



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2005-03

Collaborative applications used in a wireless
environment at sea for use in Coast Guard
Law Enforcement and Homeland Security missions

Klopson, Jadon E.; Burdian, Stephen V.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/2311>

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**COLLABORATIVE APPLICATIONS USED IN A WIRELESS
ENVIRONMENT AT SEA FOR USE IN COAST GUARD LAW
ENFORCEMENT AND HOMELAND SECURITY MISSIONS**

by

Jadon E. Klopson
Stephen V. Burdian

March 2005

Thesis Advisor:
Second Reader:

Alex Bordetsky
Glenn Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE March 2005	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Wireless Applications for Use in Coast Guard Law Enforcement and Homeland Security Missions		5. FUNDING NUMBERS	
6. AUTHOR(S) Jadon E. Klopson, Stephen V. Burdian		8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public use; distribution is unlimited		12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) This thesis analyzes the potential impact of incorporating wireless technologies, specifically an 802.11 mesh layer architecture and 802.16 Orthogonal Frequency Division Multiplexing, in order to effectively and more efficiently transmit data and create a symbiotic operational picture between Coast Guard Cutters, their boarding teams, Coast Guard Operation Centers, and various external agencies. Two distinct collaborative software programs, Groove Virtual Office and the Naval Postgraduate School's Situational Awareness Agent, are utilized over the Tactical Mesh and OFDM network configurations to improve the Common Operating Picture of involved units within a marine environment to evaluate their potential impact for the Coast Guard. This is being done to increase the effectiveness and efficiency of Coast Guard units while they carry out their Law Enforcement and Homeland Security Missions. Through multiple field experiments, including Tactical Network Topology and nuclear component sensing with Lawrence Livermore National Laboratory, we utilize commercial off the shelf (COTS) equipment and software to evaluate their impact on these missions.			
14. SUBJECT TERMS Mesh, Orthogonal Frequency Division Multiplexing (OFDM), Groove Virtual Office, Situational Awareness Multi Agent System, Internet, Nodes, Wireless, IEEE 802.11, IEEE 802.16, Peer to Peer relationships, Collaborative Environment, Common Operating Picture, Tactical Network Topology, Lawrence Livermore National Laboratory, Tactical Satellite, Deepwater		15. NUMBER OF PAGES 109	16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**COLLABORATIVE APPLICATIONS USED IN A WIRELESS ENVIRONMENT
AT SEA FOR USE IN COAST GUARD LAW ENFORCEMENT AND
HOMELAND SECURITY MISSIONS**

Jadon E. Klopson
Lieutenant Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1994

Stephen V. Burdian
Lieutenant, United States Coast Guard
B.S., United States Coast Guard Academy, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
March 2005**

Author: Jadon E. Klopson
Stephen V. Burdian

Approved by: Alex Bordetsky
Thesis Advisor

Glenn Cook
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the potential impact of incorporating wireless technologies, specifically an 802.11 mesh layer architecture and 802.16 Orthogonal Frequency Division Multiplexing, in order to effectively and more efficiently transmit data and create a symbiotic operational picture between Coast Guard Cutters, their boarding teams, Coast Guard Operation Centers, and various external agencies. Two distinct collaborative software programs, Groove Virtual Office and the Naval Postgraduate School's Situational Awareness Agent, are utilized over the Tactical Mesh and OFDM network configurations to improve the Common Operating Picture of involved units within a marine environment to evaluate their potential impact for the Coast Guard. This is being done to increase the effectiveness and efficiency of Coast Guard units while they carry out their Law Enforcement and Homeland Security Missions. Through multiple field experiments, including Tactical Network Topology and nuclear component sensing with Lawrence Livermore National Laboratory, we utilize commercial off the shelf (COTS) equipment and software to evaluate their impact on these missions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	OBJECTIVES	3
C.	RESEARCH QUESTIONS	5
D.	SCOPE	5
E.	METHODOLOGY	5
F.	ORGANIZATION OF THESIS	5
II.	NETWORK CONFIGURATION	7
A.	INTRODUCTION.....	7
	1. Coast Guard Integrated Deepwater System.....	7
B.	BASIC NETWORKING BACKGROUND	9
	1. Computer Networks.....	9
	2. Mesh Networking.....	9
	3. Basic 802.11	9
	4. Basic 802.16	10
	5. Network Comparison.....	11
C.	CONFIGURATION.....	11
	1. 802.16 Hardware	12
	2. Redline Access Node-50e (AN-50)	12
	3. 802.11 Mesh Hardware.....	13
	4. Network Operations Center.....	14
D.	GROOVE WORKSPACE CONFIGURATION – A TECHNIQUE FOR INFORMATION FILTERING.....	14
III.	GROOVE COLLABORATIVE CAPABILITIES BACKGROUND	17
A	INTRODUCTION.....	17
B.	BASIC COLLABORATIVE FEATURES	17
	1. Basic Collaborative Tools.....	17
	2. Peer-to-Peer Architecture	18
	3. Extensibility	18
	4. Workspace	19
	5. Alerts	19
	6. File Sharing.....	20
C.	COMMUNICATION MODE/TEAM FORMATION.....	20
	1. Team Formation.....	20
	2. Presence Awareness	20
D.	NETWORKING CAPABILITIES	21
	1. Requirements.....	21
	2. Connections	21
	3. Bandwidth Optimization	22
E.	INTERFACES AND TERMINALS.....	22
	1. Specifics of Database or Knowledge Base Integration with tools..	22

2.	Bots	22
3.	Software Interface: API	23
4.	User Interface Customization	24
5.	User Terminals	24
a.	<i>Operating System</i>	24
b.	<i>Hardware Requirements</i>	24
c.	<i>Software Requirements</i>	24
d.	<i>Internet Connection</i>	25
F.	TYPES AND LEVELS OF MILITARY/CIVILIAN OPERATIONS	25
1.	Application to Operations	25
IV.	SITUATIONAL AWARENESS (SA) MULTI AGENT SYSTEM OVERVIEW	27
A.	INTRODUCTION.....	27
B.	BASIC COLLABORATIVE FEATURES	28
1.	Instant Messaging	28
2.	Agent Information Sharing.....	29
3.	Alert System	31
4.	Ruler.....	32
5.	Contrast (for dark map background)	33
6.	Drawing.....	33
7.	Show OFDM Sector Feature.....	34
C.	COMMUNICATION MODE	35
1.	Presence Awareness	35
2.	Network Awareness	35
D.	NETWORKING CAPABILITIES	36
1.	System Requirements	36
2.	Bandwidth Requirements.....	37
E.	INTERFACES AND TERMINALS.....	37
1.	User Interface Customization	37
2.	User Terminals.....	37
a.	<i>Operating System and Hardware Requirements</i>	37
b.	<i>Software Requirements</i>	38
c.	<i>Internet Connection</i>	38
F.	SERVER SIDE APPLICATION	38
1.	SA Agent Tracer	38
2.	Agent Administration Facility	40
V.	LAWRENCE LIVERMORE NUCLEAR SENSOR OPERATIONAL SCENARIO	41
A.	NAVAL POSTGRADUATE SCHOOL FIELD EXPERIMENT TNT 05-2	41
B.	DATE	41
C.	LOCATION.....	41
D.	BACKGROUND	41
E.	EXPERIMENT TECHNOLOGIES.....	41
F.	ENVIRONMENTAL VARIABLES.....	42

G.	MEASURES OF PERFORMANCE	42
H.	EXPERIMENT PARTICIPANTS/CAPABILITES/ASSETS	42
	1. Exercise Role Assignments (Exercise Role: Role Player).....	42
	a. <i>Boarding Team</i>	42
	2. Radiological Sensing Equipment.....	43
	a. <i>Rad Pager</i>	43
	b. <i>IdentiFINDER (Radiation Isotopic Identification Device)</i> ...	43
	c. <i>Neutron Pod – Helium-3 Detector</i>	43
	d. <i>Ortec Detective</i>	44
	3. Ships	44
	a. <i>“Coast Guard” Boarding Platform</i>	44
	b. <i>Target Vessel of Interest (TOI)</i>	45
	4. Scenario.....	45
	5. Pre 28 Feb	46
	6. 28 Feb 05	46
	7. Contingency Plans.....	48
VI.	INTEGRATION OF NUCLEAR RADIATION SENSORS.....	49
A.	INTRODUCTION.....	49
B.	RADIOLOGICAL SENSOR TRAINING AND INTEGRATION	50
	1. Training Required to Operate	50
	2. How to Interface with Hardware.....	51
C.	WHY THE SCIENTISTS NEED TO BE OUT ON THE BOARDINGS	51
D.	CHRONOLOGY OF EVENTS	52
E.	RESULTS	58
VII.	PERFORMANCE EVALUATION.....	59
A.	NETWORK PERFORMANCE.....	59
B.	COLLABORATIVE SYSTEM PERFORMANCE.....	63
C.	EVALUATION SUMMARY	65
VIII.	MANAGING CHANGE.....	67
A.	INFORMATION TECHNOLOGY MANAGEMENT STRATEGY	67
B.	ORGANIZATIONAL CULTURE	67
C.	DIAGNOSING TYPE OF CHANGE.....	69
D.	DEVELOPING A CHANGE MANAGEMENT PLAN	70
	1. Establish a Sense of Urgency	70
	2. Forming a Powerful Guiding Coalition	71
	3. Creating a Vision.....	71
	4. Communicating the Vision.....	71
	5. Empowering Others to Act on the Vision.....	71
	6. Planning for and Creating Short Term Wins	72
	7. Consolidating Improvements and Producing Still More Change	72
	8. Institutionalizing New Approaches	72
E.	LEADING CHANGE	72

1.	Dissatisfaction x Model x Process.....	72
2.	Cost of Change	74
F.	MANAGING RESISTANCE.....	75
G.	GIVING PERSONNEL THE KNOWLEDGE TO SUCCEED – ADDING IT PERSONNEL TO SMALL UNITS	76
1.	Sociotechnical Systems Design Theory	76
2.	Information Systems Technician Rated Personnel.....	77
H.	CONCLUSION	78
IX.	CONCLUSIONS AND RECOMMENDATIONS.....	81
A.	CONCLUSIONS	81
1.	Collaborative Software Tools.....	81
2.	802.11 Mesh Network	82
3.	802.16 Wireless Network	82
B.	RECOMMENDATIONS FOR FURTHER RESEARCH	82
1.	Redline AN-50e 802.16 Manpacks.....	82
2.	Adjustable Sector Antennas.....	83
3.	Port Entry Placement of 802.16 Antennas.....	83
	BIBLIOGRAPHY.....	85
	INITIAL DISTRIBUTION LIST	89

LIST OF FIGURES

Figure 1.	Coast Guard Boarding Form.....	3
Figure 2.	Coast Guard Deepwater Overview (From: Hall 2005).....	8
Figure 3.	Network Configuration.....	11
Figure 4.	Redline AN-50.....	12
Figure 5.	Omni directional antenna on Cypress Sea.....	12
Figure 6.	Laptop Computer connected to AN-50.....	13
Figure 7.	Laptops with external antennas and amplifiers.....	13
Figure 8.	GIGA Lab NOC.....	14
Figure 9.	Workspace Graphic User Interface.....	19
Figure 10.	Workspace Awareness.....	21
Figure 11.	SA Agent GUI.....	27
Figure 12.	Instant Messaging.....	29
Figure 13.	Information Sharing Views.....	30
Figure 14.	Video Motion/Acoustic Detection Alert.....	31
Figure 15.	Alert Information.....	32
Figure 16.	Ruler Representation.....	33
Figure 17.	Drawing Function.....	34
Figure 18.	Show OFDM Sector Representation.....	35
Figure 19.	Network Awareness.....	36
Figure 20.	SA Agent Topology.....	37
Figure 21.	Configuration File.....	38
Figure 22.	SA Agent Tracer.....	39
Figure 23.	Agent Admin Facility.....	40
Figure 24.	Rad Pager.....	43
Figure 25.	identiFINDER.....	43
Figure 26.	Ortec Detective.....	44
Figure 27.	“CGC” Cypress Sea.....	44
Figure 28.	USCGC HAWKSBILL (WPB 87312).....	45
Figure 29.	SA Multi Agent System.....	53
Figure 30.	Elint and Imagery Files regarding HAWKSBILL posted.....	53
Figure 31.	Boarding Team Using Ortec Detective.....	54
Figure 32.	“Meshing” between HAWKSBILL and Cypress Sea.....	55
Figure 33.	Radiological Files posted in LLNL Workspace.....	55
Figure 34.	Neutron Pod Raw Data Readout.....	56
Figure 35.	identiFINDER Target Spectrum.....	56
Figure 36.	Neutron Pod Readout.....	57
Figure 37.	Ortec Detective Readout.....	57
Figure 38.	Network Configuration.....	60
Figure 39.	Solarwinds graph of Boarding Team connectivity.....	61
Figure 40.	Solarwinds chart of NOC connectivity.....	62
Figure 41.	Solarwinds chart of Spanagel Tower connectivity.....	62
Figure 42.	Solarwinds Chart of Cypress Sea connectivity.....	63

Figure 43. Real time SA display in NOC, with live video from Cypress Sea64

LIST OF TABLES

Table 1.	802.11 family (After: webopedia.com).....	10
Table 2.	Evaluation Summary.....	65
Table 3.	Change Formula (From: Beer 1988).....	73

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

API – Application Program Interface
CG –Coast Guard
CGC – Coast Guard Cutter
COTS – Commercial Off the Shelf
DoD – Department of Defense
DSL – Digital Subscriber Loop
EAL – Evaluation Assurance Level
ELINT – Electronic Intelligence
FINEX – Finished with Exercise
FIPS – Federal Information Processing Standard
GDK – Groove Development Kit
GPS – Global Positioning System
GUI – Graphical User Interface
ID – Identification
IP – Internet Protocol
ISI – Initial Safety Inspection
IT – Information Technology
Kbps – Kilobits Per Second
LAN – Local Area Network
LLNL – Lawrence Livermore National Lab
M/V – Motor Vessel
Mbps – Megabits Per Second
MS - Microsoft
NOC – Network Operations Center
NPS- Naval Postgraduate School
OFDM – Orthogonal Frequency Division Multiplexing
OPCEN – Operations Center
PTZ – Pan-Tilt-Zoom
SA – Situational Awareness
SMS – Short Messaging System
SNMP – Simple Network Management Protocol
SSTP – Simple Symmetric Transfer Protocol
STAN - Surveillance and Target Acquisition Network
TACSAT – Tactical Satellite
TCP – Transmit Control Protocol
TNT – Tactical Network Topology
TOC – Tactical Operations Center
TOI – Target of Interest
UAV – Unmanned Aerial Vehicle
UDP – User Datagram Protocol
UI – User Interface
USCGC – United States Coast Guard Cutter

USCS – United States Customs Service
VHF – Very High Frequency
WAN – Wide Area Network
WiFi – Wireless Fidelity
WiMAX - Worldwide Interoperability for Microwave Access
XML – Extensible Markup Language

ACKNOWLEDGMENTS

We would like to thank Dr. Alex Bordetsky, Eugene Bourakov, and Glenn Cook for your kindness, dedication and devotion to our educational journey. Your passion, support, and direction have made our whole experience at the Naval Post Graduate School worthwhile. We both feel very fortunate to have been your students.

LCDR Jadon E. Klopson

To my wife Angela, thank you for being such a wonderful and loving wife. You're continued support and sacrifice has made all of my endeavors possible. You are my light, guiding me home from sea.

To my new son Jack, your recent arrival has brought more joy into my life than I thought possible. I can only imagine what great things you will accomplish in this world.

To my thesis partner, shipmate, and friend Stephen, it has been a pleasure knowing and working with you these many years. There's no one I'd rather sail with.

LT Stephen V. Burdian

First, I would like to thank my family for all their support and for believing in and supporting me. I have been truly blessed with remarkable parents, who taught me that there were no limits to what I could achieve, and humbling siblings who miraculously knew exactly what I needed, even if it was a kick in the pants.

To my one true love and fiancé Jo-Ann Feigofsky, having been someone who has always cherished and embraced all that it represents, Life has been so much more rewarding and worth living with you in it. The Love you have given me, the dreams that I have dreamt, and the future that stands before me only represent a fraction of what you have brought into my life. I finally know what Living, Loving, and being whole means. You are my inspiration to do great things in this life. I Love You.

To my buddy Jadon, thank you. I couldn't have done it without you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Since our days as the Revenue Cutter Service, the United States Coast Guard has fulfilled a mandate by our government to conduct inspections of vessels at sea to fill our country's coffers and to protect our citizens from threats, both at home and abroad. Alexander Hamilton stated

“A few armed vessels, judiciously stationed at the entrance of our ports might at small expense be made useful, sentinels of the law.” (Hamilton 1787)

And since 1790 the legacy of the U.S. Coast Guard has been established. Inspect vessels of trade, collect tariffs, save those whose lives are in peril, and protect the very infrastructure of our nation during times of war and peace.

The Coast Guard has played a pivotal role in every armed conflict in our nation's history doing what needed to be done when others were unable to do it. Protecting U.S. interests in Guantanamo Bay Cuba during the Spanish-American war, providing vessel escorts and submarine hunting during both World Wars, intercepting illegal arms shipments from the North Vietnamese during Operation Market Time in Southeast Asia, and protecting harbors in the Gulf during both Gulf wars. And notably, the Coast Guard has been on the front lines of the War on Drugs since officially declared during the Reagan Administration.

The two fundamental reasons that the Coast Guard conducts boardings are to enforce all U.S. Laws applicable in the maritime domain, which relate to maritime safety, Homeland Security, drugs, customs, fisheries and immigration, as well as to educate mariners on the proper and safe practices associated with operating vessels. On an average day, the Coast Guard will

- Save 11 lives
- Assist 136 persons in distress
- Conduct 106 Search and Rescue cases
- Protect \$3.2 million in property
- Enforce 103 security zones
- Interdict and rescue 15 illegal migrants at sea

- Board 3 high interest vessels
- Board 138 vessels of law enforcement interest
- Board 152 large vessels for port safety checks
- Seize 39 pounds of marijuana and 324 pounds of cocaine with a street value of \$10.8 million
- Conduct 296 vessel safety checks and teach boating safety courses to 289 boaters
- Conduct 20 commercial fishing vessel safety exams
- Respond to 20 oil and hazardous chemical spills
- Service 140 aides to navigation
- Monitor the transit of 2,557 commercial ships through U.S. ports
- And investigates 38 vessel casualties involving collisions, allisions, and groundings

(Coast Guard fact file)

The issue that arises is that despite the significant advances in detection and communication technologies over the past two plus decades, the Coast Guard has not successfully integrated them in a way that impacts the efficiency at which the front line sailors are able to do their job in our harbors and on the open seas. The Coast Guard does have Ion Scanners, Optical Bore Scopes, satellite communications links, and other devices that get its missions accomplished, but the Boarding teams have not been given an edge in the information arena. Vessel, cargo, and crew information is still passed word of mouth over VHF radios and continues to be extremely time consuming depending on atmospheric conditions and ranges to ground relays. Boarding forms are exactly what their name states, paper forms filled out in pen and later entered into a Maritime Information System for Law Enforcement (MISLE) database at the rate of approximately one hour per boarding for the boarding officer.

The image shows a complex Coast Guard Boarding Report form. It is divided into several main sections:

- GENERAL INFORMATION:** Includes fields for VESSEL NAME, VESSEL TYPE, VESSEL NUMBER, and BOARDING DATE/TIME.
- CREW LIST:** A table with columns for NAME, RANK, GRADE, POSITION, and various checkboxes for equipment and status.
- OPERATIONAL INFORMATION:** Includes fields for OPERATOR NAME, ADDRESS, CITY, and STATE.
- VALUATION (See Procedures annex 101, para. C):** A table listing various pieces of equipment (e.g., 100. Gasoline, 101. Gasoline, 102. Gasoline) with columns for QUANTITY, UNIT, and COMMENTS.
- REMARKS:** A large text area at the bottom for additional notes.

The form is densely packed with text and checkboxes, designed for thorough data collection during a boarding operation.

Figure 1. Coast Guard Boarding Form

This can be particularly daunting when on average; a boarding officer usually conducts between five and ten boardings in a four day period. Depending on the interest in the boarding by operational commanders, the repetitiveness of transmitting the information generated can at times bog down the whole process. Lastly, there is an inability to get our fleet the best most accurate information in an efficient manor, especially aboard smaller cutters that don't have the ability to receive information via satellite links. This can place the cutter and especially the boarding teams in a stressful situation when delayed information requires a second boarding of a vessel in transit.

