



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**BOARDING TEAM NETWORKING ON THE MOVE:
APPLYING UNATTENDED RELAY NODES**

by

Ercan Aras

September 2014

Thesis Advisor:
Second Reader:

Alex Bordetsky
Steve Iatrou

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2014	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE BOARDING TEAM NETWORKING ON THE MOVE: APPLYING UNATTENDED RELAY NODES			5. FUNDING NUMBERS	
6. AUTHOR(S) Ercan Aras				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____ N/A ____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) As gaps in maritime legislative domain enlarge, threats to our maritime-based global economy are on the rise. Terrorist organizations can leverage every loose policy to use international waters for transferring (weapons of mass destruction) WMDs or to sabotage global trade in choke-points. To prevent any threat posed by terrorist organizations, the enhancement of situational awareness in a maritime domain is crucial for international organizations and states. To prevent any threat in the outer-most perimeters, Maritime Interdiction Operations (MIO) are conducted to enhance situational awareness. Visit Board Search and Seizure (VBSS) constitutes a huge portion of the MIO. Instant communication between the MIO assets and reach-back operations centers plays a critical role both for decision makers to make the best immediate judgments, and for boarding team members to conduct boarding safely. Although networks can be extended to the vicinity of a target vessel, or even onboard, the steel structures of naval vessels obstruct signals to propagate below the main deck. Extending the network below the main deck via a wireless ad-hoc network will enhance the situational awareness. Regarding the boarding of a non-compliant vessel, tracking positions of boarding team members and sustaining reliable and scalable communication links are essential in preventing hostile actions and enhancing reaction time.				
14. SUBJECT TERMS Maritime Interdiction Operations, Boarding Team Networking, Unattended Relay Nodes, Wireless Mesh Networks Onboard Ships, Mobile Ad-hoc Networks Onboard Ships			15. NUMBER OF PAGES 71	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**BOARDING TEAM NETWORKING ON THE MOVE: APPLYING UNATTENDED
RELAY NODES**

Ercan Aras
Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS
ENGINEERING**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2014**

Author: Ercan Aras

Approved by: Alex Bordetsky, Ph.D.
Thesis Advisor

Steve Iatrou
Second Reader

Dan Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As gaps in maritime legislative domain enlarge, threats to our maritime-based global economy are on the rise. Terrorist organizations can leverage every loose policy to use international waters for transferring (weapons of mass destruction) WMDs or to sabotage global trade in choke-points. To prevent any threat posed by terrorist organizations, the enhancement of situational awareness in a maritime domain is crucial for international organizations and states.

To prevent any threat in the outer-most perimeters, Maritime Interdiction Operations (MIO) are conducted to enhance situational awareness. Visit, Board, Search and Seizure (VBSS) constitutes a huge portion of the MIO. Instant communication between the MIO assets and reach-back operations centers plays a critical role both for decision makers to make the best immediate judgments, and for boarding team members to conduct boarding safely.

Although networks can be extended to the vicinity of a target vessel, or even onboard, the steel structures of naval vessels obstruct signals to propagate below the main deck. Extending the network below the main deck via a wireless ad-hoc network will enhance the situational awareness. Regarding the boarding of a non-compliant vessel, tracking positions of boarding team members and sustaining reliable and scalable communication links are essential in preventing hostile actions and enhancing reaction time.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	OVERVIEW	1
B.	BOARDING.....	6
C.	PROBLEM STATEMENT.....	7
D.	THESIS OUTLINE.....	7
II.	ANALYSIS OF MIO AND BT NETWORKING	9
A.	OVERVIEW	9
B.	REQUIREMENTS FOR MIO BT NETWORKING.....	10
1.	Safety of Personnel	11
2.	Ease of Transportation.....	11
3.	Reliable, Robust, and Scalable Communication.....	11
4.	Tracking Positions of All BT Members	12
C.	CHALLENGES.....	12
1.	Tracking Positions of All BT members	12
2.	EM Propagation Below Main Deck	12
D.	PROPOSED POSSIBLE SOLUTIONS	14
1.	Positioning	14
2.	Reliable Communication	17
III.	WIRELESS NETWORKS USED ONBOARD SHIPS WITHIN MIO AND BOARDING.....	21
A.	OVERVIEW	21
B.	WIRELESS MESH NETWORKS.....	22
1.	Challenges.....	23
a.	<i>Throughput Degradation and Unfairness</i>	<i>23</i>
b.	<i>Resource Management.....</i>	<i>24</i>
C.	MOBILE AD-HOC NETWORKS	24
1.	Security	25
2.	Routing	25
a.	<i>Proactive.....</i>	<i>25</i>
b.	<i>Reactive</i>	<i>26</i>
c.	<i>Hybrid:</i>	<i>26</i>
D.	DIFFERENCES BETWEEN VMNS AND MANETS	26
E.	INTERNET CONNECTION FOR MANETS.....	27
IV.	EXPERIMENTATION FIELD	29
A.	CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX).....	29
B.	MIO WMD-ISR EXPERIMENTS IN ALAMEDA, CA (AUGUST 10–15, 2014).....	31
1.	Objectives of Experiment.....	31
2.	Scenario.....	32
3.	Experiment Setup	32

4.	Boarding Team Networking	34
5.	Evaluated WMN/Mobile Ad-Hoc Systems	35
a.	<i>Wave Relay Mobile Ad-Hoc System</i>	35
b.	<i>Trellis Ware Mobile Ad-Hoc System</i>	36
c.	<i>Virtual Extension Wireless Mesh System</i>	37
d.	<i>Measurement Tools Used</i>	38
V.	CONCLUSION AND RECOMMENDATIONS	47
	LIST OF REFERENCES.....	49
	INITIAL DISTRIBUTION LIST	53

