fundamental architectural elements of the network-centric enterprise are monitors and agents that provide *just in time* delivery of valuable information. Later chapters of this thesis describe the application of these concepts to the tactical MANET to add value to the information processing supply chain.

A. INFORMATION AGE ORGANIZATIONS

The information age has introduced many changes in the way that organizations must behave in order to survive (Alberts, Garstka, & Stein, 2000). Among these changes are:

1. Changing how wealth is created
2. Altering the distribution of power
3. Increasing the complexity of the world
4. Shrinking distances around the world
5. Compressing time, which alters the tempo of our lives

[3] The Open Systems Interconnections (OSI) Model developed by the International Organization for Standardization is a way to logically separate communications between two end devices into seven layers. The concept of an 8th layer indicates a higher level than is currently included in the OSI model.

These changes are significant to the military because these factors affect the threats that we face and how we respond to potential adversaries. The most successful information age organizations are able to prevail over their competition primarily through an advantage gained by their ability to collect, process, and disseminate information rapidly in order to make better decisions (Hayes-Roth, 2006).

Three phenomena of the information age are (Alberts, Garstka, & Stein, 2000):

1. The volume of information has increased exponentially
2. The time required to access the information has been reduced by orders of magnitude
3. Geographic dispersion within the organization is increasing

These factors require information age organizations to re-evaluate how information is processed. Traditionally, military command and control protocols have given priority to, and in many cases restricted to only, vertical information flows necessary to ensure the success of the hierarchical organization. Lessons learned from other information age organizations shows that may be a losing strategy (Alberts, Garstka, & Stein, 2000). The information age has led to environmental conditions changing more rapidly and organizations that succeed under these conditions must change how they approach command and control. The goal of an information age organization is to achieve synchronized, coordinated, and intelligent actions at a faster rate than the environment changes. A shared world model that includes relevant facts and beliefs about the environment allows the realization of this goal. Although the common operational picture (COP), which portrays the battle space and its actors, is an initial step towards developing that shared world model, it is a good start because it allows tactical forces to see and share the same representation of the battlespace. The COP serves the purpose of creating shared situational awareness by reducing environmental uncertainty and the number of bits transmitted (Hayes-Roth, 2006).

The Marine Corps recognized these factors through its own lessons learned in both Iraq and Afghanistan. Those lessons show that the Marine Corps must employ company sized ground combat elements that are capable of sustained independent

operations. This concept, known as Enhanced Company Operations (ECO), requires these company-sized elements to access a COP that is based on near real-time voice, data, and surveillance information (Conway, 2008).

1. Value Creation

Similar to the way that any manufacturing process is able to create value by converting raw materials into a useful product desired by consumers, information processing can also create value by delivering products that are useful to the information consumers. Manufacturers have recognized for some time that processes such as just in time delivery adds value to the products because these processes are able to ensure delivery of the right materials exactly when needed. This reduces inventory and work in process costs. On the other hand, delivering materials at inappropriate times actually creates negative value through increased costs. Until now, the Department of Defense (DoD) focused on making information more accessible and understandable; however, this resulted in little value simply because the amount of information available to the people who need it is overwhelming (Hayes-Roth, 2006).

2. Information Dominance

Superior information processing creates a competitive advantage by an order of magnitude that allows the network-enabled organization to dominate its competitors (Alberts, Garstka, & Stein, 2000). The ability to share accurate, timely and relevant information throughout a distributed organization is a critical capability towards achieving superior information processing. The ability to collect, process, and disseminate an uninterrupted flow of relevant, accurate, and timely information while exploiting and/or denying an adversary's ability to do the same leads to information dominance. Superior information processing leads to:

1. Shared awareness
2. Increased coordination of geographically dispersed forces
3. Higher tempo of operations

The true value of superior information processing is in the military outcomes that it enables, providing the ability to increase the tempo of operations and prohibit/limit the

enemy's initiatives and options. Improving our information processing at the lower levels is a critical enabler of kinetic actions, such as directing fires or air support assets onto identified targets as well as non-kinetic actions such as directing how civil and public affairs assets are best employed. In both cases a superior information position will increase the effectiveness of our forces throughout the full spectrum of warfare.

3. Network-Centric Enterprise

A network-centric enterprise is required in order to support today's organization in realizing its vision of information dominance. The network-centric enterprise recognizes that Information Technology is a significant contributor to the vision; however, it also enables knowledge sharing, which transcends IT and touches all other forms of communication between parties. The elements of the network-centric enterprise are shown in Figure 2 to illustrate how this allows knowledge to be shared quickly and efficiently between all participants, and most especially between those who are directly involved in the task/mission at hand. The sharing of this knowledge would not be limited to a stove-piped and hierarchical reporting process typical to the traditional command structure. Rather, this knowledge sharing capability allows all participants to share knowledge among those who need to know, regardless of their position in the organizational structure. This allows network-centric forces to adapt more quickly and accurately to changing battlefield conditions. This thesis focuses on improving the first two pieces of the network-centric enterprise, the "infostructure" and "sensor netting," which in turn will add value to the enterprise.

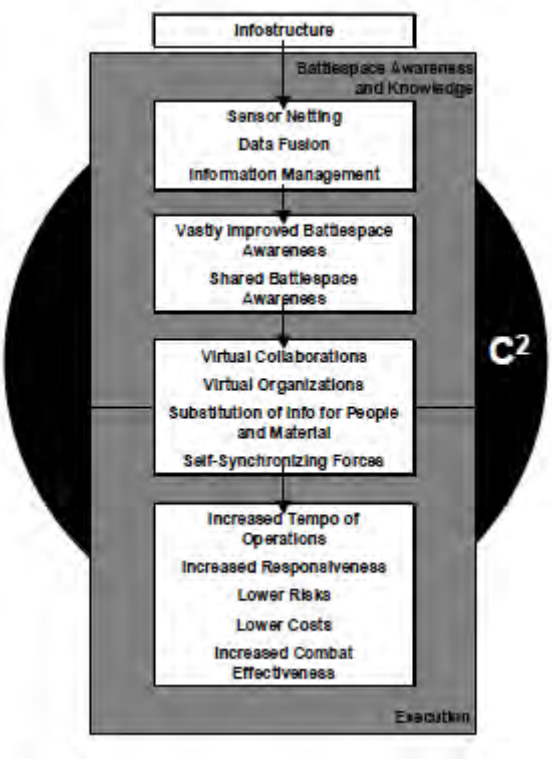


Figure 2 The net-centric enterprise (From Alberts, Garstka, & Stein, 2000)

The network-centric enterprise will consist of many command and control (C2) systems that must be able to work together. The right architecture design, made up of the *framework* as well as the *components* of the C2 systems will achieve this end state. Components are proven, reliable, and reusable elements that interrelate or interact with another. *Framework* is the structure between components that facilitates the coupling of one component to another. The end result is that the architecture provides the ability to couple components in multiple configurations within the structure of a framework in order to achieve interoperability and coherence among the C2 systems. Other value adding benefits include the reuse of known, workable solutions that lead to greater standardization and cost savings.

B. NETWORK-CENTRIC ARCHITECTURE

1. The 8th Layer Protocol

The Open Systems Interconnect (OSI) Reference Model uses 7 layers to show how communications between two systems moves through a hierarchy from the lowest level that transmits bits over a physical medium to the highest level, which allows an end user to interact with a software application. In the past, many have recognized that there are other elements not depicted by the OSI 7 layer model, including the human and business factors (Bordetsky & Hayes-Roth, 2006). The 8th layer concept, developed at the Naval Postgraduate School, extends the OSI Reference Model by adding an additional layer in order to implement the self-forming and self-controlling functionalities in tactical C4I networks also known as *adaptive networking*. According to this previous research, the 8th layer requires the creation of a new communications protocol and architecture that allows every critical node in a network to have its own specialized Network Operations Center (NOC) capability. These critical nodes, known as *hypernodes*, are the building blocks of these adaptive networks. These hypernodes are capable of managing multiple competing constraints to maximize the network's overall performance (Bordetsky & Hayes-Roth, 2006).

The 8th layer's network management hierarchy of services (Figure 3) provides individual nodes with the capabilities of self-diagnosis (Network Element Layer), sub-network view (Network Element Management Layer), end-to-end performance (Network Management Layer), Quality of Service requirements (Service Management Layer), and Service Level Agreement (SLA) negotiation (Business Management Layer). The 8th layer approach also uses a simple network management protocol (SNMP) events monitor with management information base (MIB) extensions in order to incorporate service layer and business layer elements (Bordetsky & Hayes-Roth, 2006). Later sections in this chapter provide a more detailed explanation of SNMP and the MIB.

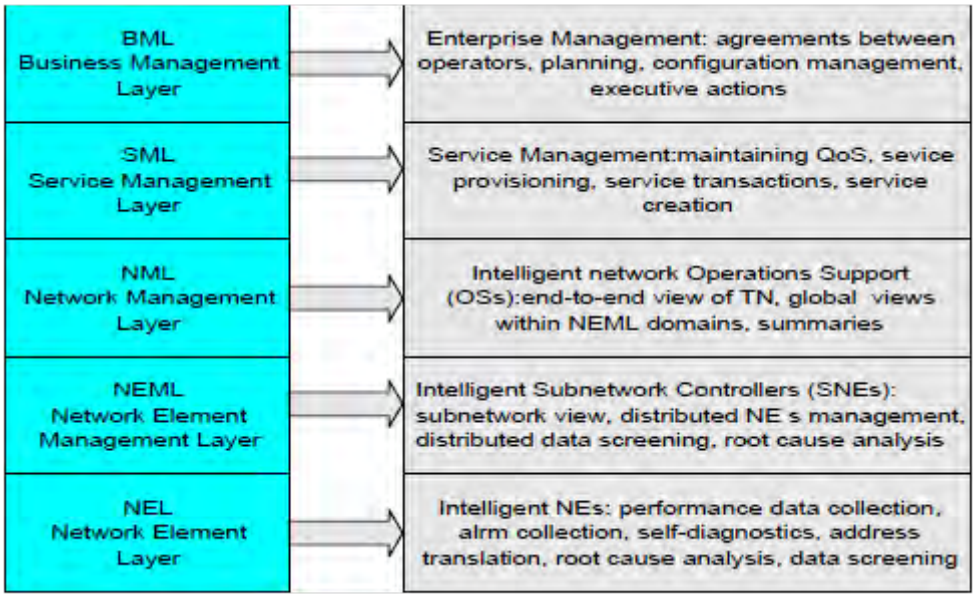


Figure 3 The 8th layer elements (From Bordetsky & Hayes-Roth, 2006)

2. Hypernodes

Hypernodes are the most fundamental building block of the network-centric architecture. The basic NOC processes incorporated into the hypernodes are the ability to collect, integrate, and display data measurements taken from the network. The process model for the NOC is a Sense-Analyze-Adapt feedback loop based upon a command and control structure (Figure 4). At the top levels, this NOC process model must identify the mission or strategic level objectives. Service level agreement (SLA) constraints and performance metrics allow managers to measure the performance against the strategic objectives. This determines the specific variables to reconfigure in order to adapt the network configuration towards a more optimal solution in accordance with the SLA constraints (Bordetsky, Dolk, & Zolla, 2004).

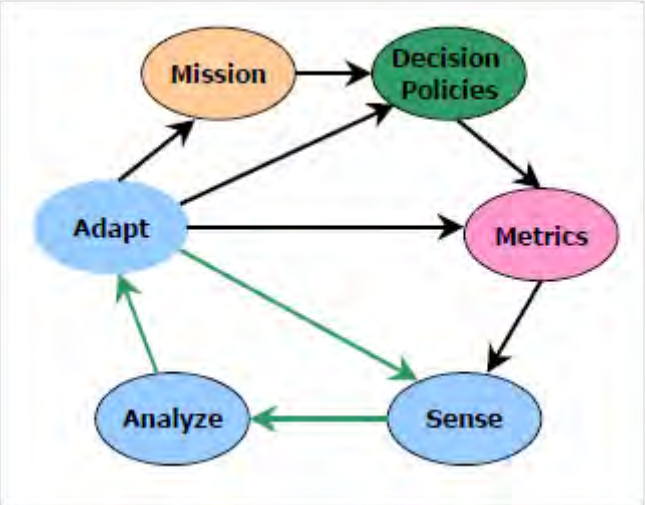


Figure 4 NOC process model (From Bordetsky, Dolk, & Zolla, 2004)

The ability of the hypernodes to perform network optimization based on multiple, competing constraints requires the incorporation of a *solver application* into the network management system. The objective of this solver application is to allow the individual NOCs to optimize their local networks and allow the overall network management system to develop a pattern for network behavior. The solver algorithm must attempt to optimize the overall network without negatively impacting any of the individual NOCs. The goals sought by this solver application must not be limited to simple network performance measures, but must recognize the importance of delivering high value information at the right time (Bordetsky & Hayes-Roth, 2006).

The final element of the hypernode incorporates a situational awareness monitor based on the Cursor-on-Target schema (CoT). The CoT schema provides the what, when, where and details to the situational awareness application flow (Curser on Target, 2004) The CoT schema is optimized for sending small packets of data very frequently and provides real-time postion location information (PLI) for all managed nodes in the tactical network. The PLI information can be displayed using any mapping applications such as FalconView™ or GoogleEarth™. Physical node locations provide data such as terrain and elevation that could also be used to support network element conrol variables.

3. Valuable Information at the Right Time (VIRT)

Network centric warfare relies upon individuals being able to receive valuable information at the right time (VIRT). However, the current state of the DoD information enterprise buries any valuable information underneath megabytes of useless information (Hayes-Roth, 2006). The delivery of VIRT is dependent on a *models-based network* that allows consumers of information to define their information requirements through specified conditions of interest (COIs); that transforms networks into integrated value chains. The framework of the *model-based network* is a Publish-Subscribe architecture where recipients identify the information that they are interested in so that the *models-based-network* is able to route matching information from the suppliers accordingly. Ideally, this network will distribute a *shared world model* to each participant, and employ processes based on conditions monitors to keep each local cache in sync. These COIs must be incorporated into the network management system SLAs in order to ensure just-in-time delivery of valuable information (Hayes-Roth, 2005).