B. OBJECTIVES

This research is being conducted to aid in the creation of a more accurate and time sensitive common operating picture between Coast Guard Boarding Teams, which typically consist of 3-7 sailors, and Coast Guard Operations Centers, whose watch standers are responsible for briefing the Chain of Command, during the execution of Law Enforcement and Homeland Security missions. Since the terrorist attack of September 11, 2001 (9/11), there have been significant increases in the efforts to improve our

nation's homeland security posture and focus on improving battle rhythm and real-time maritime domain awareness of the entire chain of command, up and down, during Coast Guard missions. In order to adequately meet this challenge, real-time transmission of data and imagery is needed for further review by superiors up the chain of command and better sharing of data needs to become the norm for our sailors on the front lines.

The ultimate goal is to identify a viable application and network configuration that will suit our organizational needs in the maritime environment for use during Law Enforcement and Homeland Security missions. This includes having the requisite robustness to run necessary applications, to provide adequate distance of signal connectivity over water and to be able to penetrate the hull of a ship while boarding teams are carrying out duties.

In addition to data and imagery transmissions for review, this experiment investigates the detection and transmission of data provided by nuclear radiation detector sensors provided by the Lawrence Livermore National Labs. These sensors are intended to be used by the Coast Guard in Homeland Security and Law Enforcement missions and the experiment will investigate and evaluate the potential for added situational awareness and feasibility of integrating these sensors into our network. The evaluation of these sensors will additionally provide a good test bed for determining the feasibility of sending real-time information to an established shore-based group for review and support of at-sea, underway units engaged in Homeland Security and Law Enforcement.

Additionally, many Coast Guard operating environments do not have technically rated personnel to provide support to an information technology (IT) system. Therefore, one of the requirements of the system will be that basic system operation and maintenance should be relatively simple to carry out for non-technical personnel.

This research will also have the added benefit of reducing the extra efforts of duplicating administrative data entry by boarding teams while conducting Coast Guard missions. This thesis will explore the feasibility of peer-to-peer capable applications, Groove Virtual Office and Situational Awareness (SA) Multi Agent System, transmitting Data via over various hardware/software configurations. If successful, this should allow for real-time data synchronization for all parties involved in mission prosecution while

reducing radio communications and a host of administrative burdens our sailors deal with in the performance of their duties.

C. RESEARCH QUESTIONS

The first question is in regards to what is the appropriate wireless configuration (hardware, software, network mode) and sensor integration aboard Coast Guard Cutters to as to optimize range and ease of use?

The second question involves investigation into various collaborative tools for use within the maritime domain that offer the greatest utility as well as ease of implementation. The two collaborative software suites investigated are the commercially developed Groove Virtual Office and SA Multi Agent System that was developed here at the Naval Postgraduate School (NPS).

D. SCOPE

Test configurations within maritime environment and conclude which one provides the optimal solution. Evaluation of bandwidth, scalability, ease of use and other human factors, and ease of system maintenance will also be conducted.

E. METHODOLOGY

Employ two wireless networks (802.11 and 802.16) and test systems in maritime environment during Tactical Network Topology (TNT) and Lawrence Livermore National Laboratory experiments (LLNL).

F. ORGANIZATION OF THESIS

This thesis is organized as follows. Chapter II describes the network configuration using 802.11 wireless mesh and an 802.16 orthogonal frequency division multiplexing (OFDM) network links. Chapter III follows the introduction and explores the capabilities and limitations of the Groove Virtual Office software package. Chapter IV explores the capabilities of NPS' collaborative Situational Awareness (SA) Multi Agent software. Chapter V describes the operational scenario conducted with Lawrence Livermore National Laboratory. Chapter VI describes the integration of LLNL's radiological sensor package with Groove Virtual Office and SA Agent. Chapter VII describes the operational performance of the various aspects of the network. Chapter VIII describes the organizational changes required to adapt to and take advantage of new

technologies. Chapter IX describes our conclusions and recommendations for further study.

II. NETWORK CONFIGURATION

A. INTRODUCTION

America's Coast Guard, a recent document that seeks to define the current and future status of Coast Guard operating capabilities, states the following about current command and decision making shortfalls: (emphasis added)

The **lack of capability to maintain situational awareness** and effective tactical display of an area of responsibility at the District or Group level, including status of reporting resources and monitoring of actions of Coast Guard resources has continued to create problems for effective force allocation. This, plus a general **lack of interoperable decision support tools, effective situational risk assessment tools, and access to remote mission reporting** information at Groups, has at times resulted in an inability to maintain situational awareness and effective tactical display by units involved in Joint-force operations. Similarly, there is a general **inability to provide real-time tactical information and a situational picture on aircraft, small cutters and boats, and at Small Boat Stations**. The Coast Guard cannot easily share tactical information effectively on a real-time basis among disparate levels of Coast Guard resources and with other agencies and private organizations. Finally, the limited capability to collect data effectively and to evaluate the effectiveness of operations can either result in too many assets being allocated or too few, as well as decisions to call off operations prematurely. (Stubbs 2000)

1. Coast Guard Integrated Deepwater System

The Coast Guard is addressing these shortfalls partially through the major acquisition program, Deepwater (Home Page www.uscg.mil/deepwater). One of the primary goals of Deepwater is to enhance the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) system and create an integrated "system of systems" for all Coast Guard cutter, boats, aircraft, and shore commands.(Anderson 2004) This network-centric concept of operations is intended to be the future of Coast Guard C4ISR.

Integrated Deepwater System



- ***Assets linked together for full interoperability.***
- ***Shoreside fusion centers link with other agencies.***
- ***Improved efficiency of Coast Guard assets by providing near-real-time information and a Common Operating Picture (COP).***

Figure 2. Coast Guard Deepwater Overview (From: Hall 2005)

In order to create the common operating picture between Coast Guard cutters, their boarding teams, and their respective Operations Centers (OPCEN) it is necessary to configure a wireless network- ideally one capable of transmitting ample throughput to support voice, video, and data transmissions.

It is within this greater framework of Deepwater that the concept of operation defined by this thesis has been formulated. This work is intended to be in step with that network-centric operations approach, focused primarily on the communications links between cutters and boats and the link back to shore commands from a near-shore environment.

B. BASIC NETWORKING BACKGROUND

1. Computer Networks

A computer network, in its simplest form, is a system for communication among two or more computers to share information. A wireless network is a computer network that uses radio frequencies instead of wires as the communications medium.

2. Mesh Networking

Wireless Mesh Networking is the implementation of a mesh network over a wireless Local Area Network (LAN). The biggest advantage of mesh networking is that it decentralizes the network infrastructure. In a client-server configuration, every node on the network must access a common server. With a standard wireless access point, every node accessing the system must share the bandwidth provided by that single access point. The great benefit of a mesh topology is that the nodes communicate with each other instead of having to reach all the way to the access point itself. This has several advantages. First, the network can grow exponentially larger than a single access point network since nodes that are too far away from the access point, can still remain connected to the network by “hopping” through nearby peers. Second, nodes are generally not limited by a single point of failure: they may be within range of several other nodes, so if one goes down, they can simply route through one of the other nearby nodes. Third, limited bandwidth improves as more nodes are added since the additional nodes each take on a share of the work, the opposite of a standard single access point network in which each computer added further subdivides the shared bandwidth. (Bach 2004)

There are many various software routing algorithms which can be installed to achieve a successful mesh network. Optimal Link State Routing (OLSR) protocol was used for this experiment primarily because it has been proven successful in prior NPS research and it is available in the GIGA lab.

3. Basic 802.11

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family as illustrated in Table 1 below.

802.11	Applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a	An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
802.11b (also referred to as Wi-Fi)	An extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS.
802.11g	Applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

Table 1. 802.11 family (After: webopedia.com)

802.11 provides moderate throughput at moderate ranges. In this experiment an 802.11b network was used to connect the boarding team to the cutter.

4. Basic 802.16

Commonly referred to as WiMAX, 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. Published on April 8, 2002, the standard defines the use of bandwidth between the licensed 10GHz and 66GHz and between the 2GHz and 11GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles to handle such services as VoIP, IP connectivity and TDM voice and data. (webopedia.com)

In this experiment 802.16 was used to connect the Cypress Sea (cutter) to the shore, and also to connect several of the shore towers back to the Network Operations Center (NOC) at NPS.

5. Network Comparison

802.16/WiMAX products provide a greater range and more throughput than those of the 802.11/WiFi equipment. In simple terms, the difference is evident by the minor variations in the names of each network: 802.11 is considered a Local Area Network (LAN) while 802.16 is a Metropolitan Area Network (MAN), the latter intended to cover a wider area than the former. (Redline White Paper)

C. CONFIGURATION

The test network used for the experimentation in this thesis were created using a combination of 802.16 (OFDM), 802.11 (Mesh), and wired Ethernet as illustrated in the below figure.

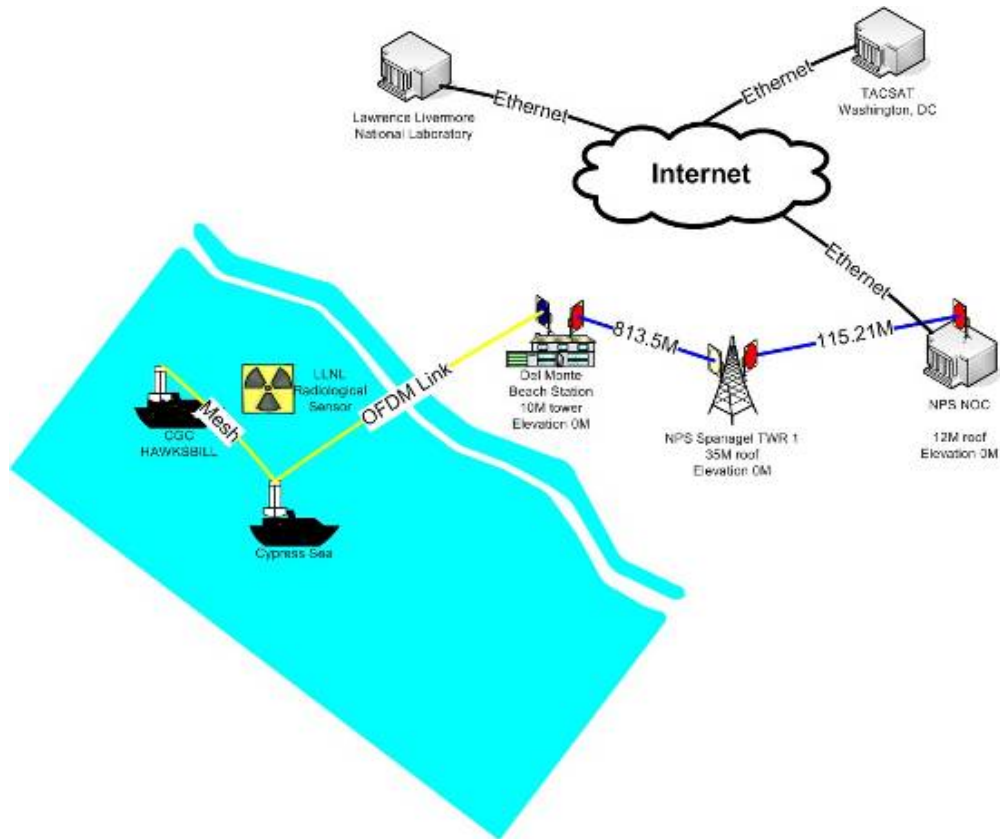


Figure 3. Network Configuration

1. 802.16 Hardware

The successful creation of an 802.16 network requires two Redline Access Node-50 (AN-50) units and two corresponding antennas between each link in the network. Multiple segments in the network require multiple paired AN-50 units.



Figure 4. Redline AN-50

From The Naval Postgraduate School (NPS) Global Information Grid Applications (GIGA) lab network operations center (NOC) to the Spanagel Tower and from the Spanagel Tower to the Beach Tower these links are created with fixed, point to point antennas, wirelessly connecting the Beach Tower to the NOC, through the Spanagel Tower. The connection between the Beach Tower and the Motor Vessel Cypress Sea is established with three 60 degree sector antennas on the Beach Tower and an omni directional antenna on the Cypress Sea



Figure 5. Omni directional antenna on Cypress Sea

2. Redline Access Node-50e (AN-50)

The AN-50 operates in the 5.4 and 5.8 GHz unlicensed bands and is rated at 72 Mbps and supports long-range links exceeding 80 km (50 mi) in clear line of sight (LOS) conditions based on manufacturer claims. (redlinecommunication.com)



Figure 6. Laptop Computer connected to AN-50

3. 802.11 Mesh Hardware

The 802.11 wireless mesh network was created with 2 commercial-off-the-shelf (COTS) Dell Latitude X300 laptop computers. The wireless radios were COTS PCMCIA cards from Proxim, with a nominal output power of 15 dBm. This configuration is rated at providing connectivity for up to 1750 feet. To boost the range of connectivity, power amplifiers and range extending antennas were used. The antennas added 2.5 dBi and increased range slightly. (Proxim.com)



Figure 7. Laptops with external antennas and amplifiers

4. Network Operations Center

The wireless networks are connected back to the NPS NOC via the 802.16 fixed tower links. The NOC provides a network bridge connecting the NPS Intranet and the public internet. At the NOC, the watch officer monitors the terminal and directs information to the appropriate entity.



Figure 8. GIGA Lab NOC

D. GROOVE WORKSPACE CONFIGURATION – A TECHNIQUE FOR INFORMATION FILTERING

While the Groove Collaborative System will be discussed at length in a later chapter, the configuration of the workspaces with respect to information filtering will be addressed here. A question that relates to network-centric operations is the idea of who should get what information and how much information is too much- i.e. how is information filtered. (Hayes-Roth 2004) If every unit was given every bit of information from every other unit there would clearly be an information overload. The process of sorting through the chaff would overburden operators. In this experiment configuration, this was addressed by the creation of several Groove workspaces that were designed to fulfill our needs for information sharing, but to also ensure information sorting occurred at some point in the information loop. The idea of every Coast Guard unit all posting data into one workspace and expecting the experts at the other end to find the information

intended for them is unrealistic. Similarly, if TACSAT posts data in a single workspace that every Coast Guard unit is checking, it may be difficult for the intended unit to find the right files. In an effort to make this experiment as realistic as possible, the NOC was given the task as information filter. This is very much in line with the actual performance of a Coast Guard Operation Center, where overall control of operations is generally maintained. The Operations Center would normally serve as the communications broker, putting the correct people in contact with each other to make sure the right people got the right information.

That same model is used here. The NOC desktop was configured with three separate workspaces: one for the at-sea operation, one for the connection to Lawrence Livermore National Lab, and one for the connection to TACSAT. From a technical standpoint, these entities could have all been in the same workspace, and all exchanged information directly, but that would have been somewhat unrealistic. With this configuration, the NOC maintains a semblance of “Net Control” and is then capable of inviting any entities into any workspace as necessary to share information and situational awareness, but only after making the conscientious decision to do so.

THIS PAGE INTENTIONALLY LEFT BLANK

III. GROOVE COLLABORATIVE CAPABILITIES BACKGROUND

A INTRODUCTION

Groove Virtual Office is a client application that functions as a peer to peer collaborative tool. Unlike most other collaborative tools, Groove can be used offline utilizing the coordination of a relay server that synchronizes all systems assigned to a workspace. Groove allows individual users to create shared workspaces on their desktop and collaborate across firewalls without the need for seeking IT expertise elsewhere, it only requires the basic computer user knowledge to install and get started.

Groove Virtual Office V3.0 is the most recent version on the market. It has several improvements from its predecessor (V2.5). V3.0 is 3-5 times faster, it has a launch-bar service and simplified workspace creation capabilities. It has improved folder synchronization, a workspace explorer, improved alerts for users and workspaces, enhanced forms and file functionality, team direction project tools and new antivirus protection. V3.0 also has simplified account creation and activation, improved its preference toolbar, and enhanced its instant messaging, printing and search functions (Groove Networks 2004).

B. BASIC COLLABORATIVE FEATURES

1. Basic Collaborative Tools

Groove Virtual Office V3.0 has thirteen built in collaborative tools aimed at increasing individual and group productivity. These collaborative tools are similar to those you would find in enterprise web portals such as PlumTree and Microsoft (MS) Sharepoint, but that's it. Groove offers you much more.

- Calendar – allows you to mark important dates and build collaborative schedules with workspace members
- Contact Manager – allows you to maintain a shared list of contacts
- Discussion – allows for detailed conversations with workspace members
- Document Review – allows for document review with workspace members
- Files – allows for the storage, organization, and sharing of files
- Meetings – allows agenda and action assignment and the recording of minutes

- Notepad – allows for writing and editing of notes to workspace
- Project Manager – allows for tracking and organizing projects
- Sketchpad – allows for creation of drawings on a sketchpad
- Forms – allows for the creation of customized applications for collecting and viewing data
- Web Links – stores and organizes your favorite Web URLs
- Pictures – allows for the display and sharing of graphic images and photos
- Chat – allows for group or individual text chatting

2. Peer-to-Peer Architecture

This is one of the key features of Groove Virtual Office. It is able to use this architecture to overcome some of the limitations and vulnerabilities associated with web-based and server-client based architectures e.g. always on network connection and availability. The availability factor is especially critical since you do not want the entire infrastructure to be brought down by several failed nodes. It is well in position to take advantage of the evolving ad-hoc networking technologies like the Naval Postgraduate School's (NPS) Tactical Mesh Network, and provide a seamless collaborative environment.

Groove Virtual Office provides facility to allow any user to access his or her workspace from any computer which Groove is installed, provided the account has been configured for such a mode. Considering that each workspace content is not stored centrally in servers, but on the individual machines allows for added assurance that you can get to your files or participate in workspace projects from anywhere, not just at a single point of failure.

3. Extensibility

Like most web portals, the Groove Virtual Office functions can be extended by integrating customized or a third party collaborative tool. It comes with a default interface with Microsoft Outlook and Lotus Notes for exchanging email and calendar information.

The Groove Development Kit (GDK) provides the toolkit and utilities to build customized applications. These include Groove Form, Groove Workspace Application Program Interface (API), and Groove Web Services API.

Groove Virtual Office API provides the Groove object model within the .Net Framework. This allows developers to build more advanced application programming logic and alternative form design within the individual Groove Workspaces.

Groove Web Services is intended for a developer building standalone application (outside the Groove Workspace) which requires access to individual Groove services or data.

4. Workspace

Groove Virtual Office's features are broadly categorized into in-workspace and above-workspace. File sharing, Discussion Board, and Calendar are examples of in-space features, while Instant Messaging and Chat are examples of above-workspace. The difference is that in-workspace features can only be used for collaboration with members of that specific workspace and above-workspace features are not limited in that way.

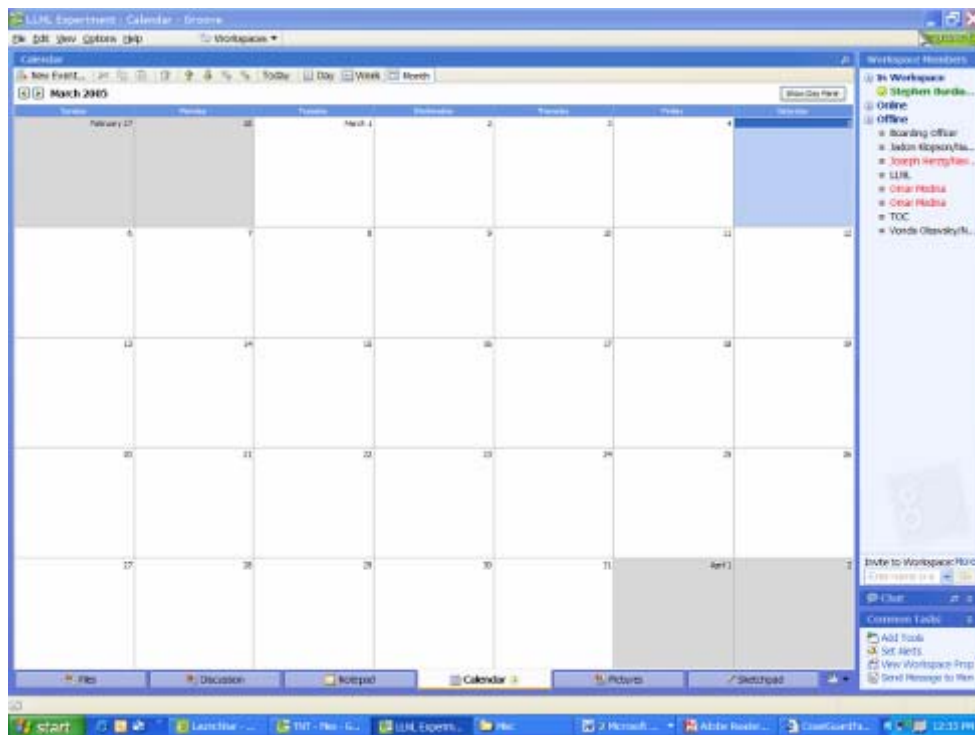


Figure 9. Workspace Graphic User Interface

5. Alerts

This is a very effective tool for managing an endless stream of activities and events, especially if you are constantly changing the workspace you are in. Groove

provides fine granularity in configuring what's, when's, and how's, allowing you to customize the alerts to your needs.