LIST OF FIGURES

Figure 1.	International Seaborne Trade (millions of tons) (from [2])	2
Figure 2.	Chokepoints and Maritime Trade Routes (from [4]).....	4
Figure 3.	Increased Maritime Threat (from [3])	5
Figure 4.	Container, Bulk Carrier, Tanker (from [7])	9
Figure 5.	Ferries, Cruise and Specialist Ship (left to right) (from [7])	10
Figure 6.	Reflection, Diffraction (left one from [11], right one from [12])	13
Figure 7.	Heading Estimation (from [14]).....	15
Figure 8.	Positioning by Trilateration (a) Desired (b) Imperfect (from [15]).....	17
Figure 9.	WLAN Propagation within Bridge Compartment (from [11])	18
Figure 10.	WLAN Propagation from Outside to Inside (left) within the Bridge (right) (from [11]).....	18
Figure 11.	Classification of Multi-hop Wireless Networks (from [18]).....	22
Figure 12.	MANET Architecture for Internet Connection (from [21])	28
Figure 13.	MIO Test bed, SF Bay , East Coast and Overseas (from [23]).....	30
Figure 14.	CENETIX Resource Portal (from [24]).....	31
Figure 15.	Link between YBI Tower and USNS Cape ORLANDO.....	33
Figure 16.	Sector Antenna Array Onboard SFPD Boat (from [26]).....	34
Figure 17.	USNS Admiral Callaghan Deck-1 Measurement Segments	34
Figure 18.	MPU4 Specification (from [27]).....	36
Figure 19.	TW-220 Performance Parameters (from [28])	37
Figure 20.	VEmesh Node and 4 Hops Networking Through and Obstacle (from [29]).	38
Figure 21.	Qcheck NPM Tool(left) and Node Ping Graph Tool (right)	39
Figure 22.	Phase-I (Securing the Ship) Measurement Stations.....	40
Figure 23.	Main Deck Search Pattern.....	41
Figure 24.	Second Deck Search Pattern	41
Figure 25.	Third Deck Search Pattern	41
Figure 26.	Fourth (left) and Fifth (right) Decks Search Pattern.....	42
Figure 27.	Virtual Extension Mesh Network.....	43
Figure 28.	Wave Relay (blue nodes), Trellis Ware(red nodes) Networks	44

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Long-Term Trends in Cellular Container Shipping (from [2])	3
Table 2.	Flags of Convenience Registration (from [2])	3
Table 3.	Experimental Results for Kothari (from [14]).....	16
Table 4.	MANET Enabling Technologies (from [19])	22
Table 5.	Throughput Degradation in WMN (from [18])	23
Table 6.	Differences Between MANETs and WMNs (from [18])	27
Table 7.	Measurements of First Phase for Wave Relay	40
Table 8.	Measurements of Main Deck-1	42
Table 9.	Measured Metrics of Network.....	44

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BT	Boarding Team
C2	Command and Control
CENETIX	Center for Network Innovation and Experimentation
dB	Decibel
dwt	Deadweight Tonnage
EM	Electromagnetic
GPS	Global Positioning System
LAN	Local Area Network
IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
LLNL	Lawrence Livermore National Laboratory
MAC	Medium Access Control
MANET	Mobile Ad-Hoc Networks
MIO	Maritime Interdiction Operations
MPU	Man Portable Unit
NATO	North Atlantic Treaty Organization
NOC	Network Operations Center
OSI	Open Source Initiative
RHIB	Rigid Hull Inflatable Boat
SFPD	San Francisco Police Department
TEU	Twenty-Foot Equivalent Unit
TNT	Tactical Network Topology
TW	Trellis Ware
UDP	User Datagram Protocol
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
USCG	U.S. Coast Guard
VBSS	Visit, Board, Search, and Seizure
VE	Virtual Extension
VPN	Virtual Private Network

WMD	Weapons of Mass Destruction
WMN	Wireless Mesh Network
WR	Wave Relay

ACKNOWLEDGMENTS

I am always proud to be a member of my nation and my service. I would like to express my gratitude to the leadership of Turkish and U.S. navies who provide this unique opportunity that was funded by taxpayers of both countries. The future lies on our hands. The smarter and stronger we are, the more peaceful and prosperous the world will be.

Also, I would like thank to Professor Alex Bordetsky and Eugene Bourakov for their assistance and mentorship.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Globalization in the twenty-first century has led to significant changes in human life and interactions among societies. While free movement of goods increased prosperity, growing complexity of global commerce poses new challenges that generate potential threats for both state and non-state actors.

Statistics show that in a world of 70% water coverage, “80% of the world’s population lives within 100 miles of the coast; 90% of the world’s commerce is seaborne, and 75% of that trade passes through a few, vulnerable, canals and international straits” [1]. Moreover, according to the International Maritime Organization (IMO), in the last two decades there has been a three-fold increase in global seaborne trade. (Figure 1) [2]. This extreme enhancement of world trade through the maritime environment reduced unit selling prices of common goods to an affordable amount for almost everyone in the world, despite the stable production overheads. International/Multinational companies built sophisticated trade networks all over the world based on low transportation costs. Competitive environments drove companies to keep shipping costs low.