C. NETWORK MANAGEMENT STANDARDS

There are several network management standards that are in use today; among these are the Open Standard Interconnection (OSI) management, the Internet Engineering Task Force (IETF) standard, the Telecommunication Management Network (TMN) architecture, the Institute of Electronics and Electrical Engineers (IEEE) LAN/MAN standards, and web-based network management. The International Standards Organization (ISO) has adopted the OSI standard. The OSI management protocol standard is the Common Management Information Protocol (CMIP) and has built in services, Common Management Information Services (CMIS) that specify the basic services needed to perform various functions. The OSI management standard is the most comprehensive set of specifications and it addresses all seven layers of the OSI Reference Model. Two major drawbacks to the OSI management model are that it is rather complex and the CMIP stack is too large for mobile network applications. The TMN architecture is oriented towards the needs of telecommunications service providers, therefore, it addresses service level and business level considerations. The IEEE LAN/MAN

standards only address the physical and data link layers of the OSI Reference Model. Finally, web-based management systems appear to be well suited for mobile applications because these systems are able to support a more distributed architecture by using a web server for the management system and web browsers for network management stations (Subramanian, 2006).

1. SNMP

In contrast to CMIP, Simple Network Management Protocol (SNMP) is a less complicated protocol. The IETF has identified SNMP as the industry standard for managing Internet components and as a result SNMP is now the most widely implemented network management system (NMS) in use today. There are numerous Requests for Comments (RFCs) published by the IETF to define the SNMP standards (IETF, 1990). The most notable RFCs include RFC 1213 (defines the basic SNMP MIB), RFC 2578 (introduces SNMP version 2), and RFC 3414 (introduces SNMP version 3). Most networking devices that use TCP/IP support SNMP.

SNMP utilizes a manager/agent model consisting of a database of managed objects and the network protocol used for communications (DenHartog, 2010). The SNMP manager provides the interface between the human network manager and the management system. The SNMP agent itself is software that can typically run on most network devices and provides the interface between the SNMP manager and the physical devices being managed (Figure 5). The SNMP agent allows the network management system to access node-specific information from each of the managed network elements. A proxy-based system allows non-SNMP managed objects and the SNMP manager to communicate if an SNMP agent is not present (Subramanian, 2006).

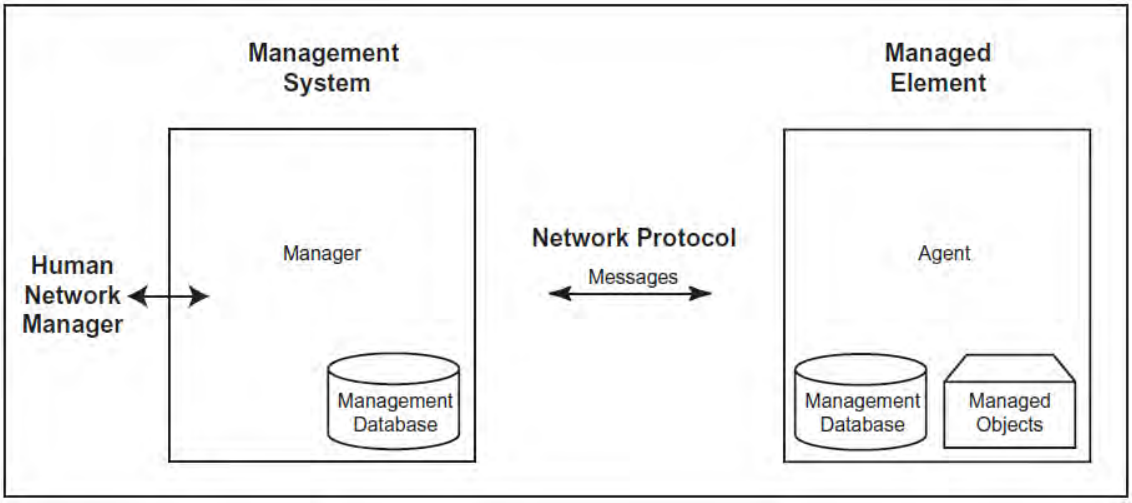


Figure 5 SNMP uses manager/agent architecture (From DenHartog, 2010)

a. Management Information Base

A well-designed management information base (MIB) is the cornerstone to any SNMP-based management system. The information contained in the MIB allows the NMS to monitor the status of remote devices in order to provide the NOC with network mapping, traffic monitoring, and alarms that provide automatic notifications when faults occur. Additional MIB elements allow for configuration and security management through the use of the NMS. Each SNMP element manages specific objects with each object having specific characteristics or variables. An Object Identifier (OID) distinguishes each variable individually in the MIB and in the SMNP messages. The manager and agents use the MIB and a small set of commands to exchange information. The MIB also serves as a data dictionary used to assemble and interpret SNMP messages. The MIB itself is a tree structure with individual variables, such as node status or description, being the leaves on the branches (Figure 6). The MIB associates each OID with a readable label and various other parameters related to that object. Each OID represents as a set of numbers separated by decimal points to indicate where that OID resides within the MIB tree (DenHartog, 2010).

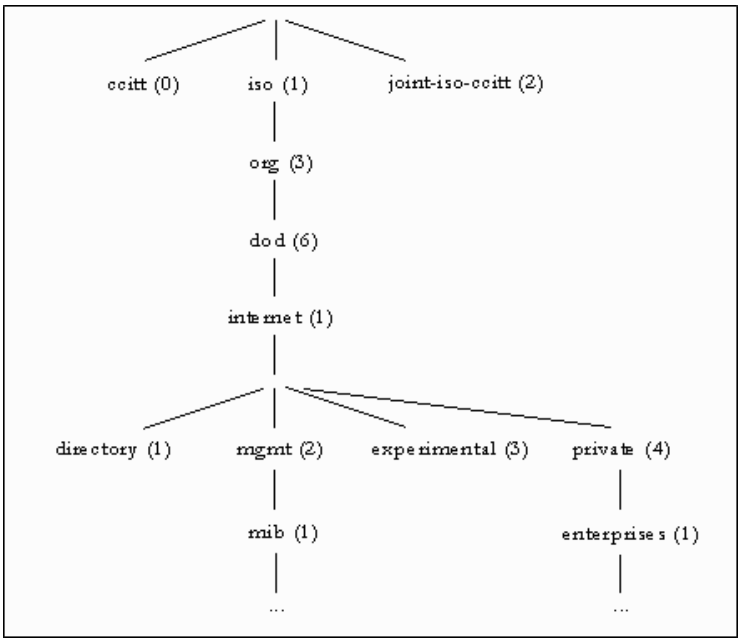


Figure 6 SNMP MIB object identifier tree (From Subramanian, 2006)

b. SNMP Messages

SNMP uses five basic messages (Get, GetNext, GetResponse, Set, and Trap) to communicate between the manager and the agent. The Get and GetNext messages allow the manager to request information for a specific variable. The agent, upon receiving a Get or GetNext variable message, will issue a GetResponse message to the manager with either the information requested or an error indicating why it cannot process the message. A Set message allows the manager to request a change to the value of a specific variable for the managed object. The agent responds to the Set message with a GetResponse to indicate that the change was made, or with an error message indicating why the change was not processed. The manager always initiates the Get, GetNext, and Set messages. The Trap is a change of state message and is the only message initiated by the agent. The agent can also use a Trap message to inform the manager of an important event such as an alarm (DenHartog, 2010).

SNMP is a packet-oriented protocol that uses Protocol Data Units (PDU) to communicate based upon the five types of SNMP messages. For example, an SNMP manager will assemble a Get packet containing the OID for each variable of interest

when it wants to know the status of a variable or characteristic. The managed element receives the Get request and looks up the OID in the MIB. A GetResponse packet contains the current status or value of the variable or characteristic for the OID requested. An error response indicates that the request was for an unmanaged object for an OID not found. Each variable binding within an SNMP packet contains an identifier, a type, and a value (if based on a Set or GetResponse). The agent checks each identifier against the MIB to determine if the object is managed and changeable (if processing a Set). The manager also uses the MIB to display the readable name of the variable and interpret its value (DenHartog, 2010).

SNMP relies upon a layered communication based upon the TCP/IP model to exchange information between managers and agents (Figure 7). An SNMP message resides at layer five of the model, the Application Layer and utilizes User Datagram Protocol (UDP), which resides at layer four, the Transport Layer. Unlike Transport Control Protocol (TCP), UDP is a connectionless protocol that places messages on a network without first establishing a connection with the recipient. Although UDP does not guarantee message delivery, it can transport a large number of messages while using fewer network resources than TCP. Internet Protocol (IP) resides at layer three, the Internet Layer.

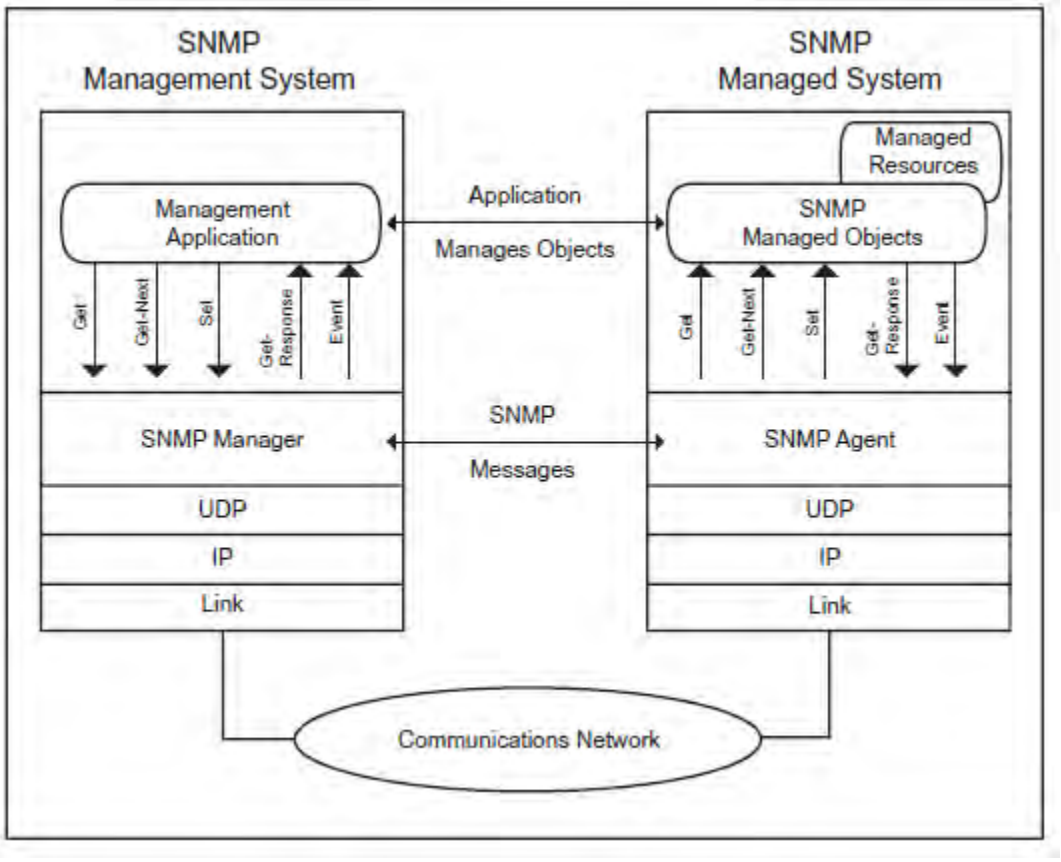


Figure 7 SNMP message passes through the protocol layers at the manager and agent (From DenHartog, 2010)

2. Remote Monitoring Agents

Remote monitoring (RMON) is a network specification that enables network monitors to exchange data even when communications with the network management system (NMS) are unavailable. This technique is useful in developing an NMS for a MANET because nodes will be entering and exiting the network frequently. RMON is an extension of SNMP and it provides another key advantage for the tactical network because a RMON can limit the network overhead of standard SNMP traffic. The RMON system uses probes to collect statistics on the remote devices and report to the management system (Subramanian, 2006). There are two versions of the RMON MIB, RMON version 1 (RMON1) and RMON version 2 (RMON2). RMON1 provides basic network monitoring at the media access control layer and below. The RMON1 MIB consists of these ten groups (IETF, 1995):

1. Statistics: real-time LAN statistics e.g., utilization, collisions, CRC errors
2. History: history of selected statistics
3. Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds
4. Hosts: host specific LAN statistics e.g., bytes sent/received, frames sent/received
5. Hosts top N: record of N most active connections over a given time period
6. Matrix: the sent-received traffic matrix between systems
7. Filter: defines packet data patterns of interest e.g., MAC address or TCP port
8. Capture: collect and forward packets matching the Filter
9. Event: send alerts (SNMP traps) for the Alarm group
10. Token Ring: extensions specific to Token Ring

RMON2 allows packet monitoring at the layers above the MAC such as application layer traffic monitoring. The RMON2 MIB adds these ten additional groups:

1. Protocol Directory: list of protocols the probe can monitor
2. Protocol Distribution: traffic statistics for each protocol
3. Address Map: maps network-layer (IP) to MAC-layer addresses
4. Network-Layer Host: layer 3 traffic statistics, per each host
5. Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts
6. Application-Layer Host: traffic statistics by application protocol, per host
7. Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts
8. User History: periodic samples of user-specified variables
9. Probe Configuration: remote configure of probes
10. RMON Conformance: requirements for RMON2 MIB conformance

D. DECISION SUPPORT SYSTEMS

An automated decision support system is also an important component of the 8th layer approach. Case-based reasoning (CBR) is an example of this type of system that uses knowledge gained from previously solved problems and extends it to the current situation. CBR provides a model for correlation for the NMS to use because incidents that occurred within the network in the past will likely repeat themselves and solutions discovered for previously resolved problems may apply to similar new problems even if the problem is not exactly the same. The CBR architecture includes the case library where previous situations and their solutions are stored. A query of the case library reveals if a matching solution already exists in a newly discovered situation. The closest match is adapted to the current situation if there is not a matching solution. The case library will update with the problem and its solution once it is resolved (Subramanian, 2006). Figure 8 shows the CBR cycle.