6. File Sharing

File sharing can be done through either adding a file to the “Files” tool within a workspace, or designating a Windows file folder as the File-Sharing workspace (as apposed to a standard workspace). The Groove file sharing features are characterized by distributed storage and automatic synchronization. You can also initiate a joint editing session of these files if more than one person is working them.

C. COMMUNICATION MODE/TEAM FORMATION

1. Team Formation

This is one of the very attractive features of Groove Virtual Office. Forming a team is seamlessly accomplished in two different ways, sending an email invitation or literally send them a file invitation on any type of storage media. This negates the need to create additional accounts, opening a special port on your firewall, or setting up additional hardware, i.e. a server.

In lieu of central management account creation where identity can be verified physically, the issue of authenticity of member's identity comes into question. Groove Virtual Office overcomes this issue by associating a unique digital fingerprint to each Groove Account. One can verify another's identity manually by comparing the digital fingerprint through another means outside Groove.

2. Presence Awareness

This feature allows you to know if another member of your workspace is either online and logged into Groove (Figure 10), or what subdivision of the workspace they are currently working in, i.e. files and calendar. Groove also allows you to block other members from “seeing” you in the workspace if you do not want them to.

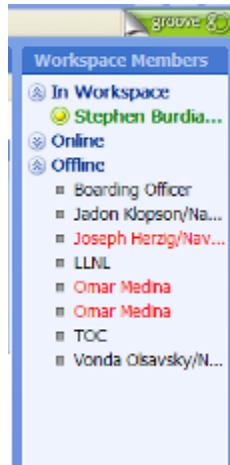


Figure 10. Workspace Awareness

D. NETWORKING CAPABILITIES

1. Requirements

Groove Virtual Office can connect via any number of mediums as long as they satisfy the minimum required connection of 56kbps. To optimize Groove V3.0, a Local Area Network (LAN), Digital Subscriber Loop (DSL), or cable modem is required. Groove works over wide area (wireless) networks (WAN) like NPS' Tactical Mesh and Orthogonal Frequency Division Multiplexing (OFDM) networks.

2. Connections

Groove Virtual Office utilizes either a hosted relay server or can be hosted by Groove Networks to relay and fan out. In the peer-to-peer configuration, computers talk to each other directly. When one member of a workspace goes offline, the relay servers queue and forward any files, messages, etc that has not been synchronized until the member returns.

On a LAN, Groove clients utilize the transmission of User Datagram Protocol (UDP) packets to make their presence known on the LAN. This is an automatic function of Groove that the user can manipulate, by changing the frequency with which the packets are broadcast. On a WAN, the groove clients use a "subscribe and publish" model. Users can detect the presence of someone else only if they previously exchanged contact information. A Groove client will send a user's Internet Protocol (IP) address and information to the relay server and other groove clients will poll the server to see who is online.

3. Bandwidth Optimization

All user activities on Groove utilize a binary differential protocol to exchange information. The Groove client determines the delta, or changes, between two files and then compresses this data to send over the network. This optimizes the bandwidth required to update the files. The “delta” files are compressed and encrypted using Extensible Markup Language (XML) structured commands that are sent to all users in the workspace.

The fan out aspect of Groove minimizes bandwidth consumption needed to transfer data. When communicating in a peer-to-peer collaboration, if a user wants to send information to other users, the Groove client determines the bandwidth use required and decided whether or not to send each user the data, or if more is optimal, to send the data once to the relay server and has the server fan out the data from there.

Groove uses a proprietary protocol, Simple Symmetric Transfer Protocol (SSTP), to communicate. This protocol is able to handle rich-context and peer-to-peer interaction, such as compression, routing, security, real-time communication and synchronous use.

In Groove Virtual Office, firewalls are transparent to the client. The Groove client determines which open ports would best suit its need for communication and utilizes these ports for communication protocol. This nuance of Groove makes it ideal for collaborating across different network and business environments.

E. INTERFACES AND TERMINALS

1. Specifics of Database or Knowledge Base Integration with tools

Automated agents are allowed access to the Groove network. They appear in the shared spaces and can access and remove data from that workspace just like their human counterparts. Automated agents in Groove are referred to as “Bots” and they can perform a discovery and connection service.

2. Bots

While the Groove Enterprise Integration Server provides a generic means to integrate Groove with external systems, it is the responsibility of a bot, to act as a proxy on behalf of a member(s) of a shared space to provide the logic for communication with an external system. For example, a FAQ bot might respond to an inquiry from a member

of a shared space by fetching from an external system the appropriate answer to a question. A bot is usually a piece of C++ or Visual Basic code, or JavaScript that operates on a tool in a Groove shared space. For example, Groove provides a bot that runs an information retrieval service, responding to questions issued in a Groove shared space via a Discussion tool, fetching an answer from an external access database, and replying to the same shared space.

Enterprise Integration Server Console: The Groove Enterprise Integration Server console is an administrative interface installed on the Enterprise Integration Server, for easily and seamlessly configuring the server's policies, services, and bots.

Bot Development: Anyone can build a bot using the bot development framework provided in the Groove Enterprise Integration Server Development Kit, and developers in an enterprise can create bots to perform other tasks to respond to specific business needs. The Enterprise Integration Server requires a license, which may be purchased directly from Groove Networks, Inc. **Bot Management:** The bot administrator configures the run-time environment for a bot, controlling functionality, e.g., the lifetime of the bot. In addition to this run-time environment configuration, each bot can offer a custom, configurable user interface to allow the administrator to perform bot-specific behavior. In situations where a bot connects to a centralized database, its configurable user interface (UI) would allow the administrator to set access control for users that will be interacting with the database (Groove Networks 2004).

3. Software Interface: API

The Groove Development Kit v3.0 gives developers three options for creating and deploying Groove-powered solutions:

Forms-based Groove Workspace Explorer tool solutions - Business process solutions (e.g. incident tracking, customer tracking) created and deployed using the Forms tool that run within Groove Workspace Explorer and may operate alongside other Groove tools;

Custom Groove Workspace Explorer tool solutions - Custom tools developed using the Groove Toolkit for Visual Studio .NET that run within Groove Workspace Explorer and may operate alongside other Groove tools

Web Services Solutions - Solutions deployed as discrete applications that consume some or all Groove virtual office capabilities via a comprehensive Web services API (Groove Networks 2004).

4. User Interface Customization

The enhancements to the familiar user interface customization features that Groove version 2.5 had are as follows: The Forms tool user interface has been overhauled to enhance the comfort level for both users and designers, as well as to enhance behavioral consistency with other Groove tools. Hidden views offer view creation, supporting the new lookup capabilities, but that the designer does not want to appear in the actual user interface.

5. User Terminals

Groove can be used on any terminal (wireless included) as long as it fulfills the following system, hardware, software, and internet connection requirements (Groove Networks 2004):

a. Operating System

Microsoft Windows NT® 4.0 with Service Pack 5 or later

Microsoft Windows 2000

Microsoft Windows XP

File-sharing workspaces (a new type of Groove workspace that works directly with folders in your Windows file system) are not supported on Windows NT4.0.

b. Hardware Requirements

Intel® Pentium® II processor (or equivalent), 400 MHz or higher · 256 MB RAM required, 512 MB RAM recommended.

100 MB available hard disk storage (with 60 MB additional space required for your data)

Display resolution 800 x 600, 16 bit, 65,536 colors

Sound card, speakers, and microphone required to use voice features

c. Software Requirements

Microsoft Internet Explorer 6.0 or later.

Lotus Notes® 5.0 or later required using Groove/Lotus Notes integration features.

To use Groove/Outlook integration features, one of the following versions of Outlook is required: Outlook 2000, Outlook 2002, Outlook 2003

To use Groove/Office integration features, one of the following versions of Office is required: Office 2000, Office XP, Office 2003

d. Internet Connection

56 kbps dialup connection minimum.

LAN with Internet access, DSL, or cable modem preferred

F. TYPES AND LEVELS OF MILITARY/CIVILIAN OPERATIONS

1. Application to Operations

Groove applies itself to Battlefield and Emergency management, and Humanitarian operations flawlessly. The peer to peer relationships that it uses allows its members to participate in information sharing and collaboration regardless of their individual locations. A great example of this occurred during the New Year celebrations across the country this year. While thousands enjoyed the festivities in Times Square and at the Tournament of the Roses Parade, law enforcement, intelligence and new homeland security agents were able to utilize Groove's capabilities to efficiently and effectively share information real time. If an officer in Texas took a picture of a suspect, it could be shared directly with the other agency officials. In the military world, groove is compatible with wireless enabled notebooks. The data that is transmitted using Groove is automatically encrypted whether it's on the user's hard drive or traveling over the network. Groove's 192-bit encryption technology has also earned a Federal Information Processing Standard (FIPS) 140-2 and Common Criteria Evaluation Assurance Level (EAL) 2+ certification, which ensures sufficient security, is provided. This and the fact that the workspaces Groove uses are invitation only. The workspaces are fully third party PKI enabled, which can require that a user authenticate themselves via their Department of Defense (DoD) Common Access Cards. Groove's non-repudiation feature digitally signs instant messages and shared space messages and verifies data integrity.

The Department of Homeland Security has been using Groove to ensure situational awareness throughout the country. They used Groove to coordinate security during the Democratic convention in Boston and the Republican National Convention in New York. The Pentagon, Coalition members, and civilian agencies are currently utilizing Groove in Iraq and Afghanistan to coordinate security and the reconstruction of those two nations. In fact, as of the 29th of June 2004, roughly 40 percent of Groove's sales have been to the government. (Groove Networks 2004)

IV. SITUATIONAL AWARENESS (SA) MULTI AGENT SYSTEM OVERVIEW

A. INTRODUCTION

SA Multi Agent System is a program that was developed by Dr. Alex Bordetsky and Eugene Bourakov at the Naval Postgraduate School (NPS) (Bordetsky 2002) in July 2002 for the purpose of increasing battlespace awareness of “war fighters” and combatant commanders during Surveillance and Target Acquisition Network (STAN) and Tactical Network Topology (TNT) experiments that are run each quarter at the Naval Postgraduate School. The common operating picture is based on maps or charts of the area of operations populated with agents that are represented by various icons like a person, truck, unmanned aerial vehicle (UAV), sensor etc. (Figure 11). The entities are located on the chart via latitude and longitude positions that can be entered manually, by clicking and dragging your symbol to your current position, or by a Global Positioning System (GPS) device. Since Situational Awareness (SA) Multi Agent System did not have any user guide information available yet, this chapter is written to provide an overview of the program and to act as a user guide for those using this software program in the future.

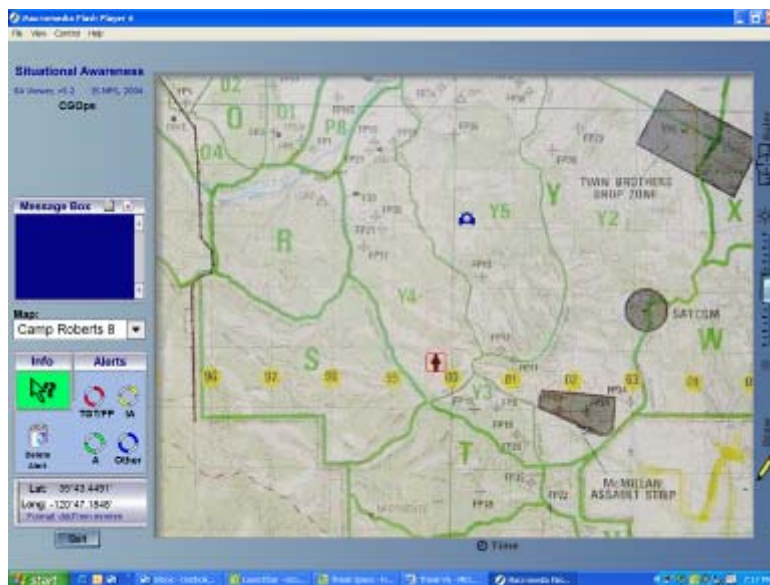


Figure 11. SA Agent GUI

SA Multi Agent System's graphic user interface (GUI) provides the user with a shared view of the common operating picture of the battlefield space. The basic functionality of any shared workspace is that it must show all the changes to any agent or system status within that workspace. SA Multi Agent System was designed to provide the war fighters, tactical operations center (TOC), and network operations center (NOC) with these real time views of the relevant operational picture.

What makes SA Multi Agent System flexible and easy for the user to use is that it was built utilizing Macromedia movie techniques. Macromedia movie provides access to "shared object" features that can be viewed on each users screen and can be continuously updated as the system's status changes. Each shared object has a set of properties that allows for modification of its view and updated status. For example, when user moves an icon on the map, it immediately updates on all screens, if alerts are generated, voice notification or visual representations in the form of blinking symbols are shown. The operational maps that are available are customizable to any map that pertains to a specific operation. These maps act as the background that the agents are plotted upon.

SA Multi Agent System is a client-server application. The combination of this traditional client-server application and Macromedia's shared object technique creates a new powerful approach to operational view sharing and provides the user with a rich and meaningful user interface. SA Multi Agent System is a database driven application which stores any changes in the operational picture in database tables so that it can provide updated operational pictures, calculate network performance variables, and allow future analysis. All events are relayed from the agent to the server where it is stored in these database tables and then the server synchronizes this data with all of the other agents. As a result, all of the agents have a real time view of the operational picture. The SA Multi Agent System also has a feature that can be made available by the administrator that allows a user to replay of any part of scenarios at any time.

B. BASIC COLLABORATIVE FEATURES

1. Instant Messaging

Instant messaging allows send a text message to another agent in the field. In order to send a message, user needs to open the message window by clicking on the icon

resembling a piece of paper on the top right hand side of the Message Box. This opens up a text window where the user can type a message. Once the message is composed, the “envelope” icon should be dragged and dropped on the agent’s icon you are contacting. If successful, there will be a voice notification and flashing line established between the user’s agent icon and the agent the message was sent to (Figure 12).

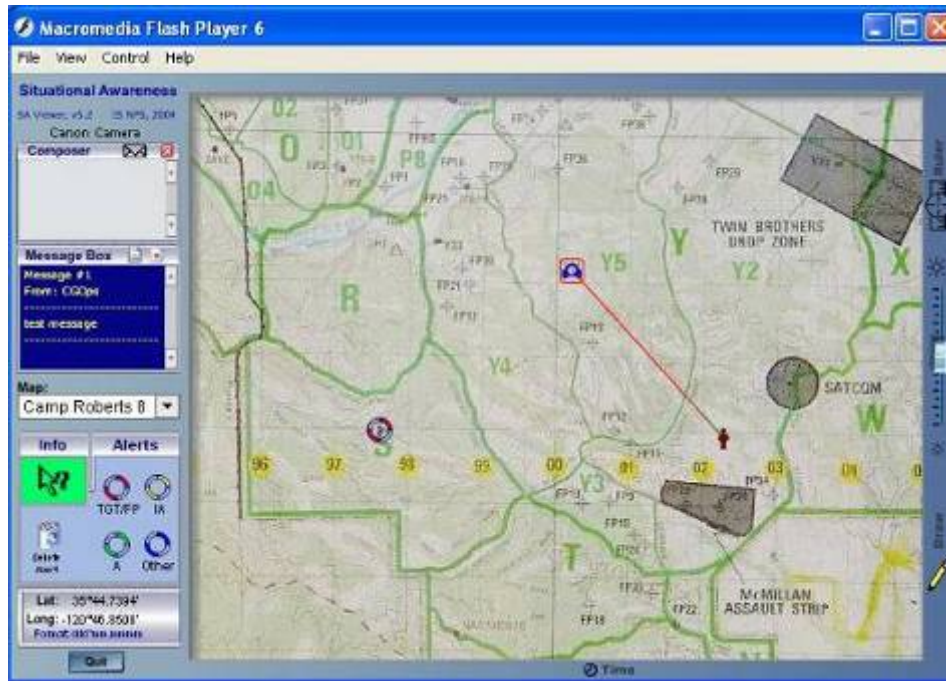


Figure 12. Instant Messaging

2. Agent Information Sharing

Information sharing is completed several different ways; by using the Info arrow button, instant messaging, through video motion and acoustic detection, using the agent’s and an alert’s information property screen etc. The Info arrow button can be clicked and dragged to the SA Agent you are interested in to attain general information about it. When the Info arrow button is dragged and dropped on the agent or alert icon, a property screen appears. The property screen contains three buttons which allow you to find out the status of the network connection, general information about the agent, and to hear and see video if the agent has that capability (Figure 13). The Info arrow button can also provide helpful tips about the basic elements of the SA screen when the user drags it over the screen element. The general information screen provides basic information about the agent and can only be modified by the system administrator or the agent itself. In regards

to the network connection, there is a visual representation of the response time, throughput in and out, and the packet sizes being transmitted from the agent. The video screen allows you to hear and see anything that is being transmitted from or to the selected agent. Video motion and acoustic event detection can be toggled to an enabled or disabled mode by clicking on the appropriate slider box. When an agent's video sensor is triggered, all the agents receive an audible alert "video motion detected" followed by the transmission of video. Two sensitivity sliders allow you to adjust the level of motion and acoustic detection to trigger an event (Figure 14). Adjustments to the quality of the audio and video can be made by adjusting the quality control button on the right hand side of agent's properties screen. The transmission rates range from 3Kbps up to 1Mbps. The quality of the video is controlled by the Macromedia application which is based on the current network connection quality. If you have a poor network connection video quality suffers and decreases the video frame rate down to 1 frame per second (fps). If you have a high quality network connection video quality increases up to a maximum rate of 15fps.

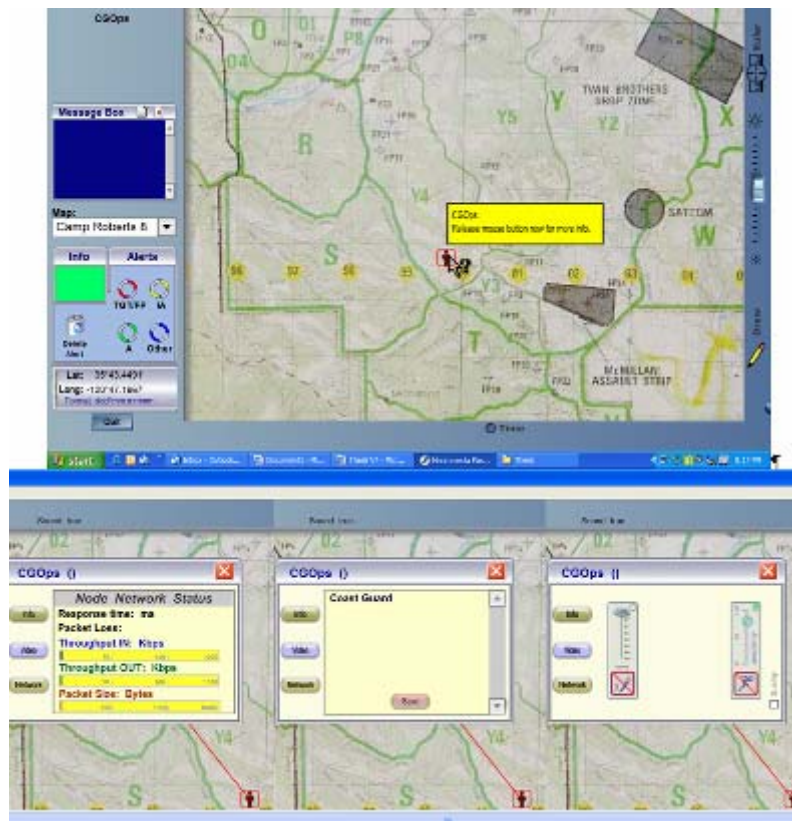


Figure 13. Information Sharing Views



Figure 14. Video Motion/Acoustic Detection Alert

3. Alert System

Alerts can be generated by any of the active agents. They are activated by clicking and dragging the appropriate alert to the relevant position. The originator of the alert will see a dynamic/spinning symbol that can be edit to include more information about what the agent is alerting others to. If you did not generate the alert, you will see a static symbol and can drag the Info button to the alert to receive amplifying information (Figure 15).