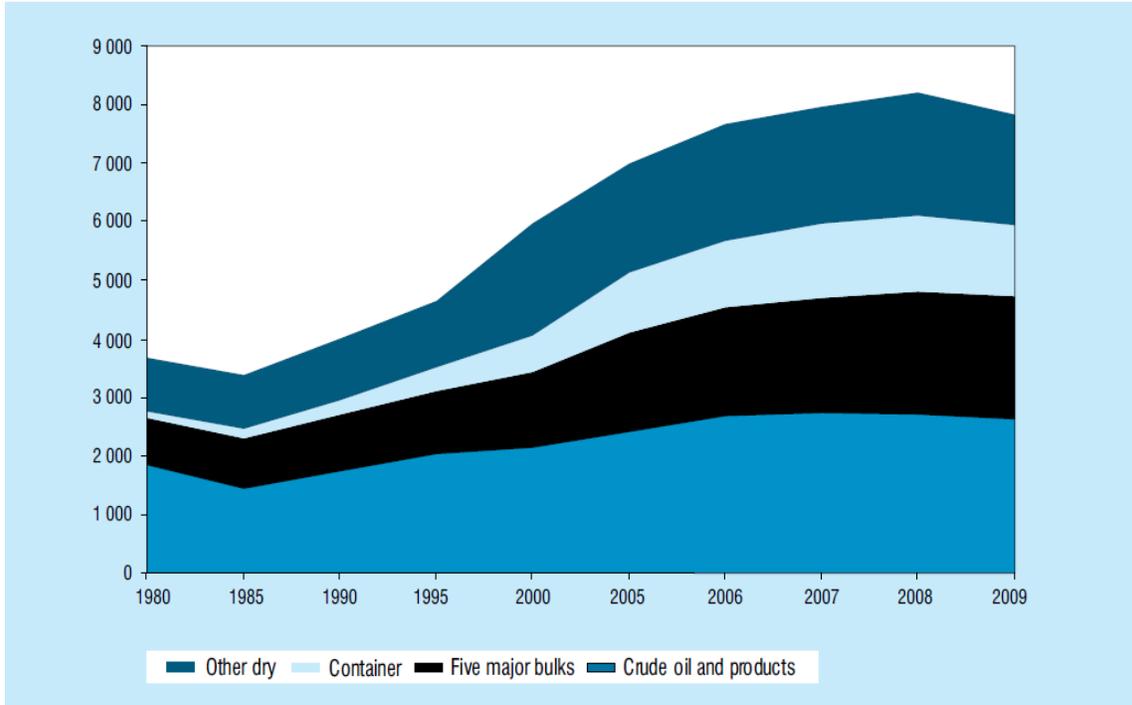


Figure 1. International Seaborne Trade (millions of tons) (from [2])

By 2010, containerized cargo generates one eighth, while crude oil generates almost half of all transported materials. In the last two decades, there have been massive increases in containerized cargo that drove construction of container ships. World container ship fleets have grown approximately seven times, and the carrying capacity of the world's container fleets has increased to 108 million dwt [2]. Based on volume/tonnage, bulk trade comprises a vast portion of world trade, while by economic value containerized goods form the largest portion [3]. Although economical value containers are most often used, compared to other materials that are transported by bulk carriers or tankers, they are the most difficult to inspect for several reasons. By 2010, the capacity of the world's container fleet was almost 13 million twenty-foot equivalent units (TEU) (Table 1). Even though states break the back of technological and logistical obstacles to inspect all containers, it is neither feasible nor economical to inspect every container entering every port.

World total	1987	1997	2007	2008	2009	2010	Growth 2010/2009 (per cent)
Number of vessels	1 052	1 954	3 904	4 276	4 638	4 677	0.84
TEU capacity	1 215 215	3 089 682	9 436 377	10 760 173	12 142 444	12 824 648	5.62
Average vessel size	1 155	1 581	2 417	2 516	2 618	2 742	4.74

Table 1. Long-Term Trends in Cellular Container Shipping (from [2])

Metaparti described the reasons behind the increased maritime threats into three categories in the article, “Rise of the Global Trade, Growth of the Shipping and Change in the Terrorist Mindset” [3].

As mentioned above, massive expansion of global sea-based trade has made significant changes in human interactions. Within this extreme expansion, the shipping industry evolves toward lucrative ways, bypassing expensive security measurements and regulations dictated by industrialized/developed states. To reduce costs and avoid imminent penalties, the shipping industry leans toward loose regulations. Open registry of the vessel, which means that the owner is not required to be a citizen of the flag state, was initiated in the 1960s by countries such as Panama and Liberia [3]. According to statistics published by the IMO, it is obvious that most of the vessels are currently registered under the flag of open registry countries (Table 2).

Flag of registration	Number of vessels	Share of world total, vessels	Deadweight tonnage, 1 000 dwt	Share of world total, dwt	Cumulated share, dwt	Average vessel size, dwt	Dwt growth 2010/2009, percentage
Panama	8 100	7.93	288 758	22.63	22.63	35 649	5.40
Liberia	2 456	2.40	142 121	11.14	33.76	57 867	12.80
Marshall Islands	1 376	1.35	77 827	6.10	39.86	56 561	13.70
China, Hong Kong	1 529	1.50	74 513	5.84	45.70	48 733	16.10
Greece	1 517	1.48	67 629	5.30	51.00	44 581	7.29
Bahamas	1 426	1.40	64 109	5.02	56.03	44 957	3.38
Singapore	2 563	2.51	61 660	4.83	60.86	24 058	1.42
Malta	1 613	1.58	56 156	4.40	65.26	34 815	10.84
China	4 064	3.98	45 157	3.54	68.80	11 112	12.90

Table 2. Flags of Convenience Registration (from [2])

Cargo that is carried by these ships has various owners from various nationalities. For instances a German ship owner can register a ship under the Panama flag, while the cargo on that ship can belong to a charity organization in South Africa, China, or Brazil. As Metaparti indicates, companies use registration flags of convenience to circumvent tax evasion and other responsibilities in case of a disaster such as an oil spill, or money laundering [3].