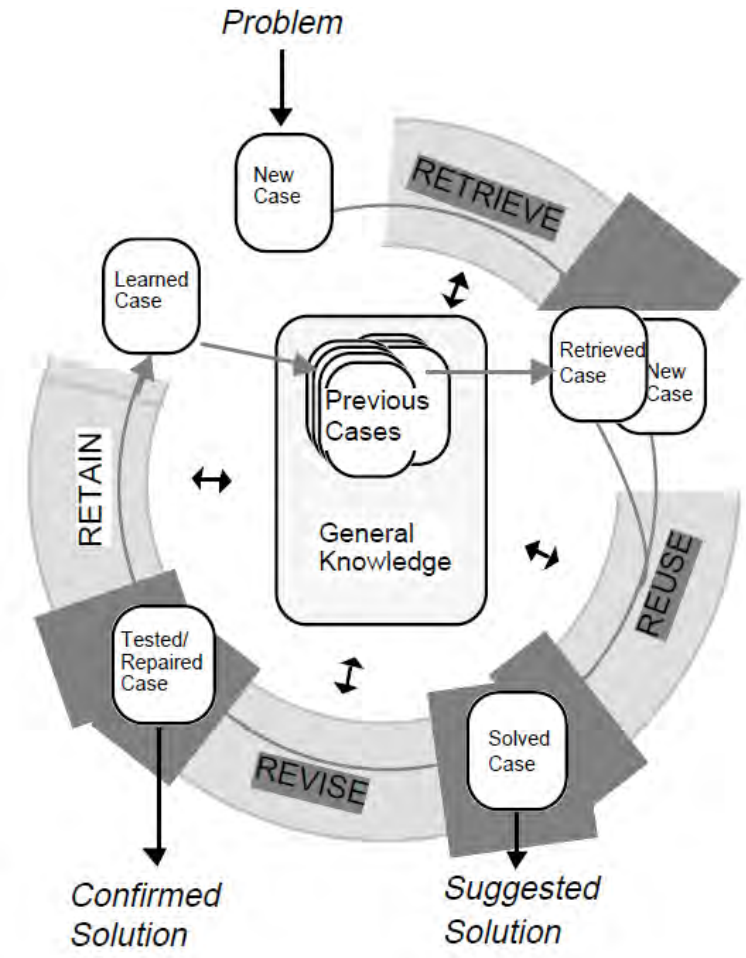


Figure 8 The CBR cycle (From Aamodt & Plaza, 1994)

E. MANAGEMENT STANDARDS FOR MOBILE AD HOC NETWORKS

There exists a significant amount of research attempting to develop standards for alternative management protocols used specifically for a MANET network management system. Despite these efforts SNMP remains the management protocol of choice. Some of the characteristics of the MANET, such as frequent reconfiguration of the network due to node mobility that dynamically changes the network's topology, are challenging for many commercially available SNMP-based network management systems. One of the many challenges in the tactical network is to reduce management traffic overhead due to limited throughput. Adhoc Network Management Protocol (ANMP) is compatible with SNMP and uses a hierarchical clustering of nodes to reduce the number of messages

exchanged between the manager and agents (Chen, Jain, & and Sing, 1999). Another alternative system is the Yelp Announcemement Protocol (YAP) that allows the agent to periodically report to the manager instead of the having the manager regularly poll the network (Chadha et al., 2004). Other efforts not focused on the specific protocol used exist to create a decentralized system that is capable of managing the unique peer-to-peer relationships active within the MANET (Brueckner & Parunak, 2004). The fact that there is no alternative standard established for MANET systems indicates that even though SNMP may not be ideal, it is the most common management protocol; therefore, SNMP can be adapted to the MANET environment as a means of standardizing how objects present information through the use of a MIB (Herberg, Clausen, & Cole, 2010).

F. TACTICAL NETWORK MANAGEMENT

A tactical MANET network management system (NMS-TM) that provides for MANET administration in both simulation-based and real-time operational environments can provide additional value for this network because it leads to an improved, more efficient flow of information. The Marine Corps Warfighting Lab website includes a description of the NMS-TM, which shows that the objectives for this network management system are to allow users to "predict, monitor, and control network behavior; this specifically includes viewing and remotely managing variables such as node status, node location, attached equipment, channel selection, frequencies, error rates, and network utilization." (http://www.marines.mil/unit/mcwl/Pages/C4.aspx) These variables are essential and will be included in the MIB for the NMS-TM system.

The most valuable pieces of the NMS-TM are likely to be features that allow the hypernodes to maximize connectivity or minimize communications disruptions by managing the physical location of other nodes within the network. Previous research shows the benefit of optimization algorithms used to move critical nodes to an optimal location in order to restore communications links within an ad hoc network while also minimizing the chance of disrupting other links within the network (Bordetsky, Bourakov, Statnikov, & Statnikov, 2005). This leads to many potential applications in

the tactical MANET system such as using aerial relay nodes managed by using these algorithms in order to optimize the network connectivity.

Ideally, this optimization solver will integrate with both the position location information found in the COP and the other variable information taken from the MIB. The NMS-TM must also be capable of receiving and storing the information so that the system can "learn" from previous network behaviors in order minimize the amount of recalculation that must be performed.

A robust network management system is essential for providing highly reliable and timely information at the tactical level. The NMS-TM will contribute towards information superiority by allowing valuable information to flow throughout the network and be delivered on time to those who need this information most. Emerging network-centric concepts potentially lead to even greater requirements for *adaptive networking* such as the integration of self-organizing clusters of semi-autonomous sensors and unmanned vehicles with human decision makers. In these predominantely mesh networks, every node has the potential of serving as a relay for other nodes and is capable of forming or healing the network based upon situational awareness of the status and capabilities of its neighboring nodes that have been learned through the 8th layer management information base.

G. SUMMARY

This chapter has explained how *model-based networks* and *adaptive networking* are key elements of the network-centric architecture needed to allow our forces to achieve a dominant information position based on accurate and timely dissemination of knowledge among distributed forces. The 8th layer architecture uses SNMP because this is an established standard for network management. The application of SNMP to the tactical network will require a new MIB that incorporates the most critical variables in this network. The next chapter provides an overview of the various segments of the tactical network, including the MANET segment and describes the unique capabilities of the TrellisWare CheetahNet handheld device used by the Marine Corps Warfighting Lab to provide the tactical MANET capability to tactical forces.

III. TACTICAL NETWORKING

During the wars in Iraq and Afghanistan, there was an "explosion in the demand for tactical communications." (Brinton, 2010) Tactical forces sought the advantages offered by Network Centric Warfare, but more often than not, the supply of bandwidth was not able to keep up with demand. Many consider tactical MANETs a key element needed to realize the vision of network-centric warfare because this provides an adaptive network to highly mobile forces. MANETs are also highly desirable because tactical forces typically operate in environments where existing telecommunications infrastructure is scarce, unusable, or completely nonexistent (Burbank, Chimento, Haberman, & Kasch, 2006).

A tactical network requires many wireless technologies (e.g., WiMAX, WLAN, cellular, and MANET) to meet all of the warfighter's needs. Each of these technologies is able to provide a unique capability based on its design specifications; therefore, they fill a particular niche within the overall scheme of the enterprise network architecture. This chapter explains why the tactical MANET fills one of the niches within the network architecture, and describes the characteristics of the TrellisWare CheetahNet tactical MANET that the Marine Corps Warfighting Lab has chosen to evaluate for intra-squad communications in support of Enhanced Company Operations.

A. RADIO FREQUENCY (RF) CHALLENGES OF TACTICAL ENVIRONMENTS

There are many challenges to providing reliable wireless communications in tactical environments. The technologies employed must be able to survive the elements (e.g., heat, dust, and rain), penetrate thick foliage, and overcome the loss of signal quality caused by multipath and Doppler effects. Multipath problems occur when transmitted signals do not arrive at the receiver solely from a straight line of sight path. When this occurs, the receiver combines signals from different paths; that can lead to signals fading and cancelling, thus resulting in temporary loss of a radio link. Doppler shifts occur

when the receiver and/or the source of the RF communications are moving. Multipath and Doppler effects can lead to bit errors and a reduced quality of the digital network (Fuller, 2008).

B. WIRELESS NETWORKING TECHNOLOGIES

Various wireless technologies are under evaluation or are already in use by operational forces. Among these technologies are: WLAN, WiMAX, cellular-based, satellite-based, and MANET. Previous research provided an analysis of the qualities of many of these various technologies based on their ability to support ECO (McHuen and Price, 2009). Each of these technologies has unique features that allow it to fill a particular niche and each has shortcomings that require the incorporation of other technologies into the network. Because this differentiation is likely to continue, the network management system design must include the basic elements incorporated into any tactical wireless technology.

1. WiMAX

The Institute of Electric and Electrical Engineers (IEEE) 802.16 standard defines the standards for Worldwide Interoperability for Microwave Access (WiMAX) (IEEE, 2004). WiMAX provides point to multipoint, broadband communications to areas not connected by fiber optic or copper cabling. WiMAX is capable of providing throughputs of up to 70 megabits per second and has a range of approximately 50 kilometers. WiMAX uses a multicarrier modulation scheme known as Orthogonal Frequency Division Multiplexing (OFDM). A limitation of WiMAX is that OFDM is sensitive to multipath and Doppler effects that occur in rapidly changing RF environments such as with mobile users (Fuller, 2008).

2. WLAN

The IEEE 802.11 series defines the wireless local area network (WLAN) standards (IEEE, 2007). The most common of these standards in use today will include 802.11g and 802.11n. A WLAN can typically provide throughputs of 54 megabits per second and a range of 100 meters without the need for copper cabling. Most WLAN

implementations have the advantage of a fixed access point in order compensate for some of the effects of changing RF conditions; however, a truly mobile ad hoc network must support mobility without being tethered to a fixed infrastructure.

3. Satellite-Based Systems

Satellite-based solutions provide beyond line of sight connectivity, but the availability of satellite channels is limited for tactical users. The existing military satellite system known as the UHF Follow-on system (UFO) only provides capacity for 600 concurrent users. DoD users also have commercial services such as Iridium to fill this access gap. That is no panacea, however, since commercial satellite services may not be available when DoD needs them most (Rosenberg, 2010), and it is cost prohibitive to use satellite connectivity exclusively (U.S. Navy To Rely on Netted Iridium Service as Gap-Filler, 2010).

The long-term solution in lieu of commercial satellites systems is the Mobile User Objective System (MUOS) that provides cutting edge technology based on commercial 3G cellular phone services. MUOS offers both voice and data in a converged, handheld device. However, the MUOS program has experienced several technical problems that delayed the launch of its first satellite, and there are other issues with the development of the MUOS handsets (Iannotta, 2009). It is likely to be several years before the capabilities offered by MUOS are available to the majority of DoD's tactical forces.

4. Commercial Cellular

The use of commercial cellular technologies on the battlefield has gained significant attention because senior military leaders recognize the potential benefits of putting these devices in the hands of a generation of soldiers and marines that have grown up using this technology. The basic requirements of any cellular network are the handsets and the cellular base stations that are typically associated with towers to increase network coverage. Current capabilities of the tactical cellular network provide throughputs of 1.8 megabits per second while ranges are dependent on the height of the mobile cellular tower placed on a tactical vehicle such as Mine Resistant Ambush

Protected (MRAP) vehicle (Lowler, 2009). The current tactical cellular solution is best suited for special operations soldiers who operate in small groups. This network requires a tethered aerostat or a circling aircraft equipped with a cellular base station in order to relay the communications. Other architectural designs have focused on integrating the cellular handsets with tactical radios filling the role of the base station (Tuttle, 2010). That used the cellular handset essentially as an external computer in order to host command and control (C2) and situational awareness (SA) applications in this case. A more efficient architectural design entails developing the tactical radios to host the C2 and SA applications internally, thus eliminating the need for an external computer worn or carried by soldiers ("New Military Radio Unveiled," 2011).

C. MANET SYSTEMS

MANET technologies are highly desirable in tactical environments because each node in the network is able to communicate with all other neighboring devices over one or more hops in order to extend connectivity to areas where a fixed infrastructure is not available. There are many factors that influence the performance and reliability of a MANET. Communications links within the MANET are continuously fluctuating due to the location of devices, power, or environmental factors.

MANET technologies are valuable for enhancing command and control because they provide network connectivity beyond line of sight and in harsh environments where this previously was not possible. A tactical MANET provides considerable flexibility through its rapid deploy-ability to provide a wireless voice and data network without any fixed infrastructure. The general characteristics for a tactical MANET include attributes such as rapid deploy-ability, ease of use, mobility, and flexibility. These features make it very suitable for military applications in environments where setting up fixed infrastructure may not be feasible or practical. The MANET nodes also allow transmission of position location information (PLI) in real-time to increase situational awareness at the company level.

1. TrellisWare CheetahNet (TW-220)

The TW-220 is a tactical MANET system that provides 220 kilobits per second (Kbps) data rates while extending communications beyond line of sight because transmissions are relayed by surrounding radios at up to 8 hops across the network. A hop is the number of relays that any individual node is away from the CheetahNet's command node. The command node is also the network timing reference, which is the reference point where all of the hop counts begin. In the TrellisWare network, every marine in the company acts as a potential repeater for all other radios in the TrellisWare network. The GPS based PLI displayed on digital maps provides each squad leader with a higher level of situational awareness in order to allow small units to achieve self-organization and self-synchronization effects of network-centric warfare.