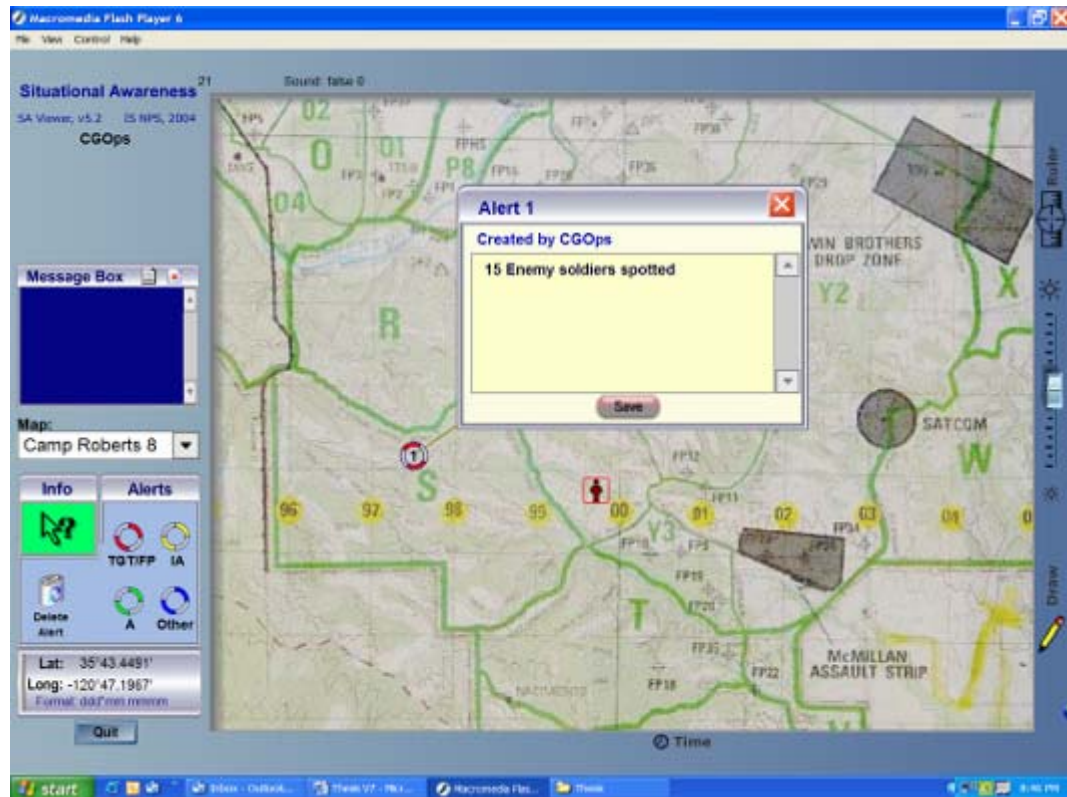


Figure 15. Alert Information

4. Ruler

The Ruler function allows the user to make a quick calculation of distance between agents, alerts or map points. To use this tool, click and drag the ruler from the right hand side of the GUI and place it on starting position of measurement. Extend the resulting line to the end position and the resulting distance will be shown (Figure 16). Distances are measured in kilometers and will be displayed in a yellow box. Click on the ruler symbol again to stop using the ruler.

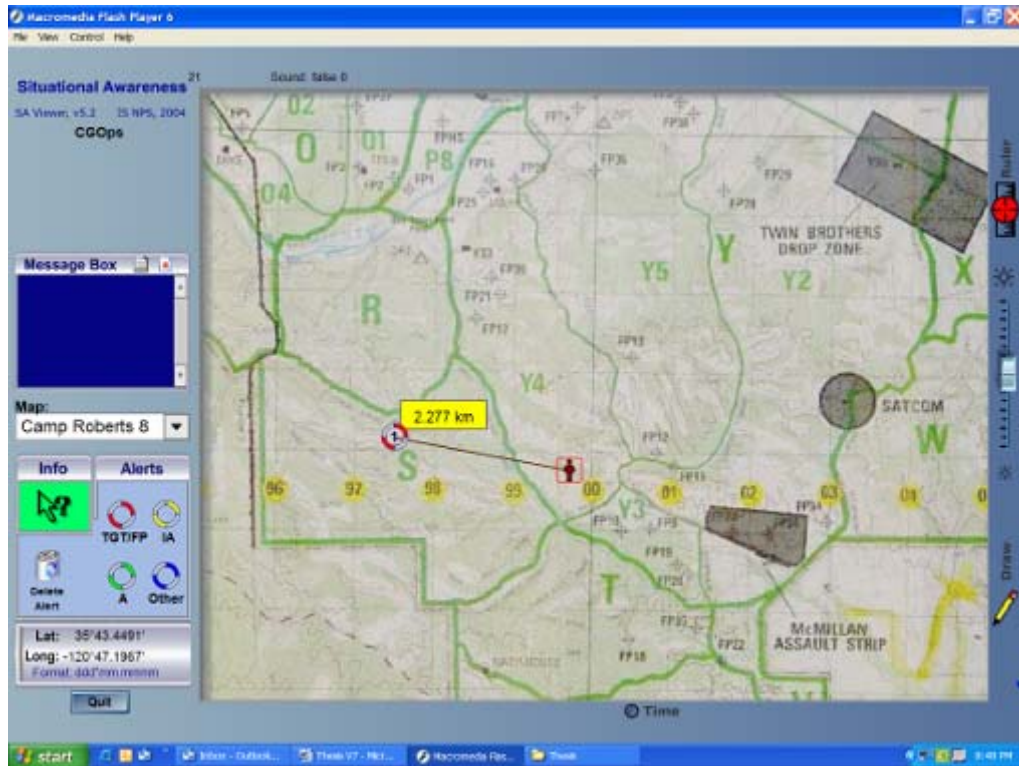


Figure 16. Ruler Representation

5. Contrast (for dark map background)

The contrast slider is located on the right hand side of the SA GUI. This function can be used when the map background you are using is really dark or cluttered. Adjust this button up or down to make the agents more defined on the screen (Figure 17).

6. Drawing

The drawing tool allows the user to place sketches on the maps similarly to sketchpad. To use this function, click on the pencil icon located on the right side of the GUI and then click on the area you would like to start drawing. Click and drag the icon to make continuous lines with you mouse (Figure 17). To remove the drawing, click on the X'd out pencil icon.

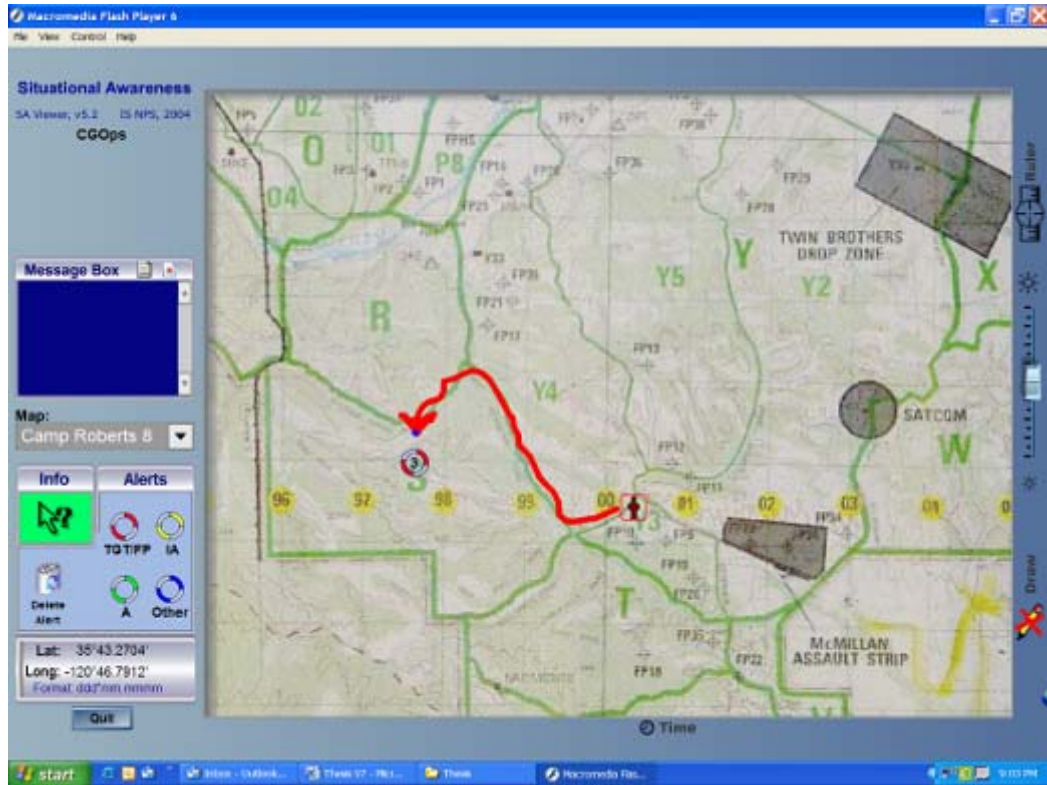


Figure 17. Drawing Function

7. Show OFDM Sector Feature

The OFDM 60 Degree Sector Antenna Switch designed and developed based on Redline's AN-50 802.16 radio set to support high speed data link for TNT experimentation within Monterey Bay. There are three AN-50 radios connected to three 60 degree sector antennas for a combined 180 degrees of coverage within the bay. Each of these antennas transmit and receive on the same frequency, which could have resulted in significant interference so Eugene Bourakov developed the orthogonal frequency division multiplexing (OFDM) Sector Antenna Switch software that allows each AN-50 to monitor its link status and maintain connectivity when a signal is established within its 60 degrees of coverage. If you are using either Monterey maps in SA Agent, you can check the "show OFDM Sector" box and a visual representation of the active sector will appear on the screen (Figure 18).

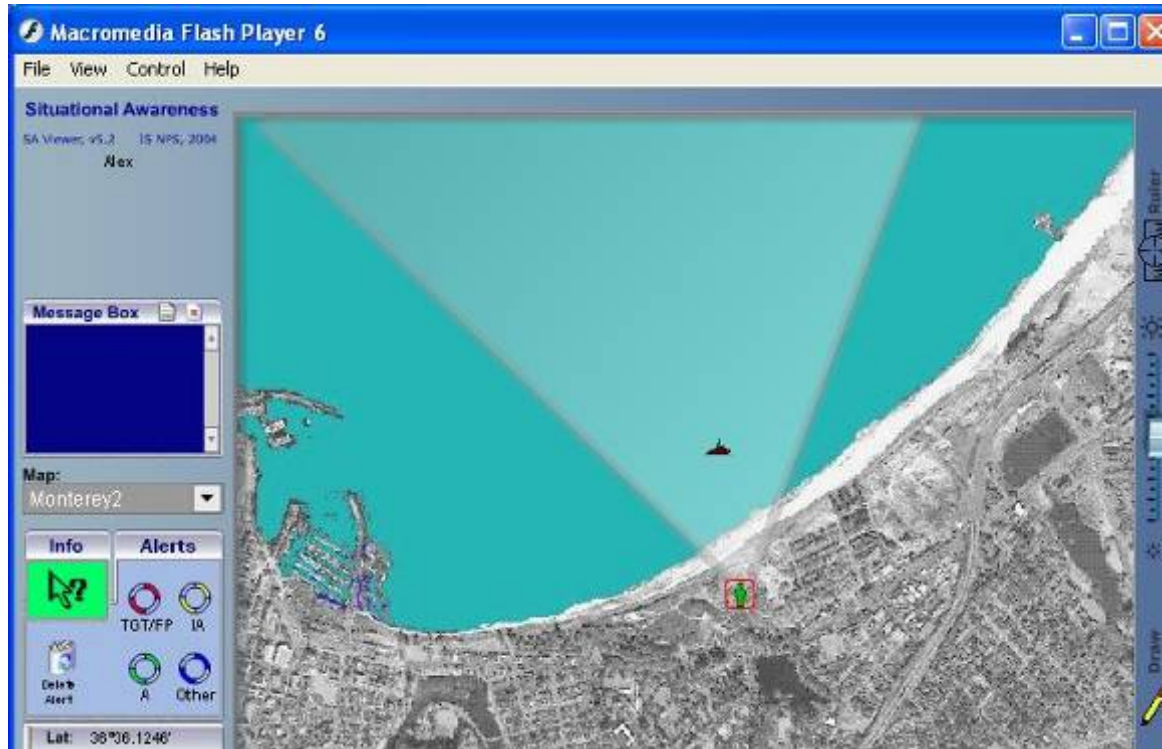


Figure 18. Show OFDM Sector Representation

C. COMMUNICATION MODE

1. Presence Awareness

Presence awareness is established once you establish a network connection to the SA server at NPS. The background color of Info arrow icon should change from red to green and confirms that your connection is established and active. If the background remains or turns red this means that a connection with the SA server has not been established or was lost. Depending on the map you are displaying and their location, other agent's icons will appear on your screen. Your agent will be differentiated from the others by being enclosed in a red square (Figure 19).

2. Network Awareness

Network awareness attained by the collaboration between Simple Network Management Protocol (SNMP) agents, which control each node's networking elements, and SA agents. The SNMP agent checks the network status of the node and collects the data. Instead of talking directly with the node's SA Agent, this information is collected by the SNMP management agent located on the SA server at NPS. This information is then redistributed back to the originating node and all the other active nodes in the SA

Multi Agent System. This information can be displayed by dragging the green information button to any SA agent, dropping it on the agent, and clicking on the Network button (Figure 19).

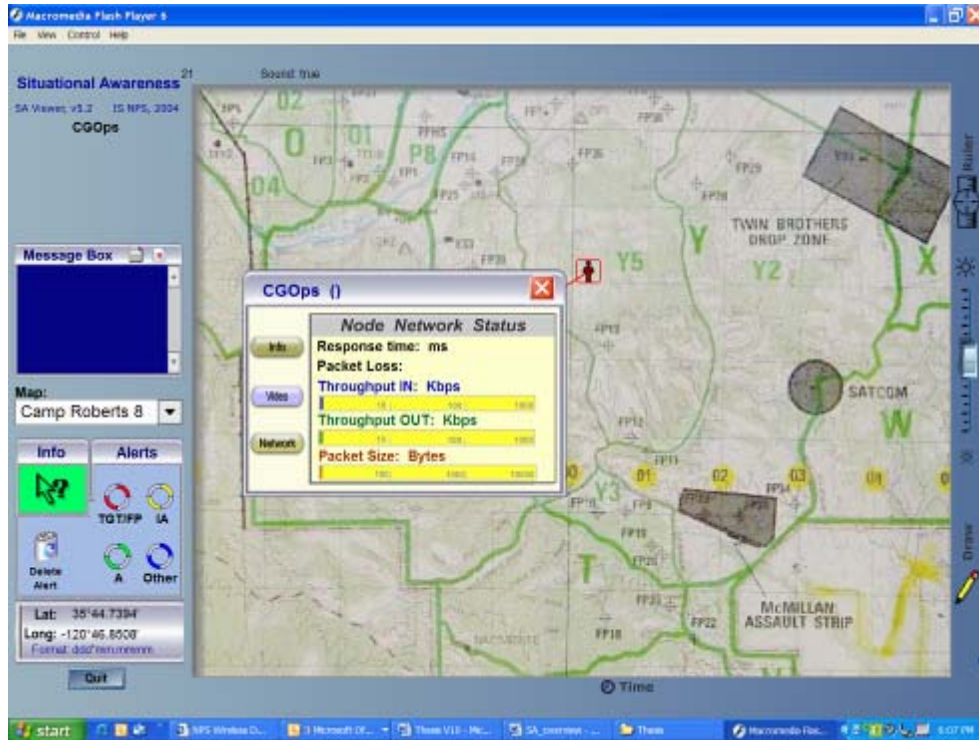


Figure 19. Network Awareness

D. NETWORKING CAPABILITIES

1. System Requirements

There are no network limitations to the way you can establish a network connection to the SA Server at NPS. Network connections can be established wirelessly over an 802.11 network using internal or external wireless cards, over an 802.16 network using a Redline AN-50 radio set, through a Local Area Network (LAN), over an Internet connection, and via a 900 MHZ radio link. The SA server is also configured to use satellite communications via Iridium phones or modems. A general representation of the different types of connections is shown in Figure 20.

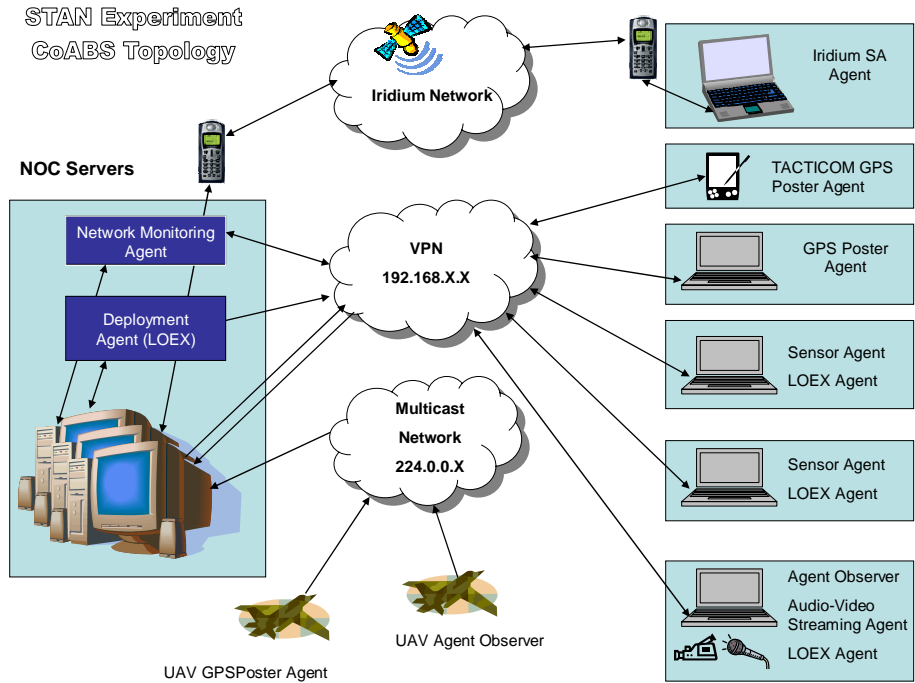


Figure 20. SA Agent Topology

2. Bandwidth Requirements

There is no minimum bandwidth required to run SA Agent on a network. It is important to understand though that the slower network connection, the slower the synchronization of data.

E. INTERFACES AND TERMINALS

1. User Interface Customization

SA Agent is based on one basic visual representation. Customization is limited to choosing one of the available maps in the current version of SA Agent. The current version has 10 preloaded maps as the background of the GUI to cover Camp Roberts, Monterey Bay, and NPS' quadrangle. The available maps can be easily integrated to include any maps for any operational area.

2. User Terminals

a. Operating System and Hardware Requirements

The SA Multi Agent System was developed using several programming languages like Macromedia Flash MX on the client side and Microsoft (MS) Visual

Basic, MS C++, and Java on the server side. You can use SA Agent on a Microsoft Windows, Linux, Apple OS, or any other computer system as long as it has a version of Macromedia Flash Player created for that operating system and the machine has the ability to establish a network connection.

b. Software Requirements

SA Agent requires Macromedia Flash Player to be installed. A configuration file (text file) will also need to be located in the same directory with SA Agent (Figure 21). This file requires a user ID, server internet protocol (IP) address and Port number which will be assigned by the administrator. In case of using Multi-path network connection (wired, 802.XX, Iridium, etc.) the set of IP addresses, port numbers and interfaces will be assigned correspondingly to provide an uninterrupted network connection. This makes the connection more robust and secure.

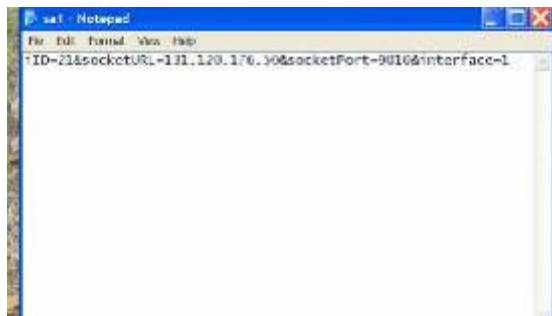


Figure 21. Configuration File

c. Internet Connection

Any as long as it makes it back to the SA server at NPS.