Besides these loose regulations and evasive policies, geographical bottlenecks and critical huge ports comprise other vulnerable parts of the maritime trade. As free trade increases, security controls over these maritime trade routes become more of an issue. Vessels that are in these ports or are transiting through these chokepoints are susceptible to terrorist attacks.

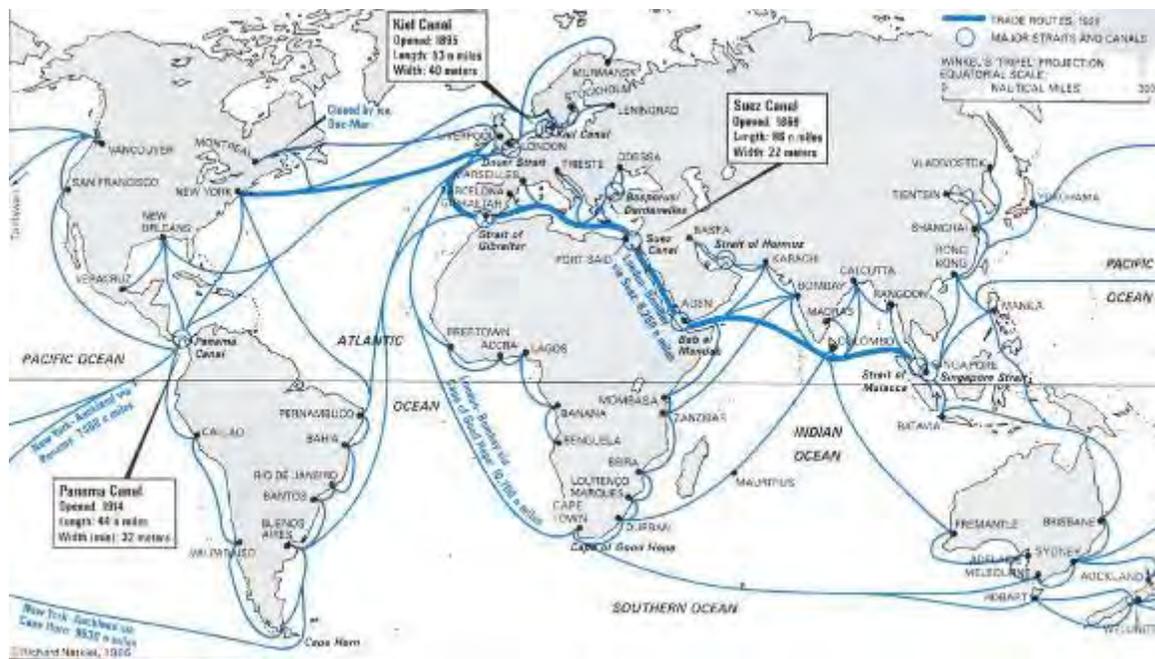


Figure 2. Chokepoints and Maritime Trade Routes (from [4])

Statistics published by the IMO about piracy reinforce the idea of increasing vulnerability of chokepoints. According to the IMO,

In 2009, a total of 406 incidents of piracy and armed robbery were reported, the highest figure since 2003 when the problem was at its

highest in the Straits of Malacca. It was also the third successive year that the number of reported incidents increased. Of these incidents, 217 were attributed to Somali pirates, with 47 vessels hijacked, and 867 crew members taken hostage. [2]

Considering all these factors, a maritime threat has evolved parallel to development of sea-based global trade. Poor regulations and lack of control over international waters push terrorist organizations to leverage these gaps. As Parker remarked during the 2011 U.S. Navy Seals operation to overtake al-Qaeda, there were indications that leaders of al-Qaeda developed plans to seize oil tankers to cripple the U.S. economy [4]. As a result of the rapid evaluation of global maritime trade without sufficient security controls, and the expansion of the shipping industry that leveraged loose regulations, massive gaps were generated that increased potential threats within an inherently ambiguous sovereignty of the maritime domain (Figure 3) [3]. Terrorist and illegal organizations are prone to leverage these gaps with the help of technological developments to harm or derail world economy. Thus, WMD, or materials to build these weapons, can be transferred without notice.