The TW-220 is considered a software defined radio that enables both voice and data streams to be simultaneously transmitted and forwarded over a tactical MANET. The general characteristics of the TW-220 are: support for up to 8 push-to-talk (PTT) voice channels, connections for external data sources via a universal serial bus (USB) cable, an Ethernet cable, or a Bluetooth® enabled device. The TW-220's embedded GPS modules allow PLI tracking via keyhole markup language (KML) or java script object notation (JSON) format, multi-hop relay extensions of up to 8 hops, and the capacity to send simultaneous video, voice, and file transfers over the network. The advantages that the TW-220 provides are its ability to track PLI of individuals instead of units and to extend simultaneous voice and data networking to the warfighter.

The TW-220 utilizes TrellisWare's Modern Topologically Extreme Waveform (TopX-II), which supports self-forming and self-healing network characteristics (Figure 9). Self-forming occurs as multiple operators discover the edge of the tactical network and go out of range of the main network. The TW-220 allows those operators to self-form their own network and continue to communicate with one another. When any one of those operators comes back into range of the main network the networks will merge or self-heal and all of the operators will re-join to the main network.

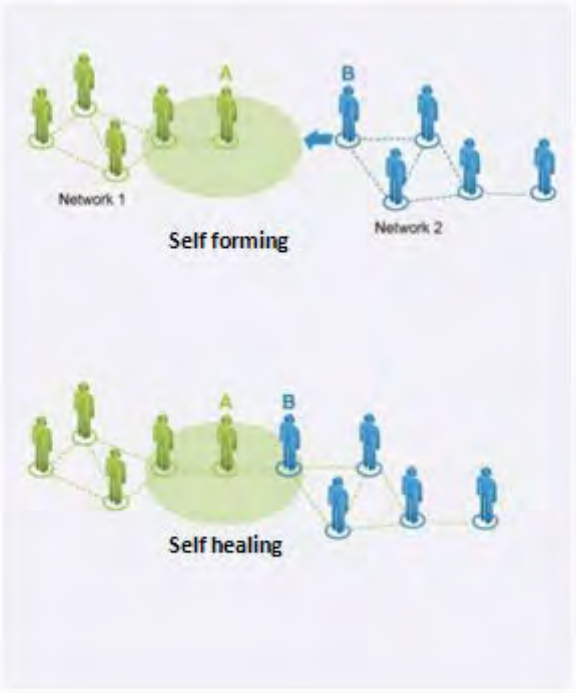
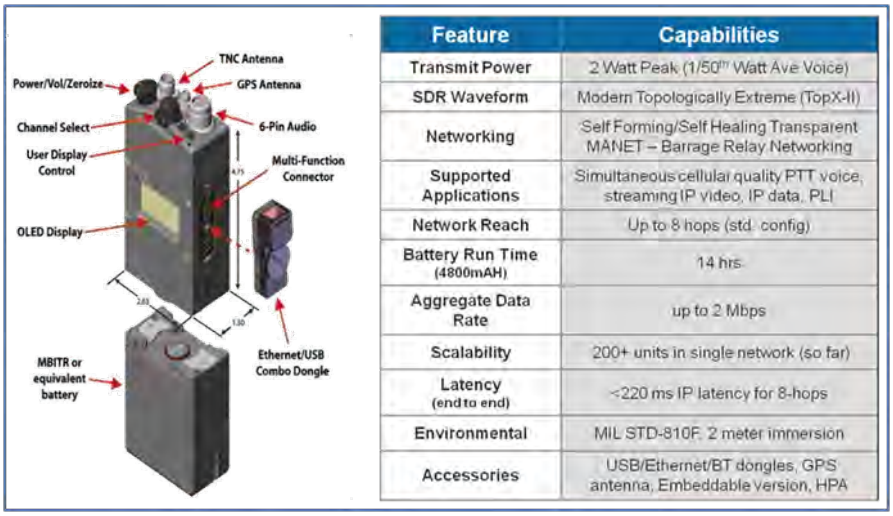


Figure 9 Self-forming and self-healing (From TrellisWare, 2010)

Figure 10 shows the specific characteristics and general capabilities of the TW-220 (TW-220 User's Guide, 2010). The TW-220 is able to perform well in challenging multipath RF environments through its use of barrage relay networking technologies that allow the TW-220 to resolve multiple transmissions from multiple sources as multipath components of the same signal (Fuller, 2008). One advantage that the TW-220 has in these challenging environments is that it is able to employ the simplest type of algorithm for packet routing: each radio re-transmits every packet it receives. The TW-220 has also demonstrated its superior scalability while forming tactical MANET networks of up to 200 nodes with little to no configuration needed once the network is deployed (LaGrone, 2010). This is substantially greater than the currently fielded Harris MANET solution that is capable of no more than 10 radios in a single network (Advanced Wideband Networking Waveform: An Overview for the AN/PRC-117G, October 2008).



Feature	Capabilities
Transmit Power	2 Watt Peak (1/50th Watt Ave Voice)
SDR Waveform	Modern Topologically Extreme (TopX-II)
Networking	Self Forming/Self Healing Transparent MANET – Barrage Relay Networking
Supported Applications	Simultaneous cellular quality PTT voice, streaming IP video, IP data, PLI
Network Reach	Up to 8 hops (std. config)
Battery Run Time (4800mAH)	14 hrs
Aggregate Data Rate	up to 2 Mbps
Scalability	200+ units in single network (so far)
Latency (end to end)	<220 ms IP latency for 8-hops
Environmental	MIL STD-810F, 2 meter immersion
Accessories	USB/Ethernet/BT dongles, GPS antenna, Embeddable version, HPA

Figure 10 General characteristics of TW-220 (From TrellisWare, 2010)

The TW-220 system has the functionality of a handheld radio device with the additional capacity to serve as a mobile wireless repeater. When troops carry this device, it not only provides them with a means of voice communication, but each radio serves as an extension of the network. Each node in the MANET has the potential to relay all other data and voice communications to other distant nodes within the network. Because each unit relays traffic over the network, adding additional nodes (radio units) to the network extends the operational range of the network.

The most desirable characteristics of the TrellisWare system are its ability to perform well in high multipath environments (Fuller, 2008), and support highly mobile nodes that do not rely on any fixed infrastructure. Once configured, the TrellisWare radios require essentially no end user interaction so there is limited need to provide any sort of special end user training. Finally, the TrellisWare system supports very high node densities in a single network.

2. MANET Use Case in Support of Enhanced Company Operations

During a major Naval exercise called Rim of the Pacific (RIMPAC) 2010, each marine in a company (i.e., Golf Company, 2nd Battalion, 3rd Marines) used a TrellisWare radio and each squad leader (Figure 11) could track position location

information on a mapping server. This exercise was the culmination of over three years of research and experimentation by the Marine Corps Warfighting Laboratory (MCWL) to test whether or not communications could support the tactics of an over-the-horizon company level assault of an objective. In this exercise, Golf Company executed a simultaneous two-pronged assault using experimental equipment and the emerging ship to objective maneuver (STOM) doctrine. Much of the exercise took place in the 7,300 acre Kahuka range dominated by challenging electromagnetic conditions, such as a triple canopy jungle. This test demonstrated the operational readiness of the TrellisWare CheetahNet system in providing voice, data and PLI capabilities to the individual marine across an 8 kilometer range with 10 mile links to helicopter assets. Marines participating in this exercise reported that they felt the CheetahNet system was ready to deploy "as-is" (LaGrone, 2010).

Figure 11 PLI from 200 node MANET during MANET use case (From LaGrone 2010)

3. Future TrellisWare CheetahNet Capabilities

The TW-220 version of the CheetahNet has been in production since 2007. TrellisWare also has offered the TW-120, or WildCat since 2008 to provide 20 watt power amplification of for the TW-220 system. The TW-220 form factor currently is 17.5 inches; it operates strictly in the ultra-wideband band frequency (UHF) range, and can support maximum data rates of up to 2 megabits per second (Mbps). In late 2011,

TrellisWare has plans to begin production of a 9.5 inch CheetahNet version (capable of 20 Mbps) that is used for intelligence, surveillance, and reconnaissance (ISR) missions. This new system will include 72-hour battery life, on board video compression, and server and router capabilities. A new WildCat II version is currently being developed to offer up to 40 Mbps data rates and quad band RF capabilities. The CheetahNet II, available in late 2011, offers 20 Mbps data rates and quad band capabilities. Future developments of the CheetahNet product line could incorporate type I encryption, SATCOM capabilities, as well as smaller form factor (9.5 inches) versions used by troops on the ground.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. APPLYING THE 8TH LAYER TO THE TACTICAL MANET NETWORK MANAGEMENT SYSTEM

The Marine Corps Warfighting Lab (MCWL) is developing the tactical MANET network management system (NMS-TM) for the Next Generation Command and Control (NGC2) radios (including TrellisWare CheetahNet) and has asked the Naval Postgraduate School to investigate the relevance of the 8th layer to the prototype NMS-TM application that has been developed by TrellisWare Technologies. Specific objectives of this investigation include:

1. Research the feasibility and benefits of a common management information base (MIB) within the NGC2 family of radios (TrellisWare surrogate radios) and the NMS-TM application.

2. Research the best employment of ground sensors in a TrellisWare surrogate MANET and in mesh/mobile ad-hoc networks in general in relation to hypernodes and the 8th-Layer.

3. Explore bandwidth adaptive solutions for hypernodes to adjust their network loads at the application layer.

4. Examine how to make NMS-TM alert the user regarding how to geographically adjust nodes to improve the overall network.

5. Research how hypernodes can support sensors in how and when to send data based on link health, network health, and bandwidth availability.

6. Examine how hypernodes on-the-move can propagate sensor data in relation to link health and bandwidth availability.

This chapter describes how SNMP and a MIB could be applied in order to add 8th layer capabilities to the NMS-TM. The next chapter of this thesis focuses on how these variables impact network performance measures in order to make recommendations on the most critical MIB variables for the NMS-TM.

A. SNMP MANAGEMENT INFORMATION BASE VARIABLES

The 8th layer approach requires a new RFC that extends the existing SNMP MIBs to include additional variables for the service and business management layers (Bordetsky and Hayes-Roth, 2006). These additional variables include:

1. Application switching
2. Node physical mobility initiation
3. Receiver Context and Requirements Modeling
4. Sender Dynamic Information Context and Transmission Requirements Modeling
5. Recipient context determination
6. SLA generation
7. SLA negotiation
8. Quality of service (QoS) monitoring and SLA assurance

Additionally, the MCWL has identified these variables for the NMS-TM system:

9. Node status
10. Node location
11. Attached equipment
12. Channel selection
13. Frequencies
14. Error rates
15. Network utilization

B. NMS-TM CURRENT NOC VIEW

The current NMS-TM NOC view is a prototype browser-based application developed by TrellisWare Technologies. This NOC view enables real-time monitoring and control of the tactical MANET. This web-based network management system can run on any personal computer (PC) connected to one of the CheetahNet radios. The Network Management System is accessed through the PC's web browser and is able to receive CheetahNet variable information from all other CheetahNet radios wirelessly connected to the network (Figure 13).

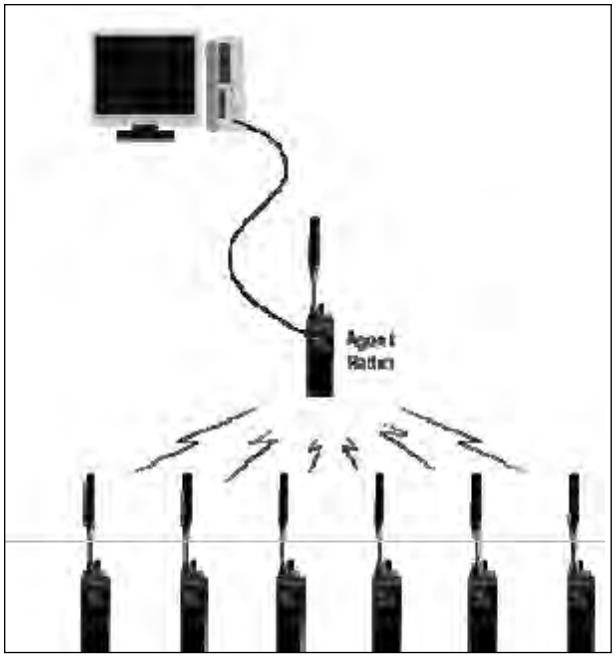


Figure 13 Relationship between PC, agent radio, and network of radios. (From Technical Note CN-TN-028)

In order to open the NMS application, an operator must first access the TrellisWare Applications homepage by opening the web browser and typing in the address of any CheetahNet radios into the browser's address bar (Figure 14). The operator then opens the Network Management System by clicking on the NMS icon.

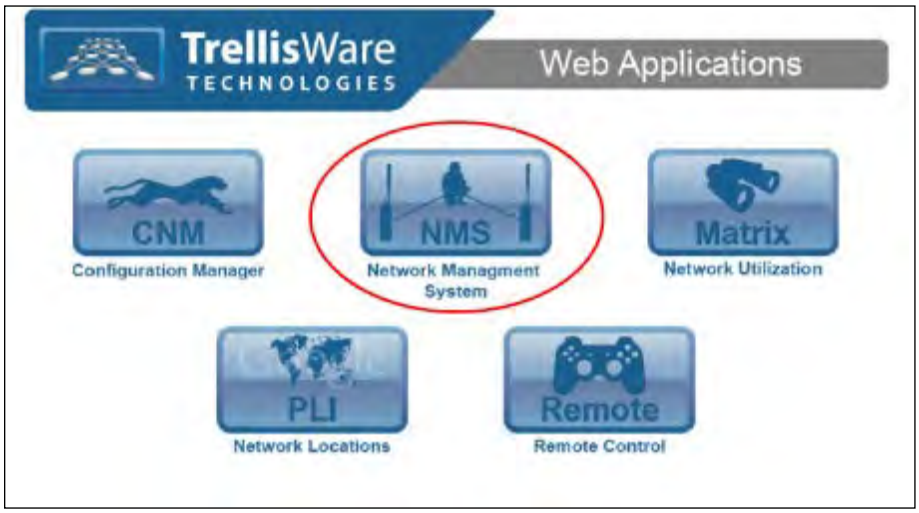


Figure 14 Web applications page (From Technical Note CN-TN-028)

The Network Management System currently includes the following functionality:

1. List of all nodes that are connected to the network
2. View of any unit alerts that have been reported
3. Network mapping that includes link status information
4. Ability to perform over the air rekey (OTAR)
5. Ability to perform over the air zeroize (OTAZ)
6. Ability to remote control any unit in the network

Once the operator has started the Network Management System application, he or she will be able to select the particular windows within the Network Management System by selecting these items from the NMS open menu (Figure 15). The items available from the open menu are alert, map, node list, OTAR, remote control, and network usage. The operator can open multiple instances of each window type (except for alert windows) and can move these windows around as needed in order to have a more complete view of the network.