F. SERVER SIDE APPLICATION

There are two administrative functions available to the SA administrator: SA Agent Tracer and Agent Administration Facility.

1. SA Agent Tracer

SA Agent Tracer is a software program that consists of socket connection port listeners and distributors. They listen to the available ports for transmit control protocol (TCP) and/or user datagram protocol (UDP) requests from all the SA agents. The Tracer processes the requests and then distributes all changes to other agents that are connected.

Any event is then recorded and distributed i.e. position changes, alerts, motion detection, new drawings, acoustic interaction, etc depending on the sensor. The confirmation is displayed in the activity log and the corresponding update shows up on each agent's screen. The connection log records the status of each agent. Another feature that is useful to the administrator is the use of the commercial mobile phone Short Messaging System (SMS). If this box is checked, it will send the message to administrator's cellular phone to notify him that a change has occurred like an agent has logged in or logged off, video motion has been detected, or important system status changes have occurred. It also allows the administrator to make changes to SA server settings from his cellular phone. The last feature available on SA Agent Tracer is to enable the Snapshot on Motion function. This applies for smart or self contained agents that have video or imaging capabilities. Snapshot on Motion allows for one of the agents (like a "smart rock") to automatically capture images after motion is detected within its set of parameters (Figure 22).



Figure 22. SA Agent Tracer

2. Agent Administration Facility

Agent Administration Facility is the Web interface to the database that allows the administrator to manage all the SA Agents in the system (Figure 23). The basic functionality of the GUI is as follows:

- ID number: Needs to be unique and not duplicated on different units
- Icon Type: can be a person, car, UAV, weather station, observer, boat or a balloon. This is also customizable
- General Comments: Provides amplifying information about the agent
- Camera Ctrl: States that the agent is equipped with a pan-tilt-zoom (PTZ) video camera that is ready to be controlled remotely
- Enabled: Allows the administrator to enable or disable agents
- Ewall: Allows the administrator to include/exclude an agent from MIT's Ewall agent list

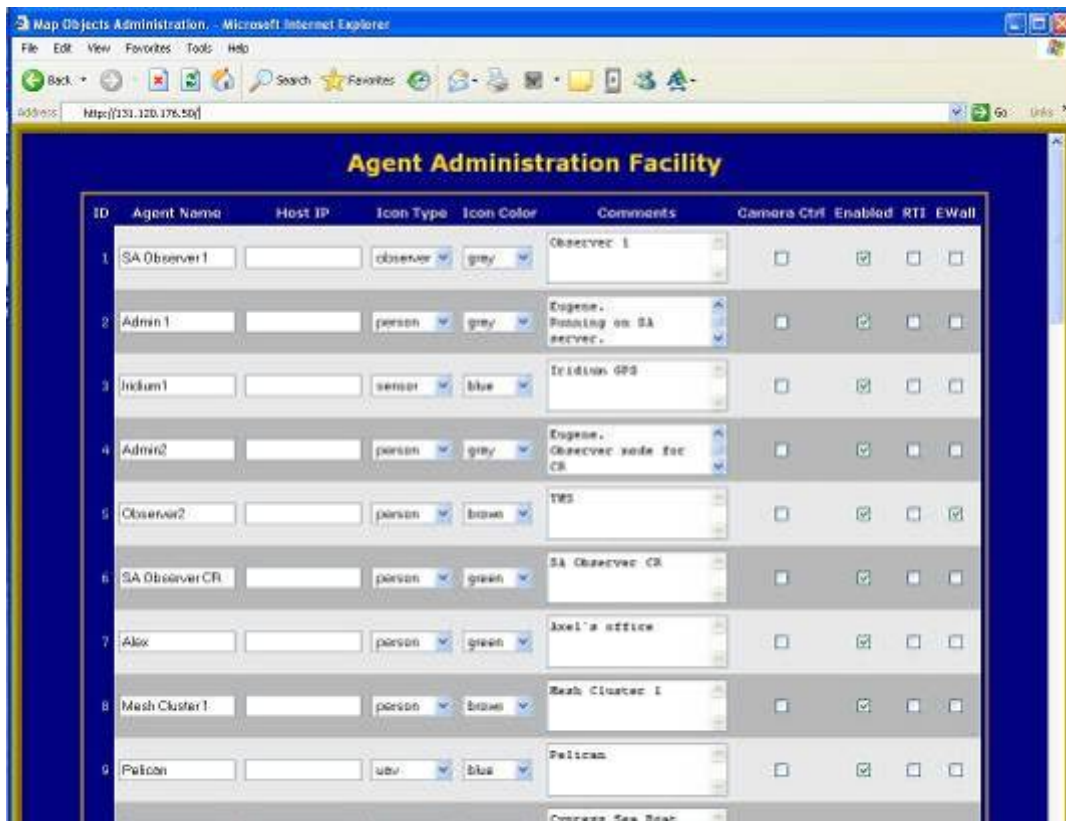


Figure 23. Agent Admin Facility

V. LAWRENCE LIVERMORE NUCLEAR SENSOR OPERATIONAL SCENARIO

A. NAVAL POSTGRADUATE SCHOOL FIELD EXPERIMENT TNT 05-2

Utilization of a Wireless Network and Collaborative Systems to Discover and Transfer Nuclear Material Sensor Data from an Underway Coast Guard Cutter to Expert Reviewer at Lawrence Livermore National Laboratory

B. DATE

28 February 2005

C. LOCATION

Monterey Bay, NPS GIGA Lab, Lawrence Livermore National Lab

D. BACKGROUND

The Coast Guard routinely conducts at sea boarding and has begun using Radiation Detectors to identify potential nuclear material being illegally smuggled in to the U.S. This experiment is the first time that the Coast Guard and the radiation equipment authorities (LLNL) have worked on a combined effort to evaluate the readings of the sensors by experts located at their home office. The goal is to leverage the current wireless networking technologies using an 802.11 mesh network coupled with an 802.16 network and the collaborative tools Groove and Situational Awareness (SA) Multi Agent System to enable the LLNL radiation experts be virtually present on an at-sea Coast Guard boarding allowing their expertise to be used to determine the degree of preventative action necessary on a individual basis.

E. EXPERIMENT TECHNOLOGIES

- Ship (Cypress Sea) with 802.11b connectivity to Boarding Team and 802.16/Orthogonal Frequency Division Multiplexing (OFDM) connectivity to the Tactical Operations Center (TOC) and SA display.
- Boarding Team with Mesh Laptop with antenna that provides 802.11b connectivity with Cutter
- SA display of underway track
- TOC with 802.11b and 802.16/OFDM connectivity with Boarding Platform (Cypress Sea) and LLNL; SA Agent display with blue force tracking.

F. ENVIRONMENTAL VARIABLES

- Weather
- Sea state
- Background wireless traffic

G. MEASURES OF PERFORMANCE

- Ability to detect radioactive material on board test platform
- Ability to correlate radioactive readings with navigational position
- Ability to provide SA to the boarding team using combination of 802.11b and 802.16/OFDM
- Initial human systems integration data integrating for Coast Guard (CG) Boarding Team using a collaborative tool and the required hardware configuration
- Initial human systems integration data integrating LLNL into live boarding scenario

H. EXPERIMENT PARTICIPANTS/CAPABILITES/ASSETS

1. Exercise Role Assignments (Exercise Role: Role Player)

- Coast Guard Boarding Platform: Motor Vessel (M/V) Cypress Sea
- Coast Guard Boarding Team: LT Burdian, Phil Kerr (LLNL), and David Trombino (LLNL)
- Target Vessel of Interest: USCGC HAWKSBILL
- Coast Guard Operations Center: NPS' Network Operations Center (NOC)

a. Boarding Team

- Coast Guard member
- LLNL personnel
- 3 Dell Latitude X300 Computers
- Collaborative Tools:
- Groove Virtual Office Version 3.0
- NPS SA Agent


2. Radiological Sensing Equipment

a. Rad Pager

Small dose rate meter (RadPager)

- Belt mount
- CsI γ -detector + LiI neutron detector
- Dose rate readout
- Audible or vibrating alarms

Thermo Electron Corporation: PM 1703GN




Used to indicate presence of, and locate sources of gamma and neutron radiation
...not a Health Physics instrument or an electronic personnel dosimeter...

No Radioisotope Identification Capability !

Figure 24. Rad Pager

b. IdentiFINDER (Radiation Isotopic Identification Device)



identiFINDER

Waterproof, Hand-held, Portable Isotope Identifier

- capable of detecting, locating, and identifying radioactive sources
- dose rate measurements
- count rate record
- recording spectra
- identifying radioisotopes

Figure 25. identiFINDER

c. Neutron Pod – Helium-3 Detector

d. Ortec Detective

POSITIVE IDENTIFICATION OF RADIOACTIVE MATERIALS

- Rapid, Simple and Reliable Classification of NORM, Medical, Industrial, Nuclear and Natural Isotopes via advanced algorithms
- Search and Identify Modes, including dose rate
- 20x Improvement in Resolution (selectivity) compared to identifiers based on NaI
- Portable, battery operated instrument
- Ready to use at all times, straight from docking station
- Digital spectrometer electronics
- A definitive portable answer to the detection of illicit trafficking
- HPGe detector cooled by miniature, high-reliability mechanical cooler that operates from battery, line power or from 12 V DC
- Performance enhanced by digital noise filter¹
- Detector element encapsulated in high reliability, low loss, all-metal seal cryostat
- Proprietary identification software



¹Patent Pending

Figure 26. Ortec Detective

3. Ships

a. “Coast Guard” Boarding Platform

M/V Cypress Sea

Length 50 ft

Beam 15 ft

Displacement 50 tons



Figure 27. “CGC” Cypress Sea

b. Target Vessel of Interest (TOI)

USCGC HAWKSBILL (WPB 87312)

Length 87 FT

Beam 19.5 Ft

Displacement 90 tons



Figure 28. USCGC HAWKSBILL (WPB 87312)

4. Scenario

A Coast Guard Cutter is on patrol in one of our nation's busy harbors. As they patrol, they maintain communications with their Sector Command Center via two networks: the Orthogonal Frequency Division Multiplexing (OFDM 802.16) and on-board tactical mesh (802.11b). For collaboration with the Sector Command Center and other vessels on patrol, they use the collaborative tools found in Groove Virtual Office and SA Agent to chat, receive tasking and provide general updates on their status during the patrol.

During the course of the patrol, several routine boardings occur. The Boarding Team maintains contact with the Cutter with their collaborative tools transmitting over an ad hoc, wireless network link. Among the tools at the boarding team's disposal are radiological detection devices. As these radiation detectors detect radiological activity, the Boarding Officer captures the signature and places it in their workspace so that the Sector Command Center and the scientists at the Lawrence Livermore National Lab can read and interpret the results in real-time.

Implementation of the technologies described in this scenario will, for the first time, permit operators in the field to have the expertise of a virtual National Laboratory at their disposal assisting them as they make critical decisions identifying possible threats and then, formulating courses of action to handle the threat.

5. Pre 28 Feb

- USCGC HAWKSBILL will be underway on normal patrol.
- Groove Workspaces are set up: (1) Boarding- for integration of Boarding Team, Boarding Platform, and OPCEN/NOC and (2) LLNL- for integrating the Livermore Lab with the OPCEN
- Training conducted for LLNL and Tactical Satellite (TACSAT) personnel on proper use of Groove an SA Agent

6. 28 Feb 05

0800 Boarding Team and Boarding Officer set up mesh laptops with amplifiers and validate positive link status.

0930 CGC HAWKSBILL picks up LT Stephen Burdian and LLNL representatives from their mooring via small boat. All equipment (Neutron Pod) will be transferred via this “boarding” embarkation which will serve as the pre-staging of the BT on the TOI vice actually conducting the at sea transfer from the CG Boarding Platform (Cypress Sea).

Cypress Sea underway from moorings with LCDR Klopson, LLNL personnel, and Neutron Pod equipment onboard

1000 Mesh network established and tested. Communications established to all parties involved. Background readings for radiological equipment will be taken and transferred to LLNL.

LLNL will hide their test radiological substance in one of HAWKSBILL spaces

All players verify that Mesh is established and SA is functioning and observed by TOC.

Cypress Sea and HAWKSBILL are on location in the bay North of NPS.

1030 Scenario begins

TACSAT personnel will forward electronic intelligence (ELINT) information and imagery of Monterey Bay to the CG OPCEN (NPS TOC) simulating the identification of the target of interest (TOI).

1035 TOC posts this information in the Groove Virtual Office Workspace Boarding which synchronized over the OFDM and Mesh tactical network to the Boarding Officer on Cypress Sea and task them to intercept the TOI and conduct an at sea boarding.

1045 The boarding team will then initiate an Initial Safety Inspection (ISI) of the TOI. During the ISI, the pager sensor will alert to the presence of a radiological substance aboard the vessel.

1100 The boarding team will then download this data from the sensor in the form of a text file to their laptop computer and post it in the Boarding Groove workspace in Groove. This information will be self synchronized back to the Cypress Sea via the mesh network, and onward to the NOC via the OFDM link.

1115 TOC determines proper procedure for file (which is to forward to LLNL) and will then copy this file and post it in the LLNL Groove space so that the data can be examined by scientists at the Lawrence Livermore National Laboratories and observed by TACSAT personnel.

1130 LLNL evaluates data and provides feedback via Groove or SA chat capability

1145 Based on LLNL evaluation, boarding team will initiate an extended ISI (Level 2 Inspection) and attempt to locate the source of the radiation.

1200 Video and audio will be fed to and from the boarding party via Groove and SA Agent. Once the source of radiation is positively located and identified the boarding will conclude. The boarding officer will then download the cumulative data from the Neutron Pod and forward the information to LLNL for evaluation.

1200 Scenario concluded. Cypress Sea and HAWKSBILL receive a finished with exercise (FINEX) message and initiates return to dockside.

1300 LLNL and CG Boarding Team participants debriefed for qualitative analysis of exercise results.

7. Contingency Plans

* If difficulty transferring the data from the detectors to the Laptops is experienced, the **Boarding Team** will open the “Phony Rad Data” folder on the desktop, and post it in the **boarding workspace**. The Boarding Officer also has these files on his desktop in the event the mesh network does not work well in the marine environment. The **Boarding Officer** should then post these files in the **NOC workspace** for synchronization over the OFDM link.*

** If severe delay in synchronizing data between the **Boarding team** and the **NOC** is experienced, the Boarding Officer on the Cypress Sea should un-invite the **NOC** from the **Boarding workspace** and forward all information from the **Boarding team** by cutting and pasting all info into the **NOC workspace**. The **NOC** will continue doing the same in the **LLNL workspace**.**

VI. INTEGRATION OF NUCLEAR RADIATION SENSORS

A. INTRODUCTION

The reason this proof of concept experiment was conducted to explore the feasibility of integrating a mesh self organizing wireless network with radiological sensors and collaborative technology to bring together people from different fields with the appropriate expertise to prevent threats to our Homeland Security from becoming disasters like the terrorist attacks of September 11th 2001. Operationally, this experiment coordinated intelligence personnel from the Navy Research Laboratory's Tactical Satellite (TACSAT) division, a Coast Guard ship and crew, and scientists from Lawrence Livermore National Laboratory (LLNL) to identify, intercept, board, collect data and then translate the data to decisively determine whether or not one of our country's harbors, Monterey Bay, was threatened by a suspicious vessel carrying radioactive material.

This experiment combined Coast Guard capabilities with those of highly skilled individuals who would respond in the event of a radiological threat. At best, the Coast Guard personnel conducting a vessel inspection would include someone who has completed Level II radiological sensor training at Lawrence Livermore National Laboratory and would be able to take a thorough round of data collection before calling in specialists for a more in depth investigation. In this experiment, specially trained personnel were part of the boarding party, which increased the teams overall field capabilities, compressed the timeline of the experiment by negating the need to wait for specialists to be notified and eventually arrive and explored the operational constraints in regards to collaboration.

The 28th of February 2005 was an optimal day for doing an experiment at sea. The weather cooperated, all the key players showed up on time, and we were able to successfully employ our collaborative software systems, tactical networks, and radiological sensors in a manner representative of real world operations.

B. RADIOLOGICAL SENSOR TRAINING AND INTEGRATION

1. Training Required to Operate

There are two different levels of training, Level I and Level II, which are offered to Coast Guard personnel. This training is focused on those Coast Guard personnel that conduct merchant vessel inspections or might have to respond to a situation involving radioactive materials. Level I training provides the basics needed to recognize a possible radiological threat and covers the use of the RadPager. Turn it on, if it goes off, make sure you contact your operational commanders and get Level II trained personnel on scene to take more in-depth readings. Level I training can be completed online over the Coast Guard Intranet. Level II is a bit more in depth and takes 24 hours of class work to complete. During Level II training, the students learn how to operate the RadPager, identiFINDER, and RadPack sensors. The course objective is “To provide practical technical training to US Coast Guard personnel to prepare them for service in possible terrorist or other criminal investigations involving hazardous radioactive materials. The training includes radioactive materials scenarios of concern to US Coast Guard ship inspectors, fundamentals of radioactive materials, radioactive safety procedures, selection and use of radioactive detection instruments, development of proficiency in the proper use of hand-held radiation detection equipment, detection and identification of radiation, and proper radioactive materials search techniques.” (National Labs 2004).

If Coast Guard inspectors were to detect radioactive materials during a vessel inspection and completed both Level I and Level II inspections, they would “reachback” to the United States Customs Service (USCS). The data collected would be downloaded and forwarded to Customs agents for their analysis. At this point, Customs would make a determination of whether or not the data required further analysis or not. If so, Customs would initiate a call for “secondary reachback”, which means that the sensor data would be forwarded to a National Laboratory, like Lawrence Livermore National Laboratory (LLNL) for more in-depth analysis. Depending on the National Laboratory’s findings, a team specializing in radiological threats would be sent to the ship for a more in-depth investigation. The Neutron Pod and the Ortec Detective are part of a suite of advance detectors that are available to specialists.

2. How to Interface with Hardware

Integration of the different radiological sensors was not very difficult to accomplish for the RadPager, identiFINDER, neutron pods, and the Ortec Detective. The RadPager, identiFINDER, Detective, and RadPack are commercial off the shelf (COTS) products with commercially available software. The RadPack did not have the ability to connect with our computers and their data was only able to be analyzed when they were returned to LLNL. For the RadPager, identiFINDER, neutron pods and the Ortec Detective it was simply a matter of loading their software on the experiment's Dell Latitude X300 computers. The RadPager has an infrared (IR) interface and would automatically download its latest text data files when it was placed next to the laptops IR port. The identiFINDER requires a serial port connection. Since the Dell laptops did not have a serial port, a USB adapter was used to make the connection. The neutron pod used a serial port connection. Lastly, the Ortec Detective connected to the Dell laptops via a USB port connection.

The sensor's software did the rest. Once the data was downloaded to the Dell computers, it was simply a matter of copying the text or PKCS documents to the appropriate workspace for synchronization and analysis.

C. WHY THE SCIENTISTS NEED TO BE OUT ON THE BOARDINGS

Simply put, the scientists have the expertise that your average Coast Guard inspector does not when it comes to locating and analyzing radiological data. A 24 hour course will never replace a life's work within the scientific community, nor should it attempt to. By giving both the Coast Guard inspector and the National Laboratory scientist effective collaborative tools on robust wireless networks, the Coast Guard will in essence be able to make the scientists part of the boarding party. In the event radioactive material is located during a vessel inspection, video and real time data can be collected and analyzed in one collaborative effort, which will make the inspection process more efficient and effective.

The current process of collecting and analyzing radiological data takes too long and can be very cumbersome. The Coast Guard Marine Safety personnel initially begin a vessel inspection only carrying the RadPager with them. If the RadPager does detect neutrons in the area, they must either call for or send for a Level II inspector to bring the

Radpack and identiFINDER devices. Notifications are made to the appropriate personnel through an operations center, which takes time. Even after the data is taken, there is not a procedure or network in place that allows for real-time transmission of the data to the scientists for analysis. After initial detection, it can take half a day or more for appropriate personnel to be dispatched to the scene to conduct a more in depth investigation. This is not to say that responses to radiological threats aren't responded to appropriately, but suggests that the current process of collecting and analyzing data can take days depending on the threat's location. This can and needs to be reduced from days to hours or minutes and can be accomplished if the proper collaborative environment is available to all parties involved.