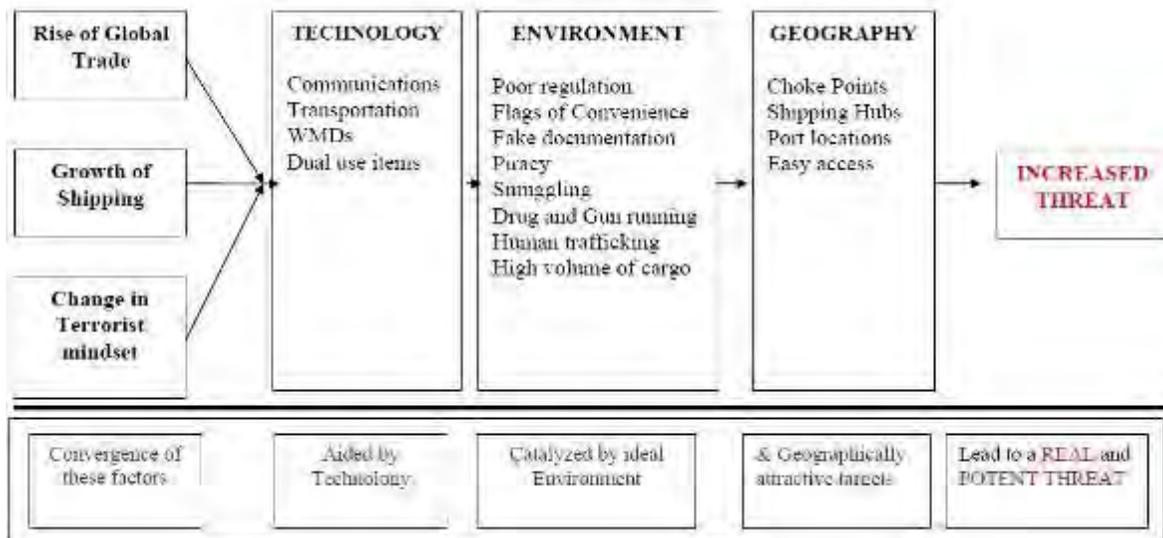


Figure 3. Increased Maritime Threat (from [3])

To prevent damages to global trade and to protect homelands, international organizations (i.e., UN, NATO), and developed states (U.S., Europe) seek to detain possible threats through defense-in-depth security perimeters. Oceans and seas are the most important domains of which they patrol and conduct reconnaissance. Through highly-qualified intelligence sources, these organizations can deploy naval warships to conduct seizures and searches, and are able to avert or destroy the threat at its origin. Therefore, instant and continuous maritime situational awareness has become a huge challenge for these organizations/states.

To be able to react instantly, decision makers need to reach the input data immediately. With current developments in technology, instant data-sharing networks are extended to most parts of world through satellites. Authorities can track or shadow any suspicious vessels or activities gathered by intelligence with either naval warships or Coast Guard cutters. However, to establish situational awareness for serious threats, authorities can order search and seizure of the target ship using professionally education boarding teams (BT). BTs are transferred to target ships with all necessary portable equipment, while reach-back networks via naval warships or cutters cover the BTs. Though networks can be extended to the ship that conduct the boarding; a lack of appropriate devices and the complex structure of ships can form a gap in communication between the BT and reach-back network operation center.

B. BOARDING

Boarding—Visit, Board, Search, and Seizure (VBSS)—is conducted at sea or in ports to prevent attempts to ruin stabilized global maritime-based economy, as well as to minimize risk of threats posed by terrorist organizations to a nation's sovereignty. There are two types of boarding: Compliant Boarding and Non-Compliant Boarding. They are defined by the United Nations as follows:

Compliant boarding is conducted in accordance with the rules of international law; that is with the consent of the ship's master and the flag State. [5]

Non-compliant boarding is conducted without the consent of the ship's master and the flag state, sometimes with the use of force and without legal authority. It is contrary to the principle of freedom of customary international law, codified by article 87 of the United Nations Convention on the Law of the Sea (UNCLOS). Non-consensual, or non-compliant boardings are only permitted in a limited number of cases (such as suspicion of piracy, slave trade, but not for anti-terrorism operations), defined by article 110 (right of visit) of UNCLOS. [6]

Sustaining a reliable and robust network that can be used to transfer data and voice between moving and stationary BT members, as well as within reach-back Network Operations Center (NOC), is vital and challenging. In a hostile environment, it is highly critical to keep communication alive and to transfer data instantly.

C. PROBLEM STATEMENT

Boarding team members conducting inspections onboard a ship, lack the ability to dynamically maintain and extend the network and to sustain connectivity for data and voice transmission between the team and within the reach-back NOC. Research questions to be investigated are:

- How can wireless relay nodes be used in a highly-reflective compartment below the main deck to sustain a reliable and continuous communication between all active BT members?
- What are the constraints and drawbacks to create such a robust dynamic mesh network onboard a ship?
- What is the throughput that can be maintained with current commercial off-the-shelf devices?
- What should the distance between two nodes be to sustain a reliable voice and data transfer?
- How many relay nodes will each boarding team member need to use to cover the boarded ship?

D. THESIS OUTLINE

This thesis is organized as follows. Chapter I presents the motivation behind this research with its scope. Chapter II analyzes BT (boarding team) networking requirements, challenges, possible solutions, and feasibilities.

Chapter III summarizes currently used wireless mesh technologies and protocols. Chapter IV illustrates and discusses the findings of an experiment conducted in Alameda, CA during August 10–15, 2014. Chapter V presents conclusions based on the findings of the experiment, and areas/questions for future research.

II. ANALYSIS OF MIO AND BT NETWORKING

A. OVERVIEW

Typically, BT members will include between two and eight members depending on the size of the ship or the expected threat level. Taking into account current vessels on a maritime domain, BTs can board various types of vessels over 600 feet. According to the IMO, by January 2011, there were 103,392 commercial ships in the world fleet registered in over 150 nations [2]. This massive fleet is categorized generally in five types of vessels. Container ships carry most of the world's manufactured goods and products (Figure 4). Bulk carriers transport raw materials such as grain, coal, and iron ore, and have the distinctive appearance of hatches extending above the main deck (Figure 4). Tankers transport crude oil products and liquid chemicals. Oil pipelines and vents on the deck create the main difference compared to bulk carriers (Figure 4). Ferries and cruise ships—most of which are Ro-Ro (roll-on-roll-off)—are used to transport passengers, cars, and commercial vehicles (Figure 5). Ice breakers, research vessels, and salvage tugs, supply vessels for the offshore oil industry, and form specialist ships (Figure 5). Other vessels, such as fishing vessels and yachts, are vulnerable due to their small size.