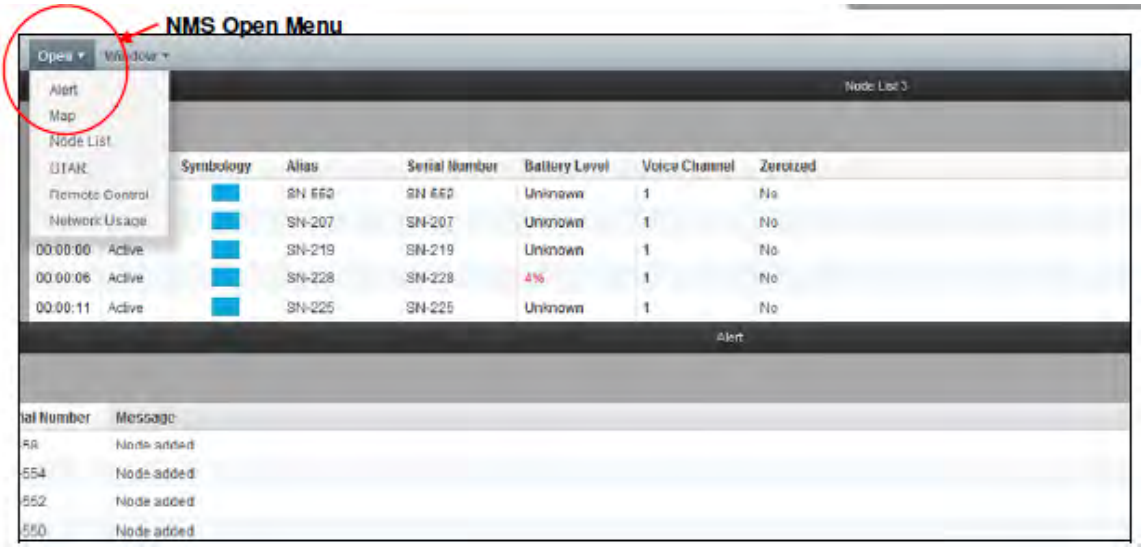


Figure 15 NMS open menu (From Technical Note CN-TN-028)

The NMS window menu allows the operator to hide or show any of the windows that are currently open. This menu allows the operator to resize any of the windows and to select columns to search from in any of the table views (Figure 16).

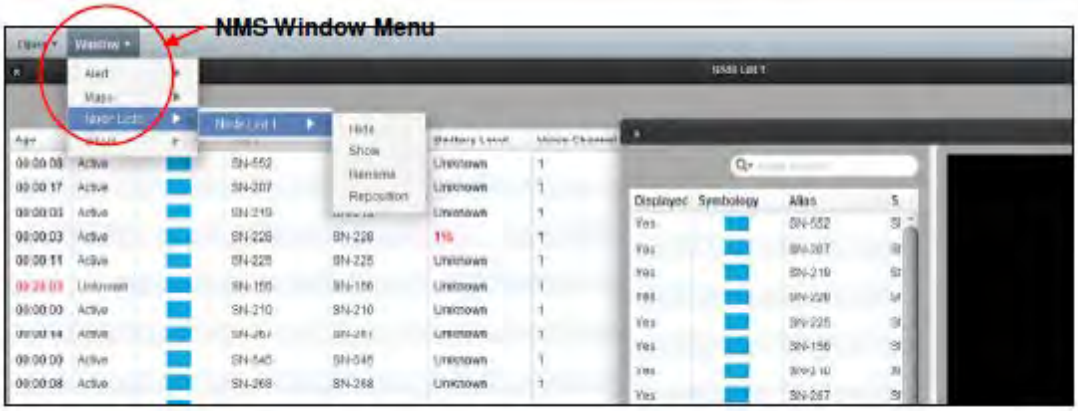


Figure 16 NMS window menu (From Technical Note CN-TN-028)

The alerts window allows the operator to see any unit alerts that have been sent to the Network Management System. The current capabilities include alerts for any units that have a low battery status or units that have requested a cryptographic re-key. The alerts window is a table view that includes the date and time of the alert message, unit alias, unit serial number, and a brief description of the message (Figure 17).

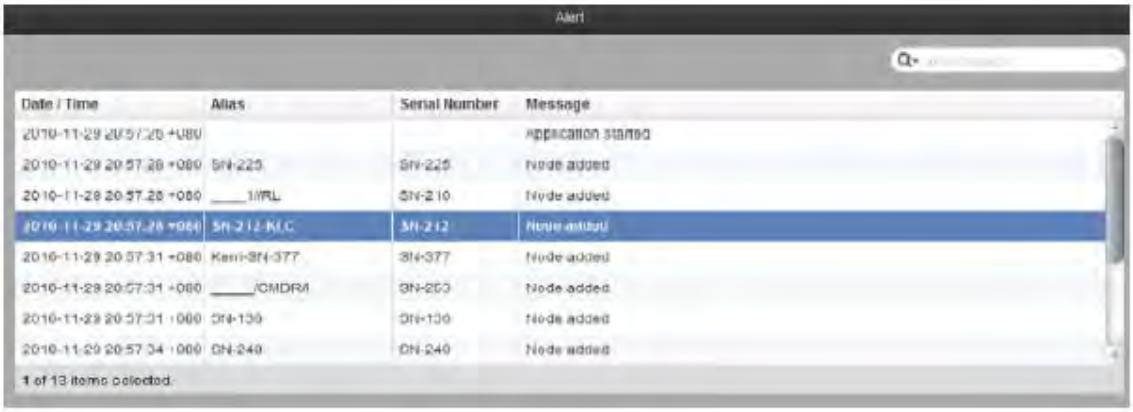


Figure 17 Web applications page (From Technical Note CN-TN-028)

The map window displays the physical node location on any map-based application (Figure 18). The operator's PC, which runs the map applications, must meet the following minimum requirements:

1. Operating System: Windows XP or Windows 7, Mac OS X, Linux
2. Web Browser: Mozilla Firefox 3.6+
3. Java: Java Runtime Environment (JRE) version 1.6.0_21+ (for maps)

4. WorldWind Map Server: GeoServer 2.0.2 (for maps)
5. CPU: Core Duo, 2.4 GHz+
6. System Memory (RAM): 2GB.
7. Hard Disk: 4GB free space (depending on imagery)
8. Graphics Card: 3D Capable with 256MB VRAM
9. Screen: 1024x768 pixel resolution

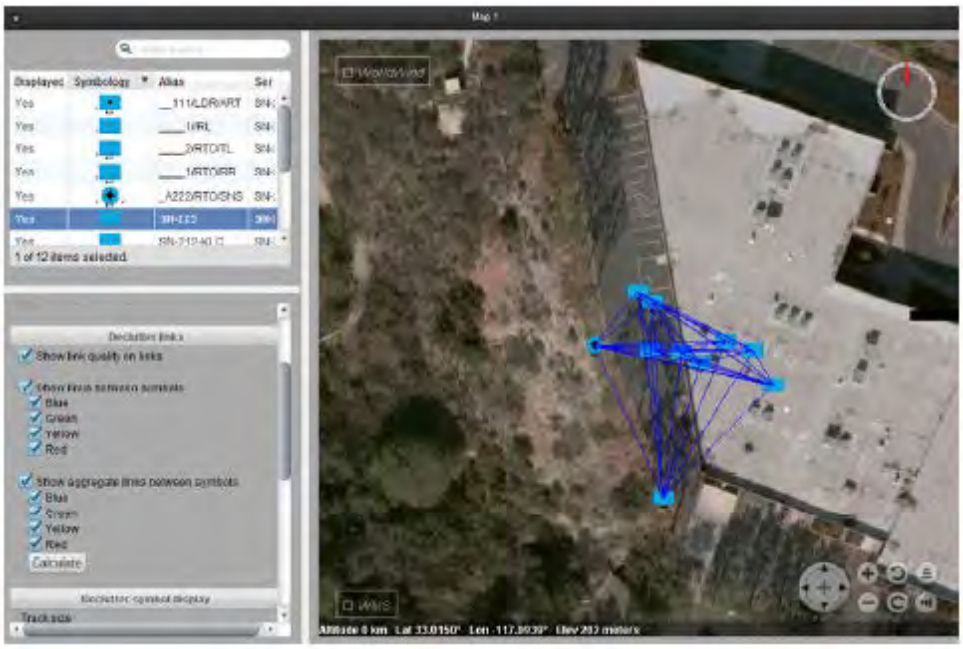


Figure 18 NMS map display (From TrellisWare Technical Note CN-TN-028

The map display uses pre-existing military standard symbols for each node based on the type of unit that node represents. Within the map display the operator is able to choose filtered views in order to de-clutter the map based on unit echelon (i.e., battalion, company, platoon, squad, or team lead) or to de-clutter based on link status. The link status displays the link quality either between individual tracks (i.e., hops) or as an aggregate link to the command unit. The link status display uses different colors to indicate link quality. The operator can also de-clutter the map to only show a particular color link as well, for example only display red or yellow links in order to quickly visualize any units with a poor signal. The color and their indicator are:

1. Red=acceptable voice, poor data
2. Yellow= good voice, acceptable data
3. Green= good voice, good data
4. Blue= excellent voice, excellent data

The node list window is a table-based view of all of the units in the network. Clicking on the column headers also includes a search box as well that will sort this table. The node list provides real-time information for each unit such as age, status, serial number, battery level, voice channel, zeroized status, and alert count (Figure 31). The operator can right click on any of the units from the node list in order to see a menu that will allow the operator to perform an over the air rekey or over the air zeroize on the selected unit.

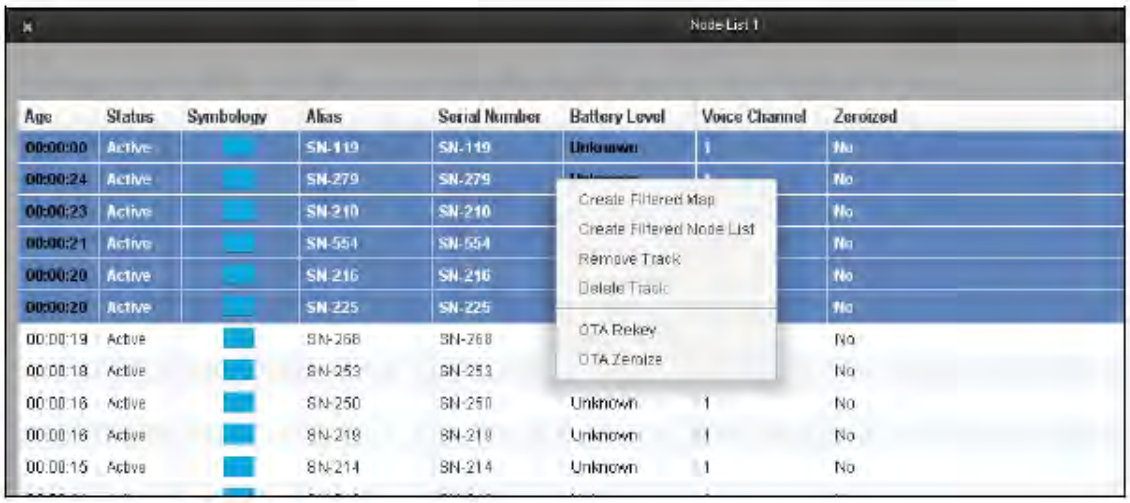


Figure 19 Node list from NMS (From Technical Note CN-TN-028)

The remote control window is also available through the NMS open menu and it allows the operator to change certain device parameters such as frequency, power settings, volume, voice channel, and to zeroize the cryptographic keys. While the current NMS-TM as developed by TrellisWare Technologies is able to incorporate many of the necessary variables into the NOC view this monitoring requires a “human in the loop” for any configuration changes. Future upgrades to this NOC view must allow machines to do more of this processing in order to reduce the burden on human operators.

C. VALUE ADDED TO NMS-TM BY THE 8TH LAYER

The current NOC view as developed by TrellisWare Technologies in the NMS application includes link status, signal, and range information in the map view but requires a human operator to reconfigure any of these variables by re-locating any nodes to provide additional relays for critical nodes. Because the current system does not use the SNMP standard these variables are not in an OID or MIB structure. The development of the 8th layer SNMP monitoring will add value to this system by not only collecting these network performance measures, but comparing them to business management layer and service management layer constraints in order to optimize network coverage and reconfigure critical variables without requiring a human operator.

Additional MIB variables that monitor SLA and QoS constraints will include throughput, latency, and application layer information to add greater value to this system, particularly when new ISR versions of the CheetahNet are deployed in the network that support server and router functions. Finally, the use of SNMP standards within the NMS-TM could lead to the collection of MIB information from all wireless systems including WiMAX, WLAN, satellite, and cellular systems from across an integrated tactical network architecture. This would allow messages to be passed through other means when tactical links are unavailable.