D. CHRONOLOGY OF EVENTS

Prior to the commencement of the experiment, all computers and radiological sensors were tested and found to be in good working order. Background Readings were taken without the radioactive source present so they could be compared with actual readings during the experiment. A radioactive source of californium and americium was placed on board the HAWKSBILL. The radioactive sources were: Am-241, 11.25 MicroCuries and Cf-252, 4.4 MicroCuries.

The Cf source was shielded by an inch of lead. Network connections were made over the internet with Groove and SA Multi Agent to Lawrence Livermore National Laboratory and the Naval Research Laboratory's TACSAT personnel in Washington, DC. The following timeline shows the highlighted parts of the experiment:

0939: Communications were established with NPS' NOC, LLNL, and TACSAT personnel using Groove Virtual Office (LLNL Workspace).

1052: Video and audio established at NPS, LLNL, aboard "CGC" Cypress Sea, and at TACSAT using SA Multi Agent System. NPS' NOC and Cypress Sea were the only assets sending audio and video (Fig 29).



Figure 29. SA Multi Agent System

1124: TACSAT placed an Alert icon on the SA screen depicting the target of interest (TOI) HAWKSBILL. NPS' NOC and Cypress Sea acknowledged receipt of the alert.

1129: TACSAT posted electronic intelligence (ELINT) information and imagery files of Monterey Bay (Fig. 30) in the LLNL Experiment workspace. These files showed the presence of the vessel "HAWKSBILL" which roused suspicions and necessitated further investigation. This information was copied and placed in the NOC workspace for synchronization with the "CGC" Cypress Sea.

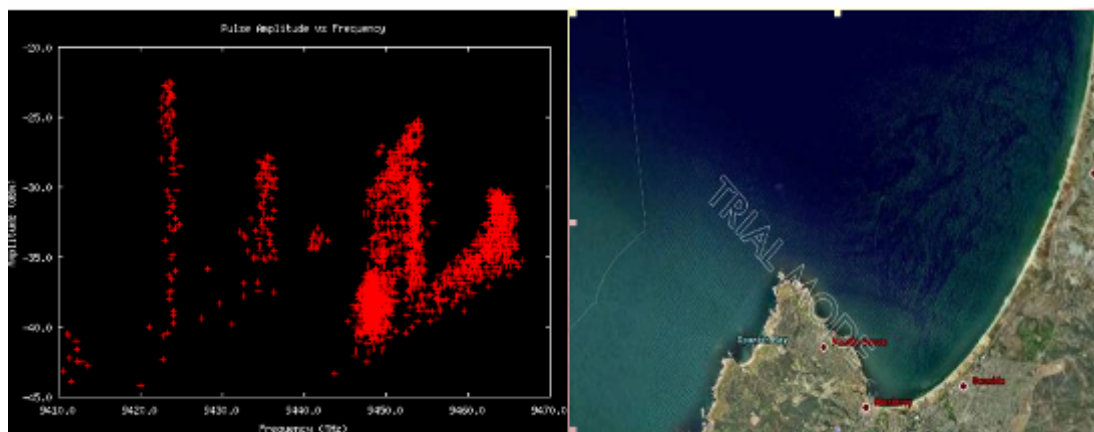


Figure 30. Elint and Imagery Files regarding HAWKSBILL posted

1149: The intercept and commencement of a boarding of the HAWKSBILL was simulated. The boarding team was unable to establish consistent connectivity with Cypress Sea over the Mesh (802.11) network. The boarding team gathered radiological data using the RadPager, identiFINDER, Ortec Detective, and Neutron pod aboard the HAWKSBILL (Fig. 31). Initial readings from the RadPager noted neutron and gamma readings. The IdentiFINDER analyzed the gamma spectrum and identified the source as either Am with a confidence level of 7-9. The presence of americium could signify that this is a plutonium source since americium is a daughter product of plutonium. Further measurements with the neutron pod and Detective were made. This data was downloaded to the boarding team's laptop for transmission over 802.11 mesh network once it was established.



Figure 31. Boarding Team Using Ortec Detective

1200: The mesh network was unable to be established with any consistency and deemed unsuitable for experiment. The Cutter and NOC concluded that best course of action was to complete the experiment aboard the Cypress Sea utilizing the 802.16 OFDM network only.



Figure 32. “Meshing” between HAWKSBILL and Cypress Sea

1220: The boarding team and radiological sensors were transferred to the Cypress Sea to continue the experiment. After setting up their equipment aboard the Cypress Sea, radiological data was downloaded for transmission over the OFDM network to the NOC.

1241: Radiological data files were posted in LLNL workspace and receipt was acknowledged by LLNL and TACSAT (Fig. 33).

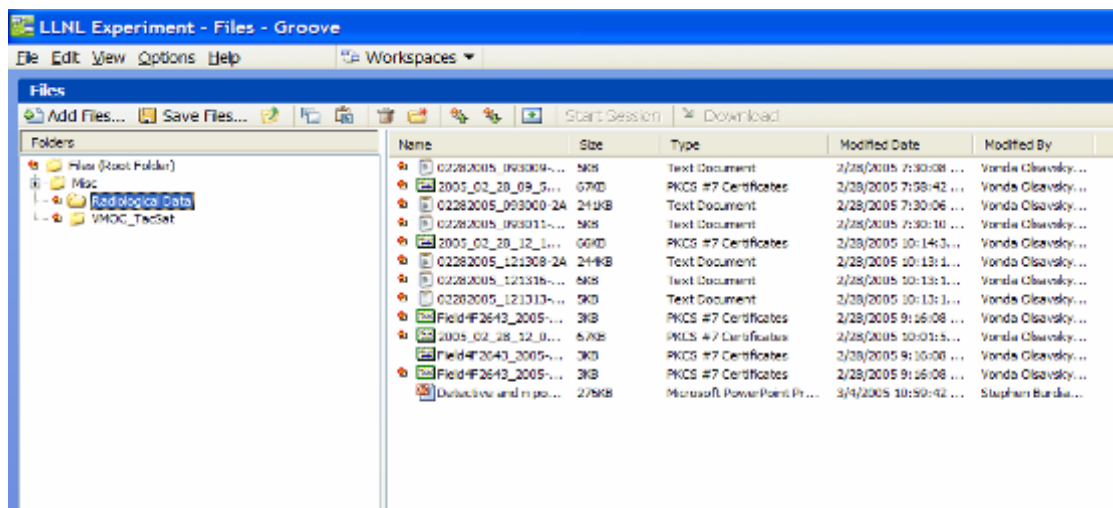


Figure 33. Radiological Files posted in LLNL Workspace

1318: LLNL positively identified the radioactive substance aboard the HAWKSBILL as Californium and Americium (Figures 34 – 37) from the Neutron pod and Detective data.

```

D:\0228006_11513_26-Typel - Notepad
File Edit Format View Help
02/28/2005, 12:11:14, data stored
\\storage-card\0228006_121313-26-Typel.log
**** Counter Setup ****
mode = Neutron Generator -26-Typel Rossi-Alpha Analysis
1. bin width (microseconds)
312. bins
1. Mode 26 Delay (microseconds)
311. Mode 26 Length (microseconds)
**** Counter Data ****
Total Run Time = (1s. #of bins) X (Bin width) X (Total Cycle Count) / 1000000 = Time in seconds
Total Run Time = 311 X 1 X 403513 / 1000000 = 236.85514 seconds
Total Number of bins = (1s. #of bins) X (Total Cycle Count)
Total number of bins = 311 X 403513 = 23855141 bins ( 2.37e+08 )
Average Count Rate = Total Count / Total Run Time (sec)
Average Count Rate = 4220 / 236.85514 = 17.8168
Bin No., Data
0., 20
1., 40
2., 25
3., 24
4., 29
5., 25
6., 28
7., 28
8., 27
9., 28
10., 27
11., 28
12., 27
13., 30
14., 35
15., 27
16., 27
17., 19
18., 23
19., 24
20., 20
21., 19
22., 19
23., 19
24., 20
25., 22
26., 17
27., 19
28., 19
29., 25
30., 25

```

Figure 34. Neutron Pod Raw Data Readout

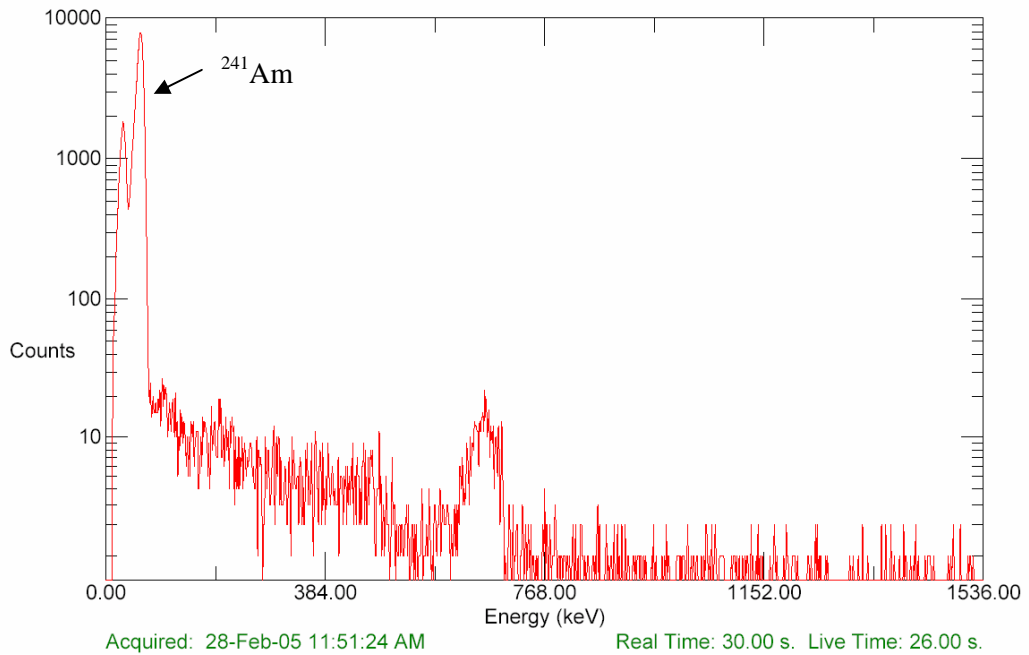
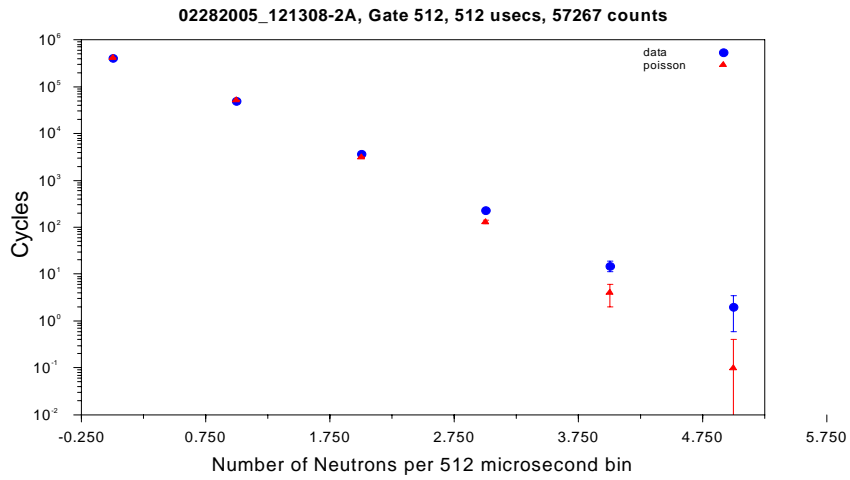


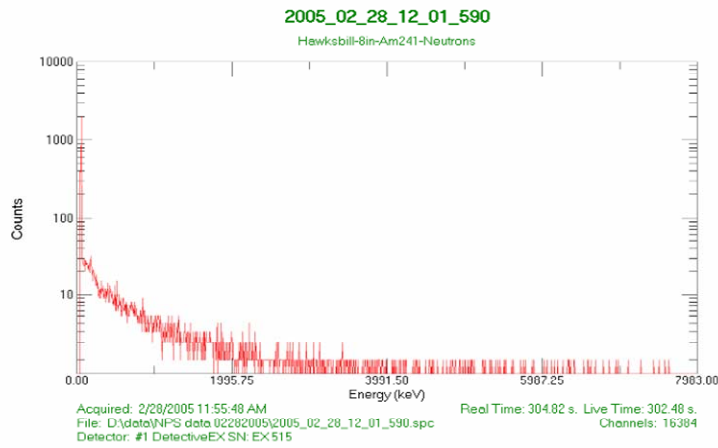
Figure 35. identIFINDER Target Spectrum



With Source: Solves as 8.75 ng (~4 μCi) Cu Cf²⁵² source

LF Nakae 3/2/2005

Figure 36. Neutron Pod Readout



Detective Gamma-ray Spectrum (5 minutes) on source (Note 59.5KeV Am241 peak and fission Gammas from Cf²⁵² source).

LF Nakae 3/2/2005

Figure 37. Ortec Detective Readout

1321: Having ruled out the presence of plutonium aboard the HAWKSBILL, the exercise was concluded.

E. RESULTS

The results of this experiment were promising. Despite the inability of the boarding team to successfully maintain a persistent connection with the Cypress Sea over the 802.11 mesh network, the Cypress Sea had full connectivity with TACSAT personnel in Washington, DC and LLNL scientists in Livermore, California over the 802.16 OFDM and internet networks. SA Multi Agent System provided each player with a common operating picture that accurately depicted real-time locations and communications between all of the experiment's participants. Groove Virtual Office allowed for improved synchronization of the data collected at sea to the NOC and scientists back at the lab for analysis. These two collaborative software suites were successful in taking a process which includes data collection, notifications, and analysis, which could upwards of a day down to several hours. It also allowed the scientist to have direct input into the continued investigation. They were able to ask for additional readings, provide direction in regards to data collection, and ask questions to clarify what data they were looking at. The flexibility that TNT network and the collaborative software suites provided allowed for a suspected plutonium source to be positively identified as Californium and Americium.

As a result the success of this proof of concept experiment, both Lawrence Livermore National Laboratory and the Navy Research Laboratory's TACSAT division are considering establishing a Maritime Awareness test bed at the Naval Postgraduate School. Future experimentation will be based on the work completed during the LLNL/TACSAT scenario with the exception that both LLNL and TACSAT will conduct future operations over TNT's intranet instead of the commercial internet.

VII. PERFORMANCE EVALUATION

A. NETWORK PERFORMANCE

The network configuration for the experiment was comprised of a combination of wired internet and intranet links as well as wireless 802.11 and 802.16 links. The Boarding Team node on CGC HAWKSBILL is extreme edge of the network. It is connected to the Motor Vessel Cypress Sea via an 802.11b mesh network connection. The Cypress Sea is then networked to the Del Monte Beach Station via an 802.16 OFDM wireless link. The Del Monte Beach node is a radio tower with several fixed antennas. It has 3 sector antennas that allow it to connect to the Cypress Sea on the water and another antenna which provides a point-to-point connection with the Naval Postgraduate School (NPS) Spanagel Hall node, which is a radio tower. In addition to the link to the Beach, the Spanagel tower also has a point-to-point connection with the NPS Network Operation Center (NOC) tower, which communicates through its antenna on the roof of Root Hall. The NOC is the central node of the network, serving as the join point between the wireless 802.16 links and the wired intranet. The bridge between the NPS intranet and the public internet is contained within the NOC. The other nodes used in the experiment, Lawrence Livermore National Lab (LLNL) and Tactical Satellite (TACSAT) Washington DC are both connected to the network via the public internet.

The network configuration was successful in connecting the various nodes and was generally capable of handling the required throughput for all the experiment applications. The fixed 802.16 nodes on the Spanagel and Beach Towers performed as well as a wired network with no appreciable packet loss. The mobile 802.16 link from the Beach Tower to the Cypress Sea was able to maintain a connection for the entire duration of the experiment. During the experiment, real-time video was maintained over the SA Agent program and real-time chat was maintained over the Groove system.

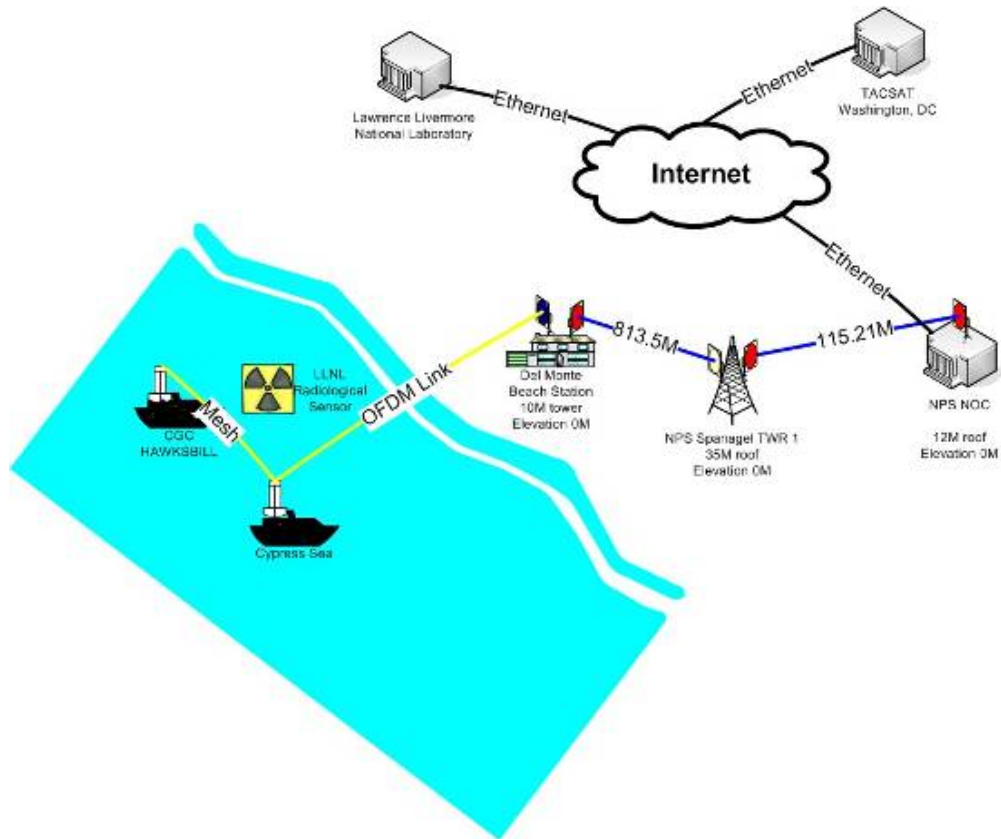


Figure 38. Network Configuration

The one weak link in the network proved to be the 802.11 mesh segment between the Cypress Sea (Cutter) and the HAWKSBILL (Boarding Team). In their earlier thesis work, Eric Bach and Mark Fickel used a term to describe the 802.11 mesh network which serves as a very good descriptor of the mesh performance in this testing and experimentation- fragile. (Bach 2004) During the experiment, the 802.11 mesh proved to be very fragile, with very limited network connectivity.

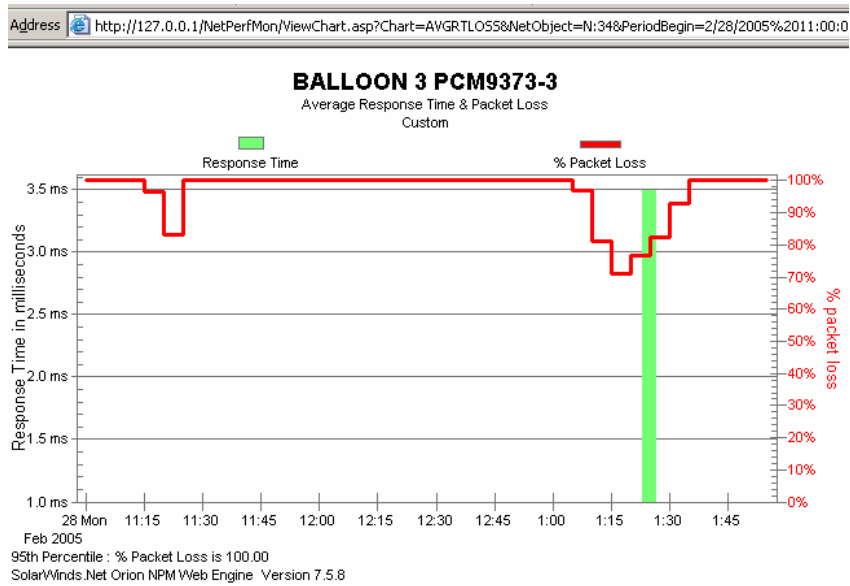


Figure 39. Solarwinds graph of Boarding Team connectivity

A combination of factors led to the fragile and intermittent connectivity of the 802.11 mesh segment of the network. The 802.11 wireless radio frequencies are easily disrupted by various interferences such as cordless phones, Bluetooth devices, and microwave ovens. Any and all of which are regularly used on board Coast Guard cutters as well as target vessels.