Figure 4. Container, Bulk Carrier, Tanker (from [7])



Figure 5. Ferries, Cruise and Specialist Ship (left to right) (from [7])

As mentioned in [8] and [9], a Rigid-Hulled Inflatable Boat (RHIB) boarding operation consists of six main phases: During the deployment phase, BT members are transferred to target vessels either by a helicopter or by a RHIB. After deployment, BT members climb aboard, or are dropped onto, the main deck of the target vessel (insertion phase). While onboard the target vessel, BT members move from the main deck to their first objective, which is generally to secure high-priority critical compartments (i.e., bridge, engine room, steering gear compartment), and to gather the crew together in a safe place for the ID check of seafarers (infiltration phase). After taking precautions against an imminent threat, BT members move toward their primary objective, such as the detection of WMD signatures, the seizure of the vessel, or rescue space (objective phase). After completion/fulfillment of the required mission, BT members move from the objective area back to RHIB (exfiltration phase). Finally, the extraction phase includes the voyage back to the main ship [8].

B. REQUIREMENTS FOR MIO BT NETWORKING

Considering complex structure of ships and inherent restrictions and challenges of maritime domain establishing a network between BT members requires elaborate effort. Significant and critical requirements have been analyzed in below sections.

1. Safety of Personnel

BTs have to be prepared for both types of compliant and non-compliant boarding. When boarding a hostile/non-compliant ship, the threat level is higher than a compliant ship; however, the MIO BT network should be able to prevent and minimize the potential risk. For instance, BT members may have to split into smaller groups to conduct further research, or to perform a safety check in different compartments of the ship. During investigation, there may be an intentional ambush, as well as accidental or sanitation incidents. Current operational procedures may force the BT leader to maintain a specific timeframe between the departure and return of all BT members. However, this methodology may have flaws and weaknesses, because a long time-out does not always indicate a problem. Even so without knowing the situation decision makers will not be able to make the right decision. The MIO BT network should be able to keep track of each BT members' position by tracing their actions to make sure they are safe.

2. Ease of Transportation

BT members have to be transferred to the target vessel either by air via a helicopter, or by sea using a RHIB. In addition to strong winds and high seas that may encumber transfer, heavy load may also prevent the transfer of BTs. Each BT member carries 20–25 pounds of gear, so it is recommended that additional weight should not be applied to their packs. Their communication equipment should be light, portable, and easy to deploy and use.

3. Reliable, Robust, and Scalable Communication

During boarding, team members may disperse and search almost all compartments in the vessel from the bridge to engine room. To coordinate mutual efforts, sustain situational awareness, and provide the safety of members, the BT network should provide reliable and robust links that will enable data transfer and voice communication. In unknown environments, BT members must

be prepared to encounter worst-case scenarios. As mentioned previously, a portable network should be scalable to cover all areas in the ship.

4. Tracking Positions of All BT Members

The exact location of the BT members within a vessel is crucial for the safety of members and situational awareness. In the case of a non-compliant boarding, knowing the exact location will diminish possible risks and lead decision makers to prevent possible threats, and to pinpoint accidents.

C. CHALLENGES

To fulfill requirements with current technologies, challenges described in below sections have to be considered.

1. Tracking Positions of All BT members

In the current technological infrastructure, a GPS (Global Positioning System) is used to designate a position over the Earth. The system is based on a basic methodology known as trilateration, which relies upon received electromagnetic signals from three satellites that are orbited in a known position and are processed to find the accurate location [10]. Though boarding team members will be in an open space during the first phase of boarding (and capable of being tracked via a GPS), a search below the main deck (beneath the steel structure of the ship) prevents the reception of GPS signals. Therefore, current commercial off-the-shelf GPS trackers do not provide a reasonable solution to being able to track BT members.

2. EM Propagation Below Main Deck

In his master's thesis, Chaabane [11] analyzed the propagation of electromagnetic waves within ships. As determined, there are three main challenges that affect the propagation below the main deck of the ship: absorption of electromagnetic energy, dispersion of the signals, and interference among the disseminated signals.

As electromagnetic waves travel within a ship compartment made mostly of steel, energy from the signal is absorbed by material, depending upon the characteristics of materials and characteristics of electromagnetic waves (frequency and wave length). Therefore, attenuation of the electromagnetic (EM) waves will vary for different materials at different wavelengths [11].

In addition to the absorption of energy, EM waves will either disperse or penetrate through material based on various characteristics of the wave, such as the arrival angle of the wave and relative permittivity between the mediums. As a result, an incident wave may promote a transmitted wave and a reflected wave. Due to the complex structure of the ships, diffraction is another physical incident that may be observed. “Diffracted waves scatter from discontinuities such as edges and tips” [11]. Diffraction waves may allow the signal to reach various areas where reflected or direct waves cannot reach.

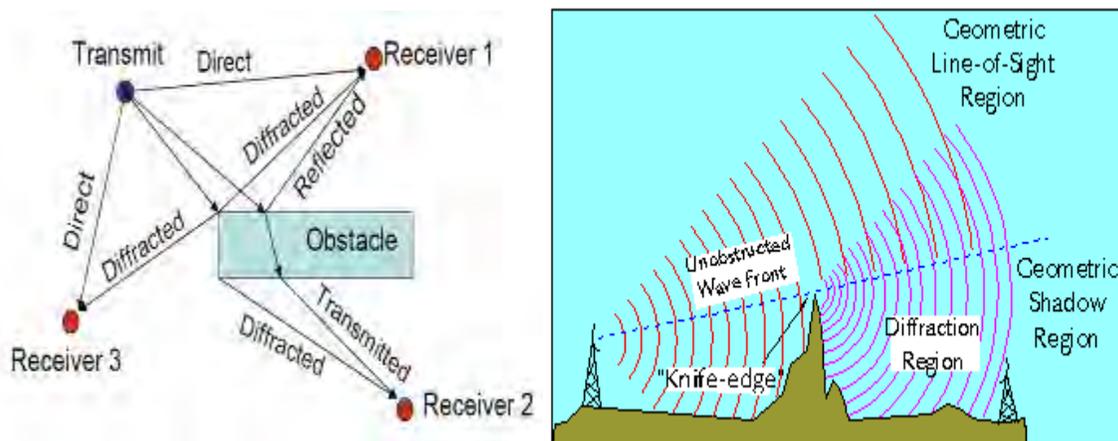


Figure 6. Reflection, Diffraction (left one from [11], right one from [12])