D. NMS-TM 8TH LAYER CAPABILITIES AND ARCHITECTURE REQUIREMENTS

The development of an RF "heat map" capability would enhance the NMS-TM and allow greater capabilities such as forecasting network coverage and identifying where additional relay nodes are required in order to support the tactical scheme of maneuver. These additional relay nodes could be passive relays such as unattended nodes placed in favorable locations where line of sight is present. Another option is to increase the number of troops within the formation that carry a MANET radio, which also creates more relay links. Unmanned vehicles could also support the movement of relay nodes within the network. A solver application could optimize the network by

relocating these additional nodes to areas where network coverage is weak. For example the solver could calculate the waypoints for unmanned vehicles that provide aerial relays

These types of capabilities require algorithms capable of performing terrain analysis since location is one the critical network variables that determines relay node placement. The use of a decision support system such as Case-Based Reasoning would enable predictive capabilities through the replay of previously recorded cases for forecasting future or planned network coverage in unknown situations based upon knowledge learned from previously recorded experiences. This replay capability requires a database system that must be included into the network management system architecture. The two most likely sources for collecting the data that would be stored within the NMS-TM database would be to capture this data from the information streams passed within the web based NMS architecture, or to incorporate an RMON capability within each node in the TrellisWare network.

1. Web-Based NMS Data Streams

Each node in the TrellisWare network reports information on the critical network variables through series of hypertext transfer protocol (http) Get and Post methods. This web–based reporting uses java script object notation (JSON) data streams that could populate the data used by the NMS-TM database system in order to provide enhancements such as replay and network analysis capabilities. Below is an example of the data captured from JSON data streams[4]:

1. voice_channel: 1
2. battery: 96
3. age: 0
4. hop_count: 1
5. zeroized: false
6. alias: 144
7. serial_number: 224
8. unit_id: 00:1e:3f:00:4b:20
9. location: mgrs: 10S FF 00281 49640
10. altitude: 32.0
11. longitude: -121.87900543212891
12. latitude: 36.58697509765625

[4] The sample JSON data was collected using the WireShark network analyzer.

13. climb: 0.0
14. speed: 0.0
15. heading: 350.0
16. distance: 5.75
17. link_quality: 33.0
18. age: 0
19. destination_id: 00:1e:3f:00:53:a0
20. source_id: 00:1e:3f:00:4d:40

2. Hypernode RMON Agents

Each node in the tactical MANET must be capable of including a RMON agent to retain node status and performance data during situations when connectivity to the command network is unavailable. It is common for nodes within the tactical MANET that are at the edges of the network to exit the command network and form alternate networks. An RMON agent will allow these nodes to continue to collect node status and local area network information, and transmit this data to the NMS as soon as these nodes re-connect to the command network. This technique would also allow the node to select an alternate means for transmitting this data such as using the Iridium satellite link if that is available. This will be of even greater significance when tactical MANET nodes are the communications backbone used to transmit data from unattended sensor devices. In these cases, the tactical MANET nodes equipped with sensors are essentially separate local area networks monitored by the RMON agent.

E. SUMMARY

The 8th layer will add value to the tactical network by enabling intelligent and adaptive network control within the tactical mesh network and enabling the concept of VIRT by giving priority to highly valued information and filtering out low value bits (Hayes-Roth, 2005). Adaptive network control uses computing resources to optimize the network and allows human operators to focus on other tasks. The 8th layer allows this by providing each node with its own NOC capability based on feedback information received from network monitors including the SNMP events monitor, the situational awareness (SA) constraints monitor, and the service level agreement (SLA) constraints monitor. The approach chosen to initially develop the 8th layer incorporates the

functionality of all three monitors into a single SNMP monitor because this is a well-established standard. The next chapter documents field research conducted to make recommendations on the critical network variables and management database structure required to support these NMS-TM enhancements.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESEARCH METHODS, DATA COLLECTION, ANALYSIS

This research occurred in three separate phases. The first phase of testing occurred during Tactical Network Topology (TNT) experiments, specifically TNT 10–01 in November 2009. During this phase, a tactical MANET based on the TrellisWare CheetahNet supported communications requirements for a notional battalion level operation. The TrellisWare TW-220 radios provided voice and data communications between the notional combat operations center (COC) and the actors playing the role of platoon, squad, and team leaders. Data applications included live streaming video, file transfer, and position location reporting into the situational awareness view using Cursor on Target.

The second phase of data collection occurred at TNT 11-03 in May 2011. That event focused on whether or not network performance such as throughput and latency changed when the number of physical hops and/or node density within the network was increased. The final phase of testing occurred during TNT 11-04 in August 2011, where the TrellisWare data collection utility collected network data to analyze the relationships between network variables and network performance criteria.

A. PHASE 1: TRELLISWARE EVALUATION

The basic concept of operations (CONOPS) selected to evaluate the TrellisWare CheetahNet was based on requirements developed by Headquarters Marine Corps Command, Control, Communication, Computers (HQMC C4) and First Marine Expeditionary Force (I MEF) to validate the ability of a radio[5] that used the Advanced Networking Wideband Waveform network (ANW2). This CONOPS was chosen because it addressed the urgent requirements for a wideband networking radio capability that was submitted by I MEF Forward in support of current operations (IMEF and HQMC C4, 2010).

[5] Designated AN/PRC-117G (Army/Navy Portable Radio Communication).

The TrellisWare validation was conducted during the Tactical Networking Topology (TNT) 10–01 at Camp Roberts, California from 11–21 November, 2009 (King & Puff, 2009). The phase 1 evaluation considered the following requirements:

1. Combat Relevant PLI. The ability to map PLI information to a specific individual or entity in order to de-conflict Fires
2. Marine Air Ground Task Force (MAGTF) Shared Situational Awareness. The ability to utilize live streaming video between troops in contact and higher echelons of command in order to prosecute Fires
3. Tactical Data Network Extension. The ability to provision consistent, persistent, and sustained network services and data over tactical radios.
4. Continuous Internet Protocol (IP) traffic and continuous synchronization between databases

The concept of employment was based on a battalion communications scenario (Figure 20) where one wireless domain provided data and voice connectivity for two notional rifle companies throughout the battalion's area of operations (AO). The rifle companies each had their own dedicated voice channel for internal communications. Additional voice channels were allocated for commander and co-commander communications and a fourth channel was used for open communications with every unit in the network. A WildCat unit was set up in the COC as the commander's radio. In addition each company also had a co-commander radio that was also a WildCat unit. The rest of the units in both companies consisted of handheld TW-220 units.

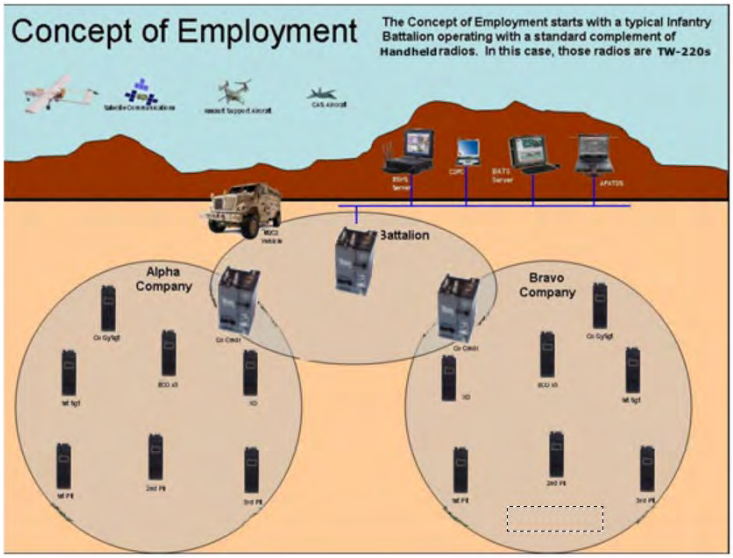


Figure 20 Concept of employment used for testing NMS-TM for CheetahNet (From King & Puff, 2009)

1. Equipment List and System Configuration Settings (Same for all Phases)

a. TrellisWare 220 Radios (Figure 21)

The TrellisWare radios used for field testing were configured as follows:

1. Profile: 2
2. Voice Channels: 3 voice/1 over ride
3. Maximum Voice/Data Hops: 8
4. Data Rate Range: 225–245 Kbs
5. Standard manpack antenna

Figure 21 TW-220 CheetahNet radio

b. Personal Computers with Windows XP w/SP 3 (Figure 22)

The personal computers used for field testing were configured as follows:

1. NAV
2. Mozilla Firefox
3. Ixia Chariot Q-Check or IPerf
4. CheetahNet Manager
5. FileZilla FTP server
6. Unreal Media Server 6.0 and Unreal Streaming Media Player
7. NPS Cursor on Target Parser Application
8. WINDOWS FIREWALL TURNED OFF

Figure 22 PC connected to CheetahNet radio

2. Results of Phase 1

a. Live Video.

During the TNT scenarios, the transmissions of two separate live video feeds from any node on the TrellisWare network to any other node on the network was successfully demonstrated (King & Puff, 2009). These tests also demonstrated that the video feed could be maintained from a mobile node and could be re-established upon that node exiting and re-entering the command network.

b. Transmission and Collection of PLI Information.

PLI information was collected from up to 30 mobile and fixed nodes and displayed in the Google Earth™ application at the notional battalion COC as well as at a mobile node with a laptop connected.

c. Voice Traffic

The results of testing at the TNT 10–01 exercise suggest that reliability and availability of voice communications across the TrellisWare mesh network is enhanced when greater node density is deployed across the network. Initially, results showed that a mobile node was not able to sustain continuous voice communications while traveling from the notional battalion jump CP located at the Scan Eagle site to the COC location or to main side at Camp Roberts. After the fixed nodes were emplaced using multiple TW-120 Wildcat HPAs and 50 foot antenna masts with omni-directional antennas, communications were maintained from the Scan Eagle site to the main side. After further increasing the number of nodes that were deployed, communications with a mobile node (recon OP) from beyond the East Garrison site to the Scan Eagle site was maintained.

Figure 23 Map of fixed and mobile TrellisWare nodes during TNT 10–01

d. Network Formation (Self-healing)

The TW-220 radios clearly demonstrated the self-forming and self-healing aspects of a MANET as seen in the ability to exit and re-enter the network without requiring any user interaction. During the course of the experiments there were periods where the radio nodes dropped from the network (generally due to terrain obstructions) for short periods and alternate networks (MANETs) were formed with other nodes that were still within range. Once the primary network became visible again, the radio units automatically re-established connectivity to the primary network and were able to send voice, data, and PLI traffic without any interaction by the user. Additionally, the radios provided the user with an audible alert whenever they entered or exited a network.

B. PHASE 2: INVESTIGATION OF NETWORK PERFORMANCE MEASURES TO NODE DENSITY AND PHYSICAL HOPS WITHIN THE NETWORK

The second phase of testing occurred at Camp Roberts, California from 09–11 May 2011. The Center for Network Innovation and Experimentation (CENETIX) Situational Awareness Replay tool captured and time stamped all events. The specific measures of performance (MoP) and measures effectiveness (MoE) collected were *range*, *coverage*, *network throughput*, and *network latency*. In this test, the command radio resided inside the combat operations center (COC) at the airfield located at Camp Roberts. During this test, all TrellisWare radios were set to transmit at two watts power with the standard antenna at ground level. Network radios located on adjacent hilltops near the COC provided additional links needed to establish a three hop network (Figure 25). An additional mobile node then traveled across the network while streaming live video to the COC using the Unreal Media server application to simulate a reasonable network "load." The Ixia Q-Check network benchmarking tool collected network statistics at each of the three hops (figures 25 and 26).

Figure 24 TrellisWare PLI collected during TNT 11–03 test

1. Results from Phase 2

Figures 25 and 26 depict the network performance measures collected in phase 2. General observations from these results show only minor changes in network performance data over time as the reporting node moved from one to three hops from the command node. These changes did not affect the ability to transmit live streaming video as a mobile node moved across this network. The network performance was better at times at two or three hops than it was at the single hop. This observation seems to indicate that additional variables related to *link quality* (e.g., signal to noise ratio, fade margin, etc.) would be better for predicting network performance.