During pre-experiment testing we were able to establish and maintain strong links at ranges up to 500 yards, yet during the experiment, we could not maintain a usable link at less than 200 yards. This can be attributed to a combination of the weak performance of the 802.11 wireless network in the outdoor, over-water environment and the various levels of noise experienced on the underway ships.

As a result of this experiment, our initial reaction is that 802.11 mesh is too sensitive for Coast Guard applications. The Coast Guard needs a stronger and more resilient communication link. That link appears to be provided by the 802.16 network standard.

As stated before, the fixed links performed nearly as well as a broadband wired network.

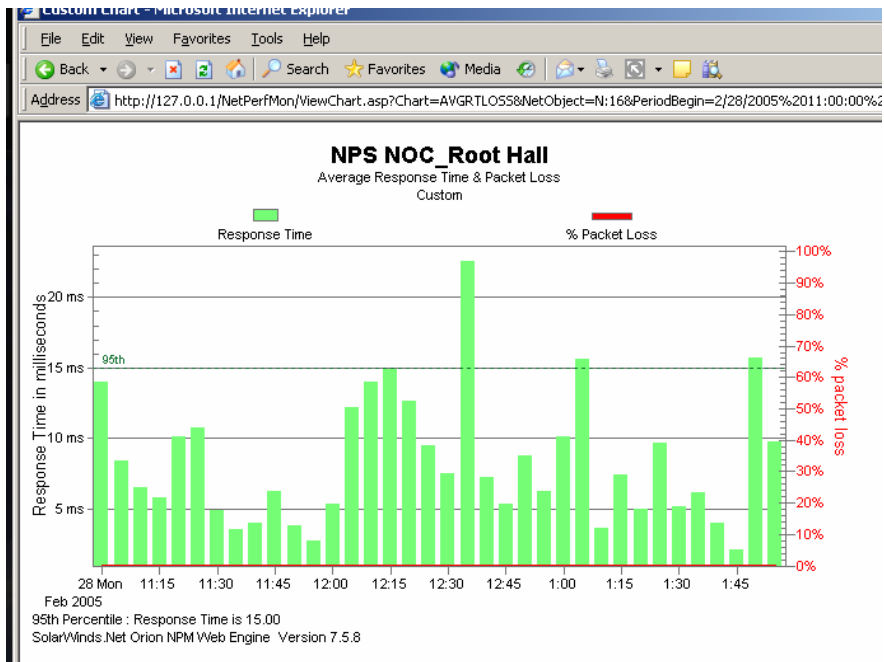


Figure 40. Solarwinds chart of NOC connectivity

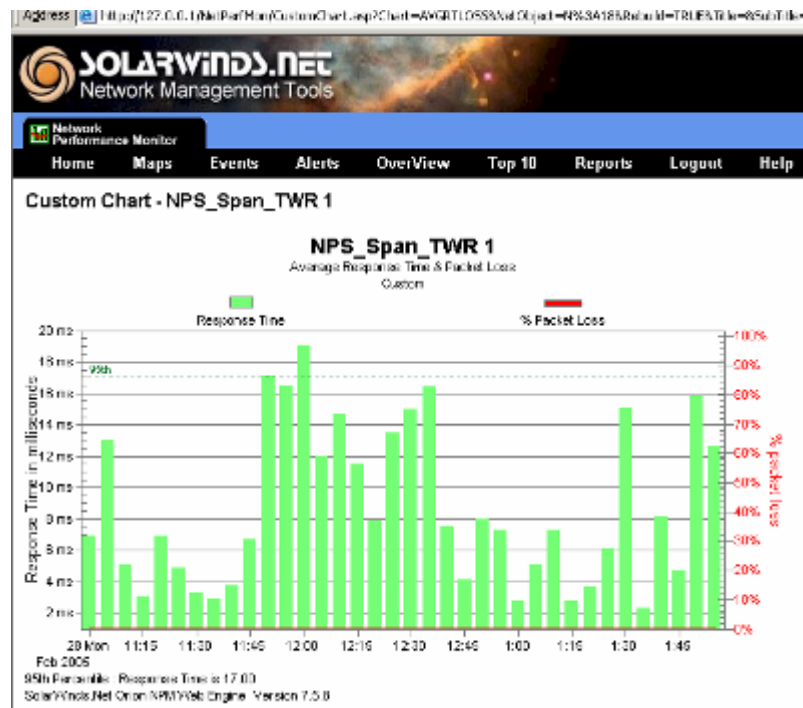


Figure 41. Solarwinds chart of Spangel Tower connectivity

The results were encouraging from the general networking aspect of the experiment, especially in relation to the performance of the mobile 802.16 link on the Cypress Sea. The omni directional antenna was able to maintain a strong link with the Beach Tower through the entirety of the experiment, functioning basically as well as the fixed 802.16 towers. The positively evaluated performance of the 802.16 network hardware has raised further options for an alternative configuration which could possibly improve upon the performance of the 802.11 portion of the network- that of utilizing Redline's new 802.16 Manpacks. This concept is discussed further in Chapter IX.

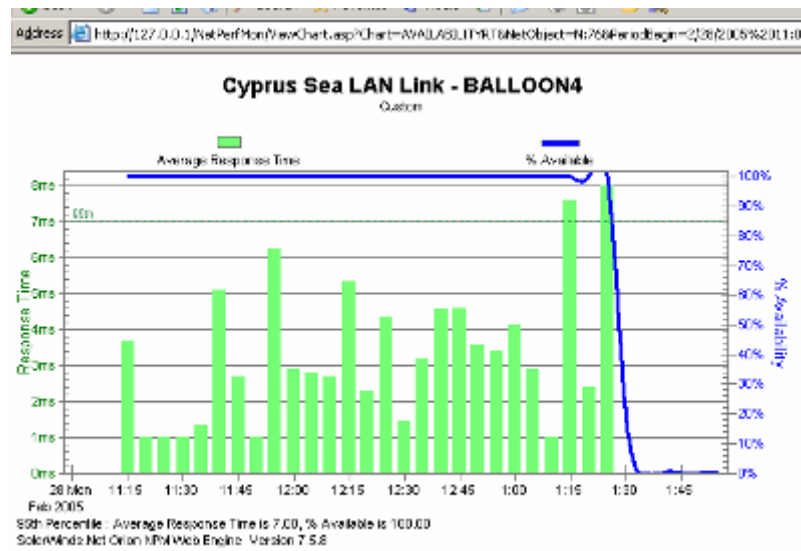


Figure 42. Solarwinds Chart of Cypress Sea connectivity

B. COLLABORATIVE SYSTEM PERFORMANCE

Two separate collaborative software systems were set up on the various computer terminals used in the experiment. Situational Awareness Agent was installed in the NOC, the Cutter, the Boarding Team, TACSAT, and the LLNL systems. This configuration enabled each node to view the position of all the others, receive real-time video from each other, as well as conduct real-time chat as required. Each of the systems described above also was configured with Groove Virtual Office software. Several workspaces were created to allow for information and file sharing, whiteboard functionality, and other collaborative work by the various entities involved as necessary.

Both collaborative systems that were tested performed well during the testing and experiment, meeting or exceeding expectations.

Groove worked very well and all files were successfully transferred between the involved parties per the experiment plan. The participants were able to transfer intelligence files from Washington DC to a patrolling cutter in Monterey Bay, and then pass radiological detector data and evaluations back and forth between that cutter and the Lawrence Livermore National Lab. These successful collaborative functions met the objectives of this experiment.

Groove was also able to function during the intermittent connections between Cypress Sea and HAWSKBILL over the 802.11 mesh network.



Figure 43. Real time SA display in NOC, with live video from Cypress Sea

SA Agent also worked well providing real time chat, video, position information, and network status during the experiment. The video and position information provided by SA Agent appears extremely well suited to Coast Guard operations. That functionality feeds directly into the Coast Guard's goal of increasing situational awareness and the common operating picture.

From an ease of use perspective, SA Agent did not perform quite as easily as the Groove system. The learning curve for using SA Agent proved to be slightly greater. While Groove functions very much like a standard Microsoft Window-based application, SA Agent is less intuitive, but nonetheless can be learned quickly.

C. EVALUATION SUMMARY

System	Functionality	Pros	Cons
802.11 Network	Poor	<ul style="list-style-type: none"> • Lightweight radio interface with PCMCIA cards • Well established standard known by many users 	<ul style="list-style-type: none"> • “Fragile”, does not maintain consistent connection • Radio frequencies easily disrupted • Short range
802.16 Network	Good	<ul style="list-style-type: none"> • Ample range for CG operations • Ample throughput for video, voice, and data • Multiple antenna options 	<ul style="list-style-type: none"> • More cumbersome hardware requirements
SA Agent	Good	<ul style="list-style-type: none"> • Real-time video and position capability • Real-time chat 	<ul style="list-style-type: none"> • Slightly less intuitive interface • No file transfer capability
Groove	Good	<ul style="list-style-type: none"> • Easy to understand interface • File synchronization function • Database integration capability • Real-time chat 	<ul style="list-style-type: none"> • No inherent video or position capability like SA

Table 2. Evaluation Summary

Based on this evaluation the 802.16 networking equipment, SA Agent, and Groove all show potential to be used as valuable resources in Coast Guard operations. The 802.11 mesh network on the other hand was not as promising and does not appear to be as well suited for maritime operations and is not recommended as part of this solution.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. MANAGING CHANGE

A. INFORMATION TECHNOLOGY MANAGEMENT STRATEGY

The Coast Guard Information Technology Management Strategy, a document produced by the Coast Guard Chief Information Officer, states the Information Technology (IT) Vision as: “The Coast Guard, as the world’s premier maritime service, delivers the right information to the right people at the right time to support all Coast Guard missions.” (Nacarra 1998)

This powerful statement sums up the reasoning behind this thesis. We intend to achieve that goal of delivering the right information to the right people at the right time to support law enforcement and homeland security.

The fundamental question of this chapter is, “How must the Coast Guard change its service culture to adapt to and take advantage of current and future advances in technology such as our proposed wireless network?” In the Coast Guard Information Technology Management Strategy, Strategy #4 is: Communicate the value of information technology to the organization. In its simplest form, this is the goal of this chapter. In order to successfully manage this change, we intend to communicate the value of this information technology to the organization through direct communications, marketing, training, and exposure. The Coast Guard will be successful in its implementation when employees view this IT system as an integral tool in the performance of their tasks which results in enhanced performance.

B. ORGANIZATIONAL CULTURE

The operational Coast Guard is an organization of professional mariners; it is an organization deeply rooted in its history and firm in its traditions. As such, the Coast Guard still teaches things like celestial navigation. It is always difficult to change an organization from within, especially when the senior leadership has been successful performing in the organization the way it is. They are not likely to be dissatisfied with the processes nor inclined to change things. An organization, such as this, obviously has a tough time accepting change to the way business is processed. Moving to technology is likely a difficult step.

One problem the Coast Guard has faced in the past is that its operating policies do not fully exploit the technological advances that have become available. One example of this is the Coast Guard's implementation, or lack thereof, of electronic charting systems. Electronic charts have been on Coast Guard cutters for many years as supplemental systems- only authorized to back up the paper charts which have always been used as the primary means of navigation. The Coast Guard has long prided itself, and rightfully so, on being highly skilled and prudent mariners. As such, the Coast Guard Navigation Standards remained staunch in their requirement that standard, paper-based charting continues on board cutters, despite technological advances. Hence, the organization would not allow the technology to replace the older method, even though it had the potential for a reduction in personnel crewing. Similar implementation efforts with technology have met similar resistance in the last few years: the Web-based personnel database with self-service functionality for members (Coast Guard Human Resources Management System) and the Abstract of Operations/Training Management Tool web-enabled operational and training database. Each of these implementations met with organizational resistance that mostly amounted to displeasure with changing to a new technology. Status quo was fine with the sailors, because the advantages of those new IT systems did not benefit them as much as they did the Admin and Support personnel behind the scenes. Work was actually increased for the average sailor.

A major part of the problem is that prior technology introductions always tended to increase work. Not only did members have to do boardings, but now they had to enter the information into the database themselves. While an HR database is clearly beneficial to the organization, many member viewed it as extra work placed on the member and resented it- especially those who were not necessarily very computer savvy.

It is this resistance that the Coast Guard desires to avoid. This chapter outlines a recommended plan of action which is intended to maximize the chances of success for the implementation of collaborative systems and wireless networks for operational Coast Guard units.

One of the benefits the organization can hope to reap is the ease at which younger sailors are able to accept new technology, which is just a byproduct of their being raised

in today's IT savvy generation. This lends itself to the operators (the boarding teams themselves) quickly adapting to this equipment and IT capability that we are suggesting. The push back most likely will come from the more senior, "crusty" sailors in command and senior enlisted positions. These individuals may tend to hold on to the old way of doing things for a lack of trust in computers or a thought that this is just going to create more work for the crews.

C. DIAGNOSING TYPE OF CHANGE

There are three basic types of organizational change: (Ackerman 1986) Developmental, Transitional, and Transformational. Developmental change is characterized by being the improvement of a skill or method that is not meeting current expectations: it is doing something better than the way it is done now. Transitional change is introduced to help an organization evolve slowly by replacing current methods with something new (such as a technological change).

Transformational change involved a major change or switch. The Coast Guard is undergoing transformational change as a result of the terrorist attack of September 11, 2001 (9/11). This addition of Maritime Security and Safety Teams and the realignment of Groups and Marine Safety Offices to form the genesis of the newly created "Sector Commands" are major transformational changes. We are modifying the way we conduct business. Another indicator of transformational change is that the final outcome may not be known at the beginning, the transformations may ultimately take the organization to a place that no one foresaw. One of the underlying reasons for this change in organizational structure was to facilitate better communication and information sharing between the Operation and Marine Safety communities. It is that same information sharing that this research is trying to promote, only on an even broader scale.

The implementation of this proposed system is not a transformational change. The fundamental business being conducted is the same. It is somewhat of a fuzzy line where this change does fall- somewhere between developmental and transitional. It is somewhat developmental in that it is just a modification of a currently employed process. But it is transitional in that it involves the introduction of a completely new technology and brings into play new participants who are now active players in the mission. This implementation should be characterized as a transitional change. This knowledge yields

several insights for the change management strategy. First, there is the reality check of taking a look at the big picture- is this type of change what is desired to be implemented? Or, should a more aggressive, transformational change be pursued instead? Second, this knowledge gives us a better understanding of the resistance to be expected. Using this quick “gut check” to assess the change strategy leads to the conclusion that (1) transitional change seems right and (2) the Coast Guard is likely to experience moderate to low resistance during this change. With this information, planners can now set out to establish a change management plan.

D. DEVELOPING A CHANGE MANAGEMENT PLAN

In his work on leading change, John Kotter lays out 8 steps that are instrumental in carrying out a successful change (Kotter 1995). These are:

- Establish a sense of urgency
- Forming a powerful guiding coalition
- Creating a vision
- Communicating the vision
- Empowering others to act on the vision
- Planning for and creating short term wins
- Consolidating improvements and producing still more change
- Institutionalizing new approaches
- We will outline our strategy using this framework.

1. Establish a Sense of Urgency

It is important to identify the factors that are driving this change. Change is most successful when driven by a crisis, which enables the organization to see the need clearly and be less likely to resist. The crisis has been pre-defined for us by 9/11 and the subsequent need for better, faster, and more reliable information exchange to increase our operational effectiveness and avoid major Weapons of Mass Destruction (WMD) disasters. The organization has a good feeling for this urgency, so we must simply make sure the connection between this change and that urgency is clearly articulated.

2. Forming a Powerful Guiding Coalition

It is important to have a group to serve as change agents and work to lead the change effort. As in the first step, we are fortunate to have this step already taken to some degree by the Program Executive Office staff of Deepwater, the Coast Guard's major recapitalization project. The Integrated Deepwater System transition is a symbiotic program to this one and will aid in acceptance of this new technology. The concepts of Net-Centric Warfare have already been introduced to the organization at large. The Program Executive Officer for Deepwater is serving as the change agent for that program, and his support will clearly aid in the acceptance of this system. With the larger scale change of adding new cutters and improved communications people are already aware of the Net-Centric Warfare concept, so it is not a completely foreign idea.

3. Creating a Vision

Deepwater has established a vision of an integrated C4ISR system that implements Net-Centric Warfare concepts. This thesis and experimentation serve as the first steps to setting a vision for the future in the small piece of the overarching Deepwater system.

4. Communicating the Vision

The Coast Guard must take an active role to get the new vision, and the great upside benefits, out to the organization. The vision needs to be marketed to the fleet. This entails keeping units well informed of the vision and progress we make towards achieving it. They can also grow acceptance and understanding for the vision by getting into the curriculum at Maritime Law Enforcement School with training the students on how to use the system. The current Law Enforcement Training Teams that tour units annually for training assistance should be well schooled on the vision and operation of this new technology, and then they will serve as additional change agents communicating the vision.

5. Empowering Others to Act on the Vision

The Coast Guard must get rid of obstacles to change and set the table for the organization to succeed with this new system. This change management strategy has been developed to do just that.

6. Planning for and Creating Short Term Wins

Once again the Coast Guard benefits from Deepwater assistance here. There is leverage to be gained by introducing this wireless networking concept with teams, ships, or stations have begun implementing C4ISR systems from Deepwater that are attempting to work towards Net-Centric Warfare. Additionally, units that have already begun using the PDA application for submitting boarding reports will also likely adapt to this system more easily. These users are already exposed to technology in the boarding arena, so the added step of wireless networking and collaborative information sharing will be a smaller, transitional change for them. By initiating the system deployment at units such as these, we increase our opportunities for successful short term wins through early successes.

7. Consolidating Improvements and Producing Still More Change

This step is accomplished by the development of employees who can successfully implement the new vision. Later in this chapter, we suggest a solution to improving the personnel allocation to better set small units up for success by adding technically rated personnel to their overly operational staffs. The Coast Guard will also succeed here by maintaining emphasis on this project throughout its infancy, with frequent reinvigoration with upper level support and an active management of the change plan.

8. Institutionalizing New Approaches

The Coast Guard accomplishes the institutionalization of these new processes by highlighting the successes as they occur and building upon them. There are clearly many more applications that can be leveraged, beyond those suggested here, to use this network to the Coast Guard's advantage and improve their overall operational effectiveness.

E. LEADING CHANGE

1. Dissatisfaction x Model x Process

Now that we have established the overarching plan for change, we need to look at specific areas that can be targeted by managers and change agents to facilitate the successful implementation of this change.

The following conceptual formula has been suggested to convey the critical factors that must be taken into account by managers in a change. (Beer 1988)

Amount of Change = (Dissatisfaction x Model x Process) > cost of change

Table 3. Change Formula (From: Beer 1988)

The overall meaning of the formula is that the Dissatisfaction with the current system, the Model of the future, and the Process must provide more than the cost of the change take away- otherwise the change will probably fail.

Therefore, we need to maximize the left side of the equation while doing what we can to minimize the right side in order to make the change work. First, we must highlight the dissatisfaction for the organization with the status quo. It is not readily apparent that there is a crisis, as we have identified, that needs to be solved. The change agents must seek to communicate the weaknesses of the current system in order to fuel their dissatisfaction. Illustrating the strong model of the future will be simple once units are able to get their hands on the new system and quickly realize the benefits with real time situational awareness and video, voice, and data transfer.

Illustrating the dissatisfaction with the current system can also be accomplished by showing some of the benefits of the new system. With the current slow pace of information feedback that occurs because of the lack of connectivity, boarding teams have two options when awaiting results of an intelligence check, radiation sensor evaluation, or other information request: (1) they can remain on board the subject vessel for an extended period of time, effectively wasting valuable time and running up very high opportunity costs by not boarding other vessels, or (2) they can leave the vessel and continue on with their mission. If indeed the information request eventually comes back positive warranting further action, the team must relocate and re-board the subject vessel. Neither option is appealing. The first option is clearly bad. There are an insurmountable number of contacts the Coast Guard must identify, prioritize, and board in every port. Wasting any time on one contact seriously detracts from our overall effectiveness. With

the second option comes the clearly underappreciated difficulty of re-boarding a vessel when information finally returns to a Law Enforcement unit after a long delay. It is a very awkward situation in which the stress levels are raised on both sides since the vessel crew obviously knows we are coming back for a reason and can increase potential problems. This results in a significantly higher level of hostility and danger on the boarding. The near real-time communication of this wireless system can help ameliorate both of these potential negatives.