Due to various characteristics of the EM wave and the complex structure of the ship’s compartments, there may be multiple reflection and diffraction waves that display the same characteristics on their end nodes. Moreover since they will use the same medium incident waves may overlap with the diffracted or reflected waves. They may interfere with each other in a way to diminish each other. As a result it is challenging to predict or calculate expected behavior of the waves within ships.

D. PROPOSED POSSIBLE SOLUTIONS

There are two major challenges to figure out. BT leader and NOC have to keep track of each member and communication below main deck has to be sustained at all costs.

1. Positioning

GPS signals cannot penetrate thick steel decks of large ships; therefore, BT members cannot use GPS-based positioning while operating below the main deck, and thus, alternative approaches have to be investigated. Regarding the propagation of EM below deck, three methods can be used to keep track of BT members. By using low frequencies—low data transfer—interaction between the steel flats and EM waves can be minimized. With the help of some common navigational techniques, embedded applications installed in small smart devices attached to BT members can remotely keep track of the positioning data of each BT member.

The first method that can be used as an application is dead reckoning.

Dead-reckoning is the process of determining one's present position by projecting course(s) and speed(s) from a known past position, and predicting a future position by projecting course(s) and speed(s) from a known present position. [13]

Knowing the speed and direction of the moving BT members, an application can calculate the estimated position. Kothari et al. [14] analyzed and discussed dead reckoning and wireless signal strength fingerprinting in their research paper. With a Nexus-S android smart phone that has an embedded accelerometer, magnetometer, and gyroscope, they tested their localization techniques solution within two different indoor environments [14]. As Kothari et al. mentioned, the system does not provide perfect localization due to an error in the movement of the sensor through time. Since each sensor has its own inadequacy, the combination of the accelerometer, magnetometer, and gyroscope was chosen to have a lower error rate and a better prediction of

position. Input from these sensors is filtered. As a result, a better heading and speed estimation is obtained, leading to a better prediction of location.

The output is an estimate of the azimuth, pitch, and roll of the phone in a global frame. As acceleration and magnetic field strength readings are received, the direction of gravity and of north may be estimated. The combined orientation filter continuously accounts for drift in the gyroscope and error conditions in the magnetometer by using one sensor to compensate for the failings of the other. [14]. [Figure 7]

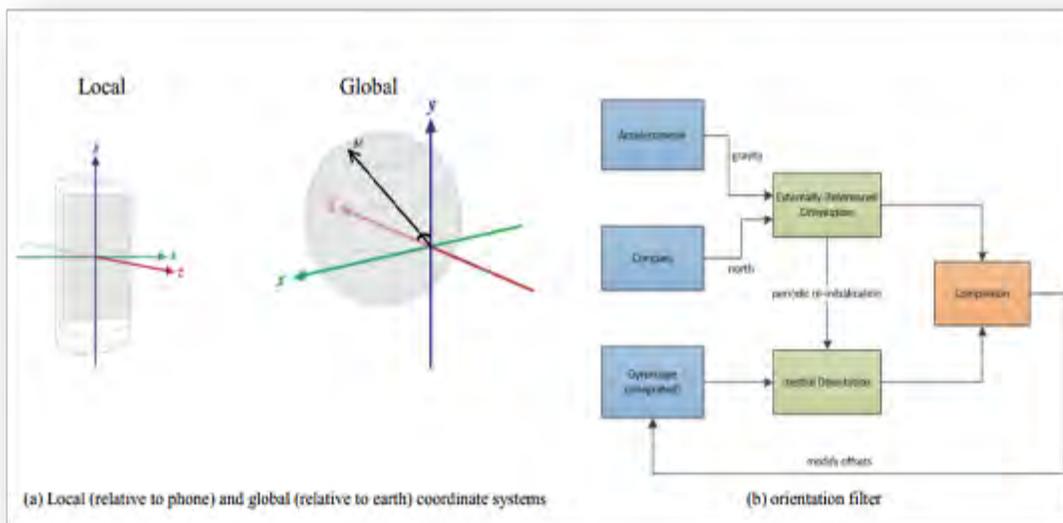


Figure 7. Heading Estimation (from [14])

In their experiment, Kothari et al. determined that only dead reckoning provides a better position estimation within indoor environments, while a combination of wireless and reckoning provides a better estimation in any location. Results for their findings in two different environments are presented in Table 3.