Link quality is a function of received signal strength, which can vary considerably as nodes move throughout the network. Network simulation tools are currently under development at TrellisWare to predict link quality under various environmental situations. A final general observation is that the effect of increasing node density, or increasing the number of nodes that are capable of retransmitting seemed to increase the quality of the network.

a. Throughput

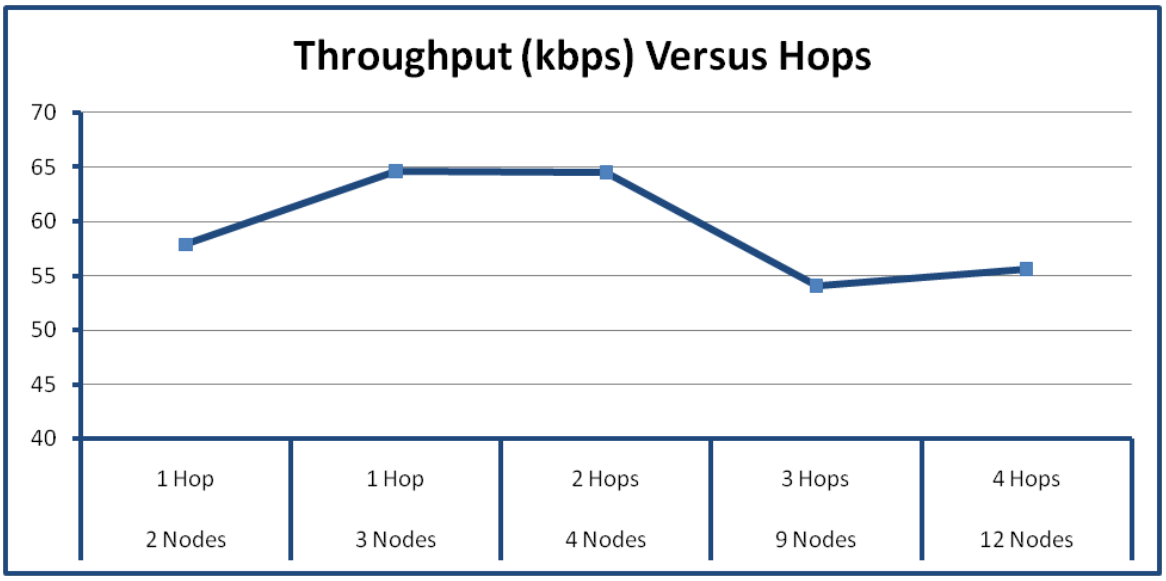


Figure 25 TNT 11–03 throughput statistics

b. Latency

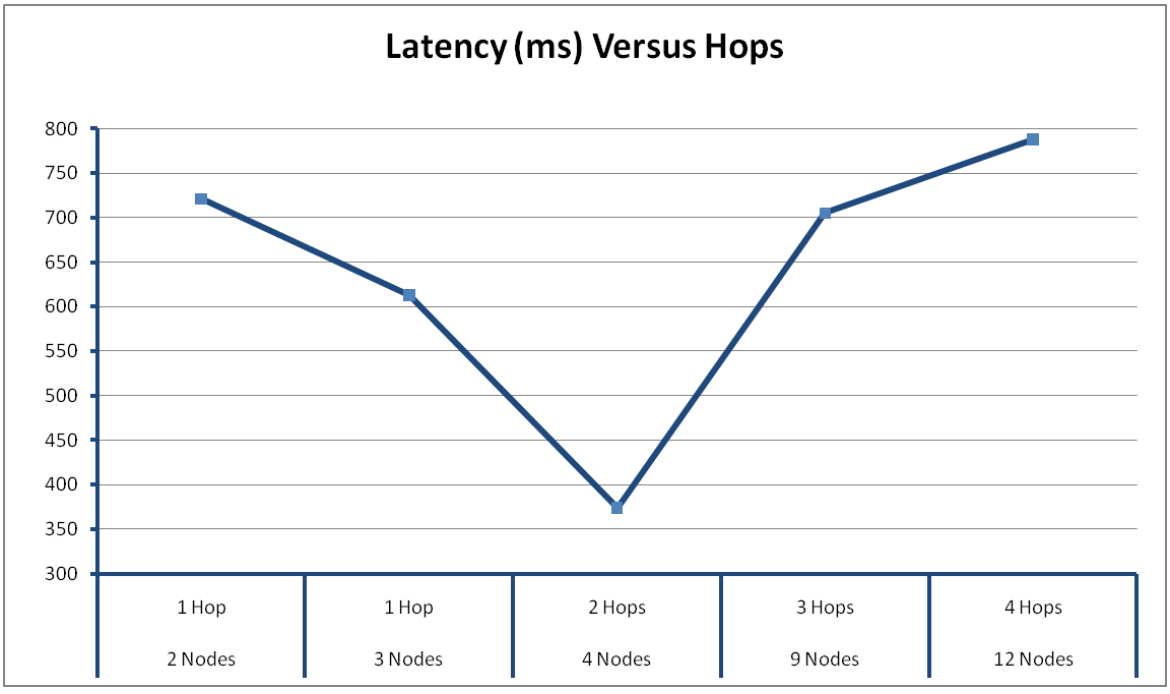


Figure 26 TNT 11–03 latency statistics

C. PHASE 3: MULTICRITERIA VARIABLE ANALYSIS

The purpose of this final phase of the research was to investigate the dependencies that exist between network variables and performance criteria in order to identify patterns that may emerge in the network's behavior over time. Pattern recognition will enable decision support (e.g., CBR) and allow network optimization for changing environmental conditions. The criteria selected for this study increase the value of the tactical mobile adhoc network (MANET) for company level and below communications by increasing benefits provided by the network. These benefits are the result of critical information flows (i.e., voice, data, and position location information) that enhance mission accomplishment through greater adaptability, agility, and/or lethality.

1. Dependent Variables

The dependent variables are the performance criteria selected for this analysis.

1. *Throughput* is a measure of the average number of kilobits per second transmitted across the network. IPerf6 was used to collect throughput measures.

2. *Latency* is a measure of the time delay in the network measured in microseconds. A terminal ping was used to collect latency measures.

3. *Link quality* is a measure of the usability of the communications channels. Link quality measures were collected from the integer values recorded in the TrellisWare USB data utility.

2. Independent Variables

The design variables selected are as follows:

1. The number of potential connections in the mesh network (see Metcalfe's Law in Table 1)
2. Pair wise distance between individual connections
3. Line of sight (LOS) or non-line of sight (NLOS) between each connection.

[6] IPerf is a free network testing utility that can create TCP or UDP data streams and measure the throughput of the network that is carrying these data streams.

3. Constraints

The technical specifications of the TrellisWare CheetahNet 220 define the following constraints (TW-220 User's Guide):

1. The distance between nodes cannot exceed 16 kilometers.
2. The hop count cannot exceed 8
3. Throughput cannot exceed 245 kilobits per second.

4. Data Collection Plan

The TrellisWare USB data collection utility was the primary means of data collection. This utility creates a SQLite database[7] onto the USB drive and records data from each radio into that database. This data was then mined for the criteria identified as relevant to this analysis and was imported into a Microsoft® Excel spreadsheet as an (N+M) * P matrix, where N = number of criteria, M = number of parameters, and P = number of measurements/observations. Throughput and latency data was imported to the spreadsheet from the text file outputs of the IPerf and the terminal ping command line requests. Table 2 shows a sample of the spreadsheet and the data collected.

Time	Lat_{N_1}	$Long_{N_1}$	Lat_{Ni}	$Long_{Ni}$	$D_{N_1 \to N_i}$	LOS	LOS Score	Quality	Throughput	Latency
1	35.71546097	-120.7641188	35.71608734	-120.7654343	0.1376	1	9	1515	56.8	512

Table 2. (N+M) * P matrix used for multicriteria data analysis

The entering assumption was that the overall strength of the tactical mesh network would be greatest when the network topology supported the maximum potential connections between each node. Likewise, the overall strength of the network would be weakest when the topology supported the minimum connections between each node. Figure 27 illustrates a network topology with the most possible connections.

[7] SQLite is an open source software library that implements a structured query language database engine.

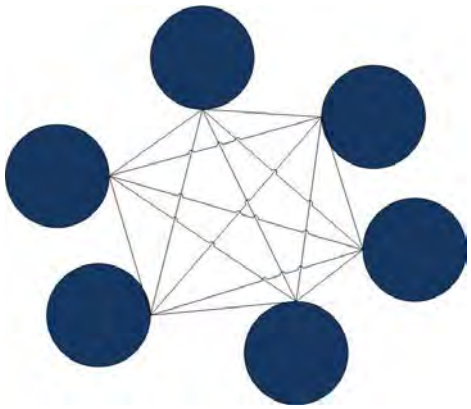


Figure 27 A network topology with maximum connections

Environmental factors, terrain obstacles, and range will cause some connections to be unavailable. That reduces possible connections from the total available. Figure 28 shows a network topology that has the minimum number of possible connections.

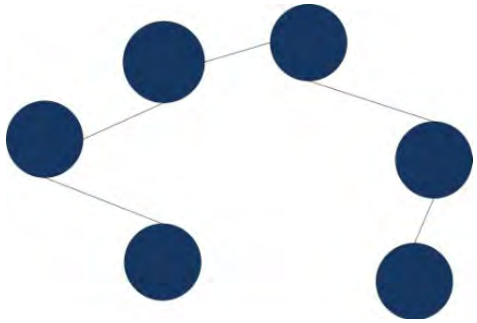


Figure 28 A network topology with the minimum connections

A tactical MANET using TrellisWare CheetahNet radios supported a notional infantry company down to the level of the fire team leader. This MANET included a total of 25 radios deployed throughout an area of operations simulating company, platoon, squad, and fire team leader positions. The network supported voice and data communications during company-level offensive and defensive operations in order to determine how the network topology changed based on the mission and how these topology changes affects network behavior. The three scenario missions conducted at Camp Roberts were: (1) movement to contact, (2) attack, and (3) defensive operations.

a. Scenario 1: Movement to Contact

In this scenario, three platoons simulated a tactical movement from McMillan Airfield towards an enemy forward operating base. The platoons attempted to maintain voice and data communications with each other and the company operations center located at McMillan.

b. Scenario 2: Attack

In this scenario, the company simulated an attack on the forward operating base (FOB). Two platoons were located in supporting positions overlooking the FOB while the third platoon simulated a flanking maneuver to attack the FOB. The platoons attempted to maintain continuous voice and data communications with each other and the company operations center located at McMillan.

c. Scenario 3: Defense

In this scenario, the three platoons simulated setting up defensive positions around the forward operating base (FOB) while maintaining voice and data communications with each other and the company operations center at McMillan Airfield.

5. Results of Phase 3

The data collected was prepared for a multicriteria variable analysis. However, the actual analysis was not performed due the limitations of the USB data collection utility that was used. The table structure (Appendix A) that was designed for this analysis considered the independent and dependent variables shown above in order to estimate how many potential connections are available to a particular node at any given point in time. This design was also selected because experience gained during phases 1 and 2 indicated that the number of available connections determines the topology of the mesh network. These variables include factors (e.g., node locations and distances between nodes) that are also known to affect the received signal strength in any wireless network, not limited to a tactical MANET. Figure 29 shows a representation of all node role names and node locations as they moved throughout the area of operations according

to scenarios 1 through 3. Similar map displays collected from the SA replay tool were used to estimate whether or not a clear line of sight was present between each of the nodes at any given time.

Figure 29 A map displaying all node locations was used for determining LOS

The table shown in Appendix A only provides the network performance from a single node's perspective because the data was only collected for one of these nodes. This was due to the TrellisWare USB dongles only supporting low power (less than 100 milliwatts) USB drives which were not able to be found for purchase at this time. A true representation of the strengths and weaknesses in the entire network topology would require a similar table to be constructed for all of the other nodes in the network. This was the goal, however low power USB drives were not available to support this additional data collection. Another limitation was due to proprietary information that the vendor was unable to disclose regarding how link quality data is calculated. Finally, the tables created by the data collection utility do not contain normalized data which further complicates the accuracy of any analysis based on this data. A better solution for future data collection would be to create a custom application that is able to collect information pertaining to network variables and performance in a similar table that can be time stamped so that the data in these tables can be normalized with the timestamp being used as the primary key for these tables.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMENDATIONS

The broader goal of this thesis has been to investigate the value gained from the tactical MANET through the ability to disseminate valuable information to tactical forces in near real-time leading to a superior information position. One of the specific goals of this research has been to determine critical SNMP MIB variables that must be included in the NMS-TM to incorporate 8th layer capabilities such as adaptive networking based on network and service level constraints monitoring.

The models for determining the value of a network, shown in chapter 1, indicate that the network's value is a function of the number of nodes that connected to the network. However, simply providing warfighters with connectivity does not necessarily increase their capabilities; more likely, it overwhelms our forces with volumes of information that may not be relevant to their immediate situation. To maximize the value of the tactical MANET, the tactical network management system must be capable of maximizing connectivity and delivering the right information in near real-time. The development of an 8th layer protocol for the NMS-TM will move towards accomplishing these goals by allowing each node within the network to become hypernodes that are capable of optimizing themselves for changing environmental conditions and information requirements of the warfighters.

A. CONCLUSIONS

Ultimately, the value of any tactical network is a result of the benefits provided though improved information flows that lead to mission accomplishment. The true value of the tactical MANET is that it can lead to a convergence of the scheme of maneuver and the network topology. This is different than other tactical networks which only support hierarchical topologies. Metcalfe's Law states that a network's value equals the total number of possible connections within the network. Metcalfe's Law can also be applied to estimate the value added by the NMS-TM because the number of connections that each node has will determine where strengths and weaknesses exist within the network topology. The best MANET topology allows each node to make the maximum

number of connections possible. Reality dictates that some nodes within this topology will not be able to maximize their connections, and this will result in these areas becoming weaknesses within the overall topology.

The development of an RF heat map view within the NMS-TM will display these weak areas as places where additional nodes can increase the number of connections to an acceptable level. Multicriteria analysis will determine the relationships between the number of connections, distances, and the performance criteria of the network. A weakness of Metcalfe's Law is that it considers all connections to be of equal value. The incorporation of 8th layer monitoring within the NMS-TM will account for certain connections being more valuable than others. This will allow service level agreement criteria to be an additional factor when deciding which nodes will receive the highest priority used for determining relay node placement.

The current NMS-TM application is a web-based network management system that provides any human operator with a NOC capability in order to view the current network status and manage several of the critical network variables. Incorporating the 8th layer concepts into this NMS-TM will shift this NOC capability from a single human decision maker to the hypernodes as decision makers, and allow the network to adapt itself autonomously to ever changing environmental conditions. The 8th layer transcends any particular wireless networking solution and seeks to create a network-centric enterprise that integrates all command and control and sensor devices into a single infrastructure. The requirements for the 8th layer include *conditions* and *constraints* monitors to enable the sensing, analyzing, and adapting for the hypernodes to maintain service level requirements.

Because the characteristics of certain technologies are better suited for various situations, the tactical network will continue to be a heterogeneous solution (e.g., WiMAX, WLAN, cellular, and MANET). A network management system that is capable of interconnecting these various wireless technologies will enable a larger number of nodes to be connected to a single network, which in itself increases the value of that network. A network management system based on well established standards allows for the integration of new technologies into the enterprise architecture.

SNMP is the most well established network management standard and the incorporation of SNMP agents within the hypernodes can meet many of the requirements of the conditions and constraints monitors. The OID structure within the SNMP MIB allows a single network management system to monitor all devices in the network. Additionally, while web-based monitoring systems could meet these requirements these web-based systems will fail when nodes are not connected to the network. The incorporation of RMON agents within each of the hypernodes allows critical network information to be collected even when these nodes have gone beyond the range of the tactical MANET.