The change plan is the process, and must be communicated to the fleet. One early step of the plan is to establish several front running test platforms, preferably at units that have shown a good acceptance of new technologies. Once people see early successes and the benefits of the technology, they will be more apt to buy into the system.

The Coast Guard can also communicate the big benefits of the system to show the gains that we will achieve such as the increased speed of the battle rhythm and information transfer with involved organizations and the added capabilities for interaction with outside agencies to increase operational effectiveness.

2. Cost of Change

The cost of change is normally measured by the losses that the organization will anticipate as a result of the change. There are several losses that can be measured.

Loss of Power. There is not much threat in this area. The main concern is that Boarding Officers may begin to feel that they are losing responsibility as law enforcement leaders by having the chain of command monitoring their efforts so closely in near real time. This same concern could be applied to Commanding Officers in respect to their concerns about the close oversight from their operational commander. To mitigate this fear of loss, we must stress the fact that oversight in this system is designed to add to the overall effectiveness of the organization, not detract from any individual's responsibility.

Loss of Competence. Many members may be intimidated by the computers and networking that are used in this new system. We can set ourselves up for success through the education of the users. Additionally, the infusion of more technical personnel

(discussed at length later in the chapter) at smaller units will aid in overall competence of the users.

Loss of Relationships and Rewards. We do not foresee any major pushback in this area. There are no major relationship changes foreseen in this implementation, so that should not be a major change hurdle.

F. MANAGING RESISTANCE

Resistance will be less if participants in any project see the change as reducing rather than increasing their current burdens (Bryant, Psychology of Resistance to Change, Management Services March 1979). That appears to be a likely scenario here. Instead of having to go through the tedious three-step process of recording boarding information on a paper form in triplicate, then entering information into a database upon return to the ship or port, then having to mail out the forms at the end of a patrol (which must be processed again at the District level of the organization). Our proposed system would enable data to be entered into a record by Boarding Officers during the boarding. Then, after validating the information, just one simple click will accomplish the goal of entering the information and putting it into the hands of the District. This should produce a reduction in overall effort. The key is to make sure the system works for the users. Even if the wireless network fails and all they have is electronic data entry, it is still a reduction of work since the Boarding Officers won't have to write it once and then type it all again later.

It will be important to point out to boarding teams and commands that this system is not intended to be a big brother watching over their every move. This system is about improving the capabilities of every boarding officer, giving them fast access to expert analysis and greatly improved intelligence and information support.

The redundant efforts of keeping a hard copy and an electronic copy often serve to undermine the work of change agents. If the users are required to duplicate their efforts, once on a hard copy form and once in the computer system, they will resent the extra work and get a feeling that management doesn't really trust the system anyway. If management doesn't think it is good enough, then why should I use this new system?

G. GIVING PERSONNEL THE KNOWLEDGE TO SUCCEED – ADDING IT PERSONNEL TO SMALL UNITS

1. Sociotechnical Systems Design Theory

In his Sociotechnical Systems Design, William Pasmore lays out several design principles to facilitate making a technical system work better. (Pasmore 1978)

- People are multi-skilled, understand the technology and are aware of how their work affects the quality of the end product.
- Problems are identified and solved at the point of where they occur, by those who actually do the work. People feel ownership for their technology and are able to maintain it under normal conditions.
- Boundaries are drawn and the physical layout arranged so that people who are responsible for completing whole interdependent tasks work together.

The crux of these principles is that we must make sure that personnel have the knowledge to use the technology and succeed. It must be there equipment and they must understand it. In order to successfully achieve this, the Coast Guard needs to put more technical personnel on the front lines of operations, so that they may participate and assist with the maintenance and operation of the technology.

Specifically, this means the Coast Guard would likely benefit from adding more Information Systems Technicians (IT Petty Officers or ITPO's) to smaller operational units, which will result in improved performance with this system as well as other higher technology systems installed on those smaller units. These technically rated personnel are able to work on the equipment and make sure it performs correctly for the operators, and even be the operators in many instances. ITPO's will serve as change agents to a degree, since they will keep systems operational avoiding the reversion to old school methods.

The current staffing and job requirements of 110' Patrol Boats shows how well an ITPO would fit into and benefit the unit. There are many technically oriented jobs on the increasingly technical cutters that are currently carried out by operationally oriented

Boatswain Mates. Jobs such as operation of the Satellite Communications equipment, Computer System Manager, Electronic Charting maintenance, Radar operation and maintenance, High Frequency Data Exchange message communications management, Information Systems Security Officer duties, and COMSEC Material Security duties are all generally currently collateral responsibilities of Boatswain Mates. While this cross training is good for the development of those Boatswain Mates, the organization would be better served by staffing patrol boats with an ITPO to take over all of those jobs as primary duties.

2. Information Systems Technician Rated Personnel

What does an ITPO offer? The Coast Guard web site (uscg.mil) has a general job description of the Information Systems Technician rate:



The Information Systems Technician (IT) Rating is responsible for establishing and maintaining Coast Guard systems that collect, store, process and forward all voice, data and video information. This includes the hardware and software used to process information. Members of the IT rating are responsible for supporting Coast Guard computer systems, analog and digital voice systems (telephones and voice mail) and are responsible for the installation and maintenance of the physical network infrastructure that ties the systems together. In addition, members of the IT rating at sea support tactical command, control, communications and computer systems being used to accomplish the Coast Guard's cutter missions.

With the ever increasing implementation of technology at Coast Guard units, ITPO's are becoming more and more necessary at smaller units. Every Coast Guard station uses advanced electronics, telecommunications and computer systems. This one example of a 110 patrol boat crew with a technical rating shortfall is present at many other stations and cutters. The new rate of Information Systems Technician is growing, and with the great amount of IT growth still coming in the future, it would greatly benefit the Coast Guard to continue to expand the strength of this technical rate.

H. CONCLUSION

We must sell the problem, not just the solution. We must focus on the fact that this is not just adding a new technology gizmo into the already cluttered e-portfolio of operators. This is an increase to our operational effectiveness, made necessary by the rapid rate at which we must have information to successfully carry out both law enforcement and homeland security missions. We must allow people to see what the future looks like when our collaborative systems are successfully networked.

The recent publication America's Coast Guard states details the command and decision shortfalls of our current systems:

The lack of capability to maintain situational awareness and effective tactical display of an area of responsibility at the District or Group level, including status of reporting resources and monitoring of actions of Coast Guard resources has continued to create problems for effective force allocation. This, plus a general lack of interoperable decision support tools, effective situational risk assessment tools, and access to remote mission reporting information at Groups, has at times resulted in an inability to maintain situational awareness and effective tactical display by units involved in Joint-force operations. Similarly, there is a general inability to provide real-time tactical information and a situational picture on aircraft, small cutters and boats, and at Small Boat Stations. The Coast Guard cannot easily share tactical information effectively on a real-time basis among disparate levels of Coast Guard resources and with other agencies and private organizations. Finally, the limited capability to collect data effectively and to evaluate the effectiveness of operations can either result in too many assets being allocated or too few, as well as decisions to call off operations prematurely. (Stubbs 2000)

The problem is real. In the new reality of our post 9/11 world, we cannot afford to make mistakes with the positive identification of a suspected terrorist. Real-time connectivity to intelligence sources will enable boarding teams to transmit photos along with names for analysis and verification. This system gives them that power.

We can neither afford to let a dirty bomb or other radioactive material come into one of our busy ports or cities. We need the capability to detect and analyze the technical readings from sophisticated detection equipment used for this purpose. This system gives them that power. It leverages technology to make boarding teams better, more in touch with information, and enables them to get important answers quickly.

This system can provide significant benefits to Coast Guard operations. The marketing of this system should be such that it highlights the fact that this is not just nice to have change, this is necessary change. We cannot afford to not leverage this technology to help us do our jobs better.

With any major change it is critical to have a change strategy to increase the odds of success. This change management strategy can and will succeed in its implementation of this new, beneficial technology.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. Collaborative Software Tools

The Groove Virtual Office and the Situational Awareness (SA) Agent collaborative software tools worked well for their purpose in this experimentation. Each system has its own benefits that it provides to Coast Guard operators and mission planners. Groove provides an excellent system for secure file transfer, whiteboard, chat and other beneficial collaborative tools. SA Agent provides real-time video and position information of assets and targets to greatly enhance overall situational awareness of users. While each system has unique assets, we were able to successfully use both systems simultaneously over the experiment network, showing that they can be used in concert gaining the benefits from each system. The combination of both tools created a very good Common Operating Picture (COP) for our near shore operating unit and the shore-side Operations Center.

While this thesis research was focused on the specific Coast Guard missions of Law Enforcement and Homeland Security, the use of Collaborative tools such as Groove and SA Agent seem to have applicability to most, if not all, missions. The collaborative planning tools lend themselves well to development of plans and carrying out actions by geographically dispersed units, whether at sea or at shore-side command centers. Search and Rescue and Environmental Response mission planning and execution both quickly come to mind as areas that would benefit from the use of a collaborative work environment such as Groove especially.

In order to gain full benefits of the COP and situational awareness features of this architecture, the wireless network must also be implemented. However, absent any acceptance of the wireless networking aspect of this thesis, we still recommend that the Coast Guard begin implementing widespread usage of Groove Virtual Office collaborative system in Operations Centers and staffs now. The use of a collaborative system provides good organization, status monitoring, resource maximization, and planning capabilities for any project- or case-based work group. The geographically

diverse units of the Coast Guard would likely benefit greatly from the enhancement of creating shared workspaces for specific project and operations. Specifically, we feel the immediate implementation of Groove in the Command/Operations Center hierarchy (Stations, Groups, Districts, and Areas) would greatly improve information sharing and increase situational awareness up and down the chain of command.

As side note, Groove Networks has recently announced that the company has been acquired by Microsoft Corporation and that the Virtual Office will be integrated into the Microsoft Office system of products. Since the Coast Guard already uses Microsoft Office as the desktop productivity software for their Standard Workstation III, the near-term integration of Groove Virtual Office into the system image for planning activities would be a logical and productive step.

2. 802.11 Mesh Network

Through our testing and experiment, we consistently found that the 802.11 mesh network did not have a consistent behavior pattern that would instill confidence in operators. The frequency is very susceptible to interference on a Coast Guard unit resulting in a network that is too fragile to be recommended for operational use.

3. 802.16 Wireless Network

The 802.16 segments of the network performed very well and warrant further investigation into how to better leverage this technology (see Recommendations below). The 802.16 technology provides higher throughput, more reliable performance in the outdoor environment, and greater distance coverage than 802.11.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

1. Redline AN-50e 802.16 Manpacks

Concurrent research going on with the Tactical Networking Topology experiments involving 802.16 Manpacks appears to be a very promising technology that would fit well into the Coast Guards requirements. The Manpacks are Redline AN-50 units that have been (1) ruggedized, (2) had a small antenna directly attached, (3) modified with an attached power supply, and (4) designed with shoulder straps to be worn as a back pack. This implementation of the mobile 802.16e technology appears to fit in very nicely work with the goals of this thesis. Based on our limited analysis of the ongoing work with this hardware, it appears to provide a better solution than the use of

the 802.11 technology for communications between cutters and their boarding teams. Follow-on work integrating these units into the Coast Guard at-sea scenario is warranted.

2. Adjustable Sector Antennas

Another area where the current network status could be improved is by adding directional antennas onto the cutter to increase range from shore capabilities. The current configuration of a 60 degree sector on the beach and an omni directional antenna on the ship has provided coverage out over 10 kilometers in experimentation. By installing a directional antenna with higher gain on the cutter ,with some type of motor or control to adjust the direction toward the beach tower, we could theoretically increase the range within which the cutter could maintain connectivity.

3. Port Entry Placement of 802.16 Antennas

Wireless networking and specifically 802.16 appears to be a very promising technology. The success of this research has created the thought of the Coast Guard installing 802.16 sector antennas at the mouth of every major port. We believe the feasibility of such a project should be investigated. This would enable Marine Safety Officers, Marine Safety and Security Teams, Small Boat Stations crews and other shipriders to have relatively inexpensive network connectivity back to shore commands through this type of network, extending connectivity several miles out in every major port. Supplied with the hardware and software described in herein, these units could be given the required connectivity to reap the benefits of the capabilities described in this thesis- enhancing the Coast Guard's ability to carry out their Law Enforcement and Homeland Security missions today rather than tomorrow. While this does not push our borders out as far as we'd prefer it is clearly an advantage over the status quo of having boarding teams board ships dockside and only then discover the presence of radioactive material or known terrorists.

Furthermore, from a speculative viewpoint, wireless technology has advance very rapidly in the past few years, it is very likely that coverage ranges could drastically increase in the near future extending this type of economical network even farther offshore. This type of network very likely has a place in the Coast Guard's area of operations.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

- Ackerman, Linda. 1986. *Development Transition or Transformation: The Question of Change in Organizations*. O.D. Practitioner, December 1986.
- Anderson, CDR Michael and Winterstine, Bruce. 2004. *A Network-Centric Approach to Maritime Domain Awareness*. Presented to American Society of Naval Engineers June 2004. Available at <http://www.uscg.mil/deepwater/media/articles.htm>. Last Accessed March 2005.
- Bach, Eric J. and Fickel, Mark G. 2004. *An Analysis of the Feasibility and Applicability of IEEE 802.X Wireless Mesh Networks Within the Global Information Grid*. Master's thesis, Naval Postgraduate School, September 2004.
- Beer, Michael A. 1988. *Leading Change*. Harvard Business School. President and Fellows of Harvard College.
- Blazevich, Ryan J. 2004. *Wireless, Long Haul, Multi-Path Networking: Transforming Fleet Tactical Network Operations with Rapidly Deployable, Composable, Adaptive, Multi-Path Networking in Austere Environments*. Master's thesis, Naval Postgraduate School, September 2004.
- Bordetsky, A., S. Hutchins, W. Kemple and E. Bourakov. 2003. Network Aware Tactical Collaborative Environments. *Proceedings of the Ninth International Command and Control Research and Technology Symposium*, 14 September 2004.
- Clarke, Kurt and Campen, Andrew. 2002. *Satellite Communications for Coast Guard Homeland Defense*. Master's thesis, Naval Postgraduate School, March 2002.
- Coast Guard Commandant Instruction Manual 16247.1C. *Maritime Law Enforcement Manual*. Revision August 2003.
- Coast Guard Commandant Instruction Manual 16247.4. *Maritime Counter-Drug and Alien Migrant Interdiction Operations*. Revision May 1999.
- Coast Guard Deepwater home page. Available from <http://www.uscg.mil/deepwater/resources/resources.htm> Last Accessed March 2005
- Coast Guard fact file. *Average Day – Coast Guard*. Available at <http://www.uscg.mil/hq/g-cp/comrel/factfile/index.htm> Last Accessed March 2005.
- Cohen, Beth and Deitsch, Debbie. *The Future in Last Mile Wireless Connectivity*. Available at http://www.wi-fiplanet.com/tutorials/article.php/10724_3065261_2802.16: Last Accessed March 2005

- Collins, ADM Thomas H. 2003. *The Integrated Deepwater System: The Coast Guard's Closest Point of Approach to Maritime Homeland Security*. Sea Power, April 2003, p. 39.
- Comer, Douglas. *Computer Networks and Internets, with Internet Applications*. Upper Saddle River, NJ: Prentice Hall, 2001.
- Department of Defense Directive 8100.1. *Global Information Grid Overarching Policy*. Dated 19 September 2002.
- Department of Defense. *Global Information Grid (GIG) Architecture Master Plan*. 29 November 2002.
- Groove Networks. *Groove Networks Announces Third-Generation Developer Offerings*. Available at http://www.groove.net/PressRelease.cfm?pagename=press_May12_2004 Last Accessed April 2005.
- Groove Networks. 2004. *Groove Security Architecture*. Available at <http://www.groove.net/pdf/security.pdf#search='Groove%20security%20architecture'> Last Accessed March 2005.
- Groove Networks. 2004. *What's New In Groove Virtual Office*. Available at http://www.groove.net/pdf/backgrounder/whats_new_in_GVO.pdf Last Accessed March 2005.
- Groove Networks. *System Requirements*. Available at <http://docs.groove.net/htmldocs/readme/sysreq.html> Last Accessed March 2005.
- Groove Virtual Office home page. Available from <http://www.groove.net/> Last Accessed March 2005.
- Hall, RADM James. 2005. *Integrated Deepwater System*. Adapted from Brief given to International Maritime Security Conference in Copenhagen.
- Hayes-Roth, Rick. *Model-based Communication Networks: Filtering Information by Value to Improve Collaborative Decision Making*. Unpublished paper dated 9 July 2004
- Jick, Todd J. 1989. *Note: The Challenge of Change*. Harvard Business School. President and Fellows of Harvard College.
- Kotter, John P. 1995. *Leading Change: Why Transformation Efforts Fail*. Harvard Business Review March-April 1995.
- Nation Labs Manual UCRL-PRES-205098. 2004. *Coast Guard Radiation Detection Training*– Chapter 6 B-1, Savannah River National Laboratory and Lawrence Livermore National Laboratory.

- Lockheed Martin Press Release. 2003. *Deepwater Team Delivers First Cutter-Based Communications System Upgrade to U.S. Coast Guard*. November 3, 2003.
- Motorola Mesh Networks home page. Available at http://www.motorola.com/businessandgovernment/northamerica/en-us/public/functions/browsesolution/browsesolution.aspx?navigationpath=id_804i/id_2523i Last Accessed March 2005.
- Nacarra, George. 1998. *U.S. Coast Guard Information Technology Strategy*. Available at <http://www.uscg.mil/ccs/cit/Docs/itstrgy.pdf> Last Accessed March 2005
- Pasmore, William and Sherwood, John. 1978. *Sociotechnical Systems: A Source Book*. Pfeiffer and Company. Information adapted from presentations slides copyrighted by Pasmore & Associates 1989.
- Proxim Wireless Networks. Orinoco 11b Client PC Card Data Sheet. Available at <http://www.proxim.com/learn/library/datasheets/11bpccard.pdf> Last Accessed March 2005.
- Hamilton, AlexanderPublius, The Federalist Papers (No. 12), *The New York Packet*, November 27, 1787.
- Redline Communications home page. Available from <http://www.redlinecommunications.com> Last Accessed March 2005.
- Redline Communications White Paper. *Advantages of Broadband Fixed Wireless Systems over 802.11 LANs* Available from http://www.redlinecommunications.com/tech/whitepapers/Redline_FW_vs_802.pdf Last Accessed March 2005.
- Redline Communications. *AN-50e Product Data Sheet*. Available from <http://www.redlinecommunications.com/products/an50/an50e.pdf> Last Accessed March 2005.
- Stillman, Rear Adm. Patrick M. 2003. *The Coast Guard's Integrated Deepwater System: Transforming America's Sentinels of the Sea*. Naval Forces, Vol. IV, April 2003, p. 97.
- Stubbs, CAPT Bruce and Truver, Scott C. 2000. *America's Coast Guard: Safeguarding U.S. Maritime Safety and Security in the 21st Century*. U.S. Coast Guard publication.
- Suitor, Kevin F.R. 2004. *From "a" to "e": The 802.16 Standard Evolution*, Redline Communications White Paper. July 2004. Available from http://www.redlinecommunications.com/tech/whitepapers/From_A_to_E_Aug_2004.pdf Last Accessed March 2005.

Suitor, Kevin F.R. 2004. *What WiMAX Forum Certified™ products will bring to Wi-Fi™*
Redline Communications White Paper. June 2004.
http://www.redlinecommunications.com/tech/whitepapers/WiMAX_wifi_June_2004.pdf Last Accessed March 2005.

Webopedia home page. Available at <http://www.webopedia.com/> Last Accessed March 2005.

Weisman, R. Groove Networks unexpectedly lands major customer: U.S. government.
The Boston Globe, 29 June 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Dan Boger
Naval Postgraduate School
Monterey, California
4. Alexander Bordetsky
Naval Postgraduate School
Monterey, California
5. Glenn Cook
Naval Postgraduate School
Monterey, California
6. Jadon Klopson
Naval Postgraduate School
Monterey, California
7. Stephen Burdian
Naval Postgraduate School
Monterey, California