The MIB variables identified for inclusion in the NMS-TM include:

1. Application switching
2. Node physical mobility initiation
3. Receiver Context and Requirements Modeling
4. Sender Dynamic Information Context and Transmission Requirements Modeling
5. Recipient context determination
6. SLA generation
7. SLA negotiation
8. Quality of service (QoS) monitoring and SLA assurance
9. Node status
10. Node location
11. Attached equipment
12. Channel selection
13. Frequencies
14. Error rates
15. Network utilization

Of these variables, node location based on the PLI information such as latitude, longitude, altitude, heading, and speed are the most critical because this determines how many connections are available for each node and the likelihood that any nodes becomes disconnected from the network. This directly impacts network coverage and network availability, and improves network quality when used to determine the locations for additional relay nodes.

B RECOMMENDATIONS FOR FURTHER RESEARCH

While this thesis has focused on the requirements of a common MIB for the NGC2 (TrellisWare surrogate family of radios) and the development of the heat map requirements, the statement of work initially provided from the MCWL included a broader vision. The following requirements from this statement of work (*MCWL-C4 FY11 NPS Tech Investigation SOW*, n.d.) have not been part of this thesis and should be considered for future work beyond the initial development of a prototype heat map layer of the NMS-TM.

1. Explore bandwidth adaptive solutions for hypernodes to adjust their network loads at the application layer.

2. Research how hypernodes can support sensors in how and when to send data based on link health, network health, and bandwidth availability.

3. Examine how hypernodes on-the-move can propagate sensor data in relation to link health and bandwidth availability.

The development of the NMS-TM "heat map" layer in the short term requires a web enabled database application that can collect and store the JSON data streams from the tactical MANET nodes so that this information can be viewed both in real-time and for replay. This data along with the network simulation and analysis tools currently under development at TrellisWare will support the heat map layer's requirements. NPS has already developed a parser application that can be expanded to collect the JSON data streams and store this information for every possible connection within the MANET at any given point in time in a database. Each row in these database tables is time stamped to facilitate replay and analysis. The outputs from the TrellisWare network simulation tool will serve as the inputs of a *mapper* application that will interface with the NMS-TM. This will determine the availability and quality of individual network connections. The heat map layer should include both a live view and a replay view of previously stored cases. That replay serves as the basis of a case library used to forecast network behavior and predict optimal locations for existing or additional nodes based upon what has been "learned" from past experiences.

Once this initial capability exists, follow on development should incorporate sensor devices into this network and determine how the network can be adapted in order to prioritize information flows according to COI's and SLA requirements. The future ISR capable CheetahNet device that is currently under development will support video compression, as well as server and router capabilities. This ISR device could be re-routed to a location based on information presented by the live view in the heat map to provide live streaming video used in order to prosecute Fires in support of troops in contact. A second example might be the employment of passive sensors that can be connected to the tactical MANET for reach back capabilities. These sensors could collect data and store it locally until able to transmit this data across the MANET when a specific COI event is reported. Each of these examples would be supported by the additional routing capabilities provided in the ISR CheetahNet device and the development of an RMON agent for the tactical network.

The development of the RMON agents themselves will enable greater availability and reliability within the NMS-TM. For example, the future developments of the NGC2 to include Iridium capabilities within the TrellisWare devices would be an ideal case for the use these RMON agents. Each node would use the tactical MANET as its primary link. When a node exits the MANET, the RMON agent could use an alert as well as mappings of MAC addresses to network interfaces in order to transmit information over the satellite link until the node rejoins the tactical MANET command network.

The realization of the ultimate goal of achieving a VIRT capability within the tactical network requires the development of devices and information fusion capabilities that do not yet exist. These devices would likely include an applications programming interface similar to modern smart phones that are capable of using a tactical MANET such as that provided by the TrellisWare CheetahNet. These devices could store the local cache of the shared world model so that only updates to that model are sent as required instead of the entire model. This would be a proper common operational picture and would further reduce the number of bits that are transmitted across the network. Finally, the incorporation of the COI monitors based critical information requirements and intelligence data (e.g., most likely enemy course of action, adjacent troops in contact,

environmental threats, etc) into the NMS-TM would allow this to become an even greater capability: it would allow for the smart push of small amounts of information.

The continuation of these efforts will transform tactical networks from their current state (i.e., mostly a broadcast of all information to everyone) to a future state where the network is capable of pushing only the small amount of information that each individual needs in a timely manner and in a clear, understandable format. Steps towards realizing this vision begin with continuing the development of the NMS-TM to incorporate these 8th layer concepts.

APPENDIX. MULTICRITERIA DATA (HYPERLINK)

http://edocs.nps.edu/npspubs/scholarly/theses/2011/September/Multicriteria_Data_PUFF.xls

THIS PAGE INTENTIONLLY BLANK

LIST OF REFERENCES

Aamodt, A. & Plaza E. (1994); Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI Communications*, *7*(1), 39–59. Retrieved from http://josquin.cti.depaul.edu/~rburke/courses/s04/csc594/docs/aamodt-plaza-94.pdf

Advanced Wideband Networking Waveform: An Overview for the AN/PRC-117G (2008 October). Retrieved from Harris Premier Customer Website: http://www.harris.com/premier.html

Alberts, D. S., Garstka, J. J., & Stein, F. P (1999). *Network centric warfare: Developing and leveraging information superiority.* Washington, DC: National Defense University Press.

Bordetsky, A., & Hayes-Roth, R. (2006). *Hypernodes for emerging command and control networks*. Monterey, CA: Naval Postgraduate School Department of Information Sciences.

Bordetsky, A., Bourakov, E., Statnikov R. & Statnikov, S (2005). *Predictive modeling for emerging tactical networks.* Monterey, CA: Naval Postgraduate School Department of Information Sciences.

Bordetsky, A., Dolk, D., & Zolla, G (2004). *Application MIB's for network operations centers collaborative management.* Monterey, CA: Naval Postgraduate School Department of Information Sciences.

Brinton, T (2010, January 8). U.S. Navy to rely on netted Iridium service as gap-filler. Retrieved, from Space News website: http://spacenews.com/military/100108-navy-rely-netted-iridium-service-gap-filler.html

Brinton, T (2010, May 7). U.S. Navy's UHF gap mitigation plan has several elements. Retrieved from Space News website: http://spacenews.com/military/100507-navy-uhf-gap-mitigation-plan.html

Briscoe, B.; Odlyzko, A.; Tilly, B.; "Metcalfe's law is wrong - communications networks increase in value as they add members-but by how much?" *Spectrum, IEEE*, vol.43, no.7, pp. 34– 39, July 2006. doi: 10.1109/MSPEC.2006.1653003

Brueckner, S.A.& Parunak, H.V. Self-organizing MANET management. *Engineering Self-Organising Systems, Lecture Notes in Computer Science*, vol. 2977, pp. 20–35. Berlin / Heidelberg: Springer

Burbank, J. L., Chimento, P. F., Haberman, B. K., & Kasch, W. T (2006). Key Challenges of military tactical networking and the elusive promise of MANET Technology. *IEEE Communications Magazine,* pp. 39–45.

Chadha, R. Cheng, H. Cheng, Y. Chiang, J. Ghetie, A. Levin, G. Tanna, H (2004) Policy-based mobile ad hoc network management, *Policy*, pp.35, Fifth IEEE International Workshop on Policies for Distributed Systems and Networks

Cebrowski, A. K., & Garstka, J. J (1998). Network centric warfare: Its origin and future. *Proceedings of the United States Naval Institute*. Volume 124, No. 1, January 1998 pp. 28–35.

Chen, W., Jain, N., & and Sing, S (1999). ANMP: ad hoc network management protocol. *IEEE journal on Selected Areas in Communications*, 1506–1531.

Conway, James T., "A concept for enhanced company operations," *Marine Gazette*, 2008, *92*(12), pp. 56–61

Coram, R (2002). *Boyd: The fighter pilot who changed the art of war.* Boston: Little, Brown.

DenHartog, M (2010, July 21). The fast track introduction to SNMP alarm monitoring. Retreived from DPS telecom website: http://www.dpstele.com/pdfs/white_papers/snmp_tutorial.pdf

Dixon, J (2010). *Integrating cellular handset capabilities with military wireless Communications.* (M.S. thesis). Naval Postgraduate School, Monterey, CA.

Economides, N (1996). The economics of networks. *International Journal of Industrial Organization*, 673–699. Nicholas Economides, The economics of networks, International Journal of Industrial Organization, Volume 14, Issue 6, October 1996, Pages 673–699, DOI: 10.1016/0167–7187(96)01015–6.

Erwin, S (2010, September 1). Army under pressure to bring broadband to the Battlefield. Retrieved from National Defense Magazine website: http://www.nationaldefensemagazine.org/archive/2010/September/Pages/ArmyUnderPresstoBringBroadbandAccesstotheBattlefied

Erwin, S (2011, February 23). U.S. troops loaded with technology, but can't harness the Power of the network. Retrieved from National Defense Magazine website: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=327

Fuller, R (2008). Performance measurements of network radio systems in harsh Multipath environments (M.S. thesis). Naval Postgraduate School, Monterey, CA.

Hayes-Roth, R (2005). *Model-based Communication Networks and VIRT: Filtering Information by value to improve collaborative decision-making.* Monterey, CA: Naval Postgraduate School.

Hayes-Roth, R (2006). *Two theories of process design for information superiority: Smart Pull vs. smart push.* Monterey, CA: Naval Postgraduate School.

Herberg, U., Clausen, T., & Cole, R (2010). MANET Network Management and Performance Monitoring for NHDP and OLSRv2. Retreived from: http://www.herberg.name/downloads/pubs/CNSM_10.pdf.

Iannotta, B. and Neff, T (2009, August 1). Comm crisis: Delay in U.S. Navy satellite program sparks reviews and contingency planning Retrieved from C4ISR journal website: http://www.c4isrjournal.com/stroy.php?F=4143565

I MEF and HQMC C4 (2010, February 15). *After Action for the I MEF / HQMC C4 Concept of Operations (CONOPS) Validation Exercise for the Harris AN/PRC-117G Falcon III Multiband Manpack Radio*

Institute of Electronics and Electrical Engineers (2004). *IEEE standard for local and metropolitan area networks specific requirements part 16: Air interface for fixed broadband access systems*. Retreived from IEEE website: http://standards.ieee.org/getieee802/download/802.16–2004.pdf

Institute of Electronics and Electrical Engineers (2007). *802.16 IEEE standards for local and metropolitan area networks specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.* Retreived from IEEE website: http://standards.ieee.org/getieee802/download/802.11–2007.pdf

Internet Engineering Task Force (1990). *Request for comment 1157: A simple network management protocol*. Retreived from IETF website: http://datatracker.ietf.org/doc/rfc1157/

Internet Engineering Task Force. (1995). *Request for comment 1757: Remote network monitoring management Information base*. Retreived from IETF website: http://datatracker.ietf.org/doc/rfc1757/

King, Z & Puff, C. (2009). *TNT 10–01 Trellisware CheetahNet Tactical Mesh Network Test Bed & USMC Battalion Communications Demonstration.* Monterey, CA: Naval Postgraduate School.

Kutsor, M. F. (2010). Application of UWB and MIMO wireless to tactical networking in austere environments (M.S. thesis). Naval Postgraduate School, Monterey, CA.

LaGrone, S. (2010, September 20). Briefing: New Horizons. Retreived from Jane's Defense Weekly website: http://search.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2010/jdw44169.htm@current&pageSelected=allJanes&keyword=MCWL TrellisWare&backPath=http://search.janes.com/Search&Prod_Name=JDW&

Lowler, M. (2009, November) Cell phones on the front lines. Retreived from Signal magazine website*:* https://63.65.212.51/signal/articles/anmviewer.asp?a=2101&print=yes

Marine Corps Warfighting Lab. (n.d.). *Naval Post-Graduate School technical investigation in support of the network management system – tactical mobile ad-hoc networking (MANET) (NMS-TM) initiative*

McHuen, H. and Price, R. (2009) Enabling enhanced company operations (ECO): An analysis of tactical communications requirements and solutions for a Marine Corps company and below (M.S. thesis). Naval Postgraduate School, Monterey, CA.

Minoli, D. (2008). *Enterprise Architecture A to Z: frameworks, business process modeling, SOA, and infrastructure technology.* Boca Raton, Florida: Taylor and Francis Group.

New military radio unveiled. (2011, June 13) Retreived from Space Daily website: http://www.spacedaily.com/reports/New_military_radio_unveiled_999.html

Odlyzko, Andrew. (2001, January 3). Content is not king. Retreived from: http://ssrn.com/abstract=235282

Reed, D. P. (1999, January 28). That sneaky exponential-beyond Metcalfe's law to the power of community building. Retrieved from http://reed.com/dpr/locus/Papers/Context%20GFN%20article.doc.

Rohr, K. C. (2006). Fighting through the fog of war. Retrieved from Marine Corps Gazette website: http://archive.mca-marines.org/gazette/06rohr.asp.

Rosenberg, B. (2010 February 25) DoD's reliance on commercial satellites hits new zenith. Retreived from Defense Systems website: http://defensesystems.com/articles/2010/03/11/cover-story-the-satcom-challenge.aspx

Situational Awareness. (2011, February). *Spotlight*, pp. 2–3.

Subramian, M. (2006). *Network management practice and principles.* Boston, Massachusettes: Addison Wesley.

Traylor, P. S. (2009, March 27). Top 10 reasons to invest in new smartphones. Retrieved from TechRepublic website: http://i.techrepublic.com.com/downloads/dl_10_reasons_smartphones.pdf

Tsirlis, Christopher T. (2008). “Communicating the kill.” *Marine Corps Gazette, 92*(9), pp. 25–30

TW-220 User’s Guide (2010, May 17). Retrieved from TrellisWare support website: https://www.TrellisWare.com/support/

United States Marine Corps (2010, February 4). Communications Control (CommCon) Strategy. Washington.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. D.C. Boger
   Naval Postgraduate School
   Monterey, California