	Mean Error of Most Probable Location		Additional Features	
	Environment 1	Environment 2	Automatically Initializes Position	Error Bounded over Time
Dead Reckoning Only	5±3 meters	6±2 meters	No	No
Wifi Only	15±10 meters	10±4 meters	Yes(<5 seconds)	Yes
Dead Reckoning and Wifi (offline)	5±3 meters	7±2 meters	Yes(<5 seconds)	Yes
Dead Reckoning and wifi (online)	3±3 meters	<i>we currently do not have comparative results for environment 2</i>	Yes(<5 seconds)	Yes

Table 3. Experimental Results for Kothari (from [14])

Although this solution is promising, it may not be sufficient for location tracking, because three-dimensional movements within a ship's compartments may estimate location errors beyond the acceptable level. Additionally, in small or narrow inner spaces of ships, such as alleyways or compartments, errors are generated between actual and estimated positions often due to high-speed movements.

A trilateration system is another option. In their research paper Cook et al. [15] analyzed indoor positioning by trilateration and proposed techniques to improve estimation of the position. Knowing the received signal strength and power of the transmitted signal, an estimated circle of the position can be derived from the following formula.

$$P_r = P_t + 20 \log\left(\frac{\lambda}{4\pi}\right) + 10n \log\left(\frac{1}{d}\right)$$

P_t is transmitted power (in dBm), P_r is received power, λ is wavelength, n is path loss exponent ($n=2$ in free space), and d is the distance within [15], [16].

Using estimated circles for each node on BT network, cross section of two received signals circles can be used to detect the position of nodes. For three-dimensional position estimations, at least four received signals have to be used. However, due to the complex infrastructure of ships, reflections and diffractions may occur in higher frequencies, which may mislead the estimation of positions (Figure 8).

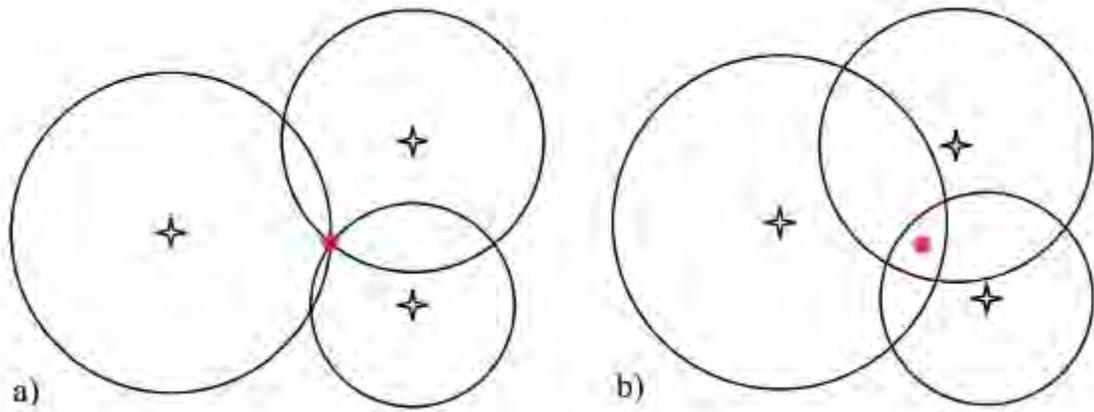


Figure 8. Positioning by Trilateration (a) Desired (b) Imperfect (from [15])

Finally, BT members can use verification of positions through voice communication. Using lower frequencies that are ideal for voice, BT members can maintain communication within a ship. With an application that includes the layout of a target ship, installed within a portable handheld device for the BT, each member can report and verify their position.

In addition to the indicated challenges, each of the first two techniques requires a three-dimensional layout/blueprint installed in a portable handheld device and integrated with suggested applications.

2. Reliable Communication

As expressed above, sustaining reliable, robust, and scalable communication is crucial for both the safety of BT members and the situational awareness within the ship. In his simulation of wireless propagation within ship compartments, Chaabane demonstrated possible paths of the waves between indoor and outdoor propagations [11]. Using a half-wavelength dipole antenna with 1-W power, he simulated a ship's bridge and showed that EM waves (WLAN 2.4 Ghz) initiated within the bridge were able to travel through open doors and be received (10 dBm) (see Figure 9) [11].

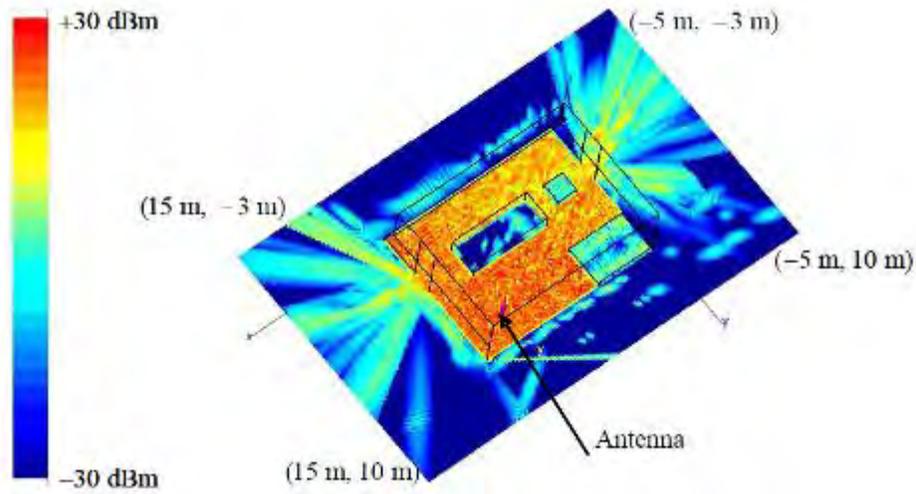


Figure 9. WLAN Propagation within Bridge Compartment (from [11])

As seen in Figure 10, wireless signals in high frequencies are prone to travel through openings, while they barely can penetrate through steel compartment walls. In addition, diffraction allows waves to travel beyond the line of sight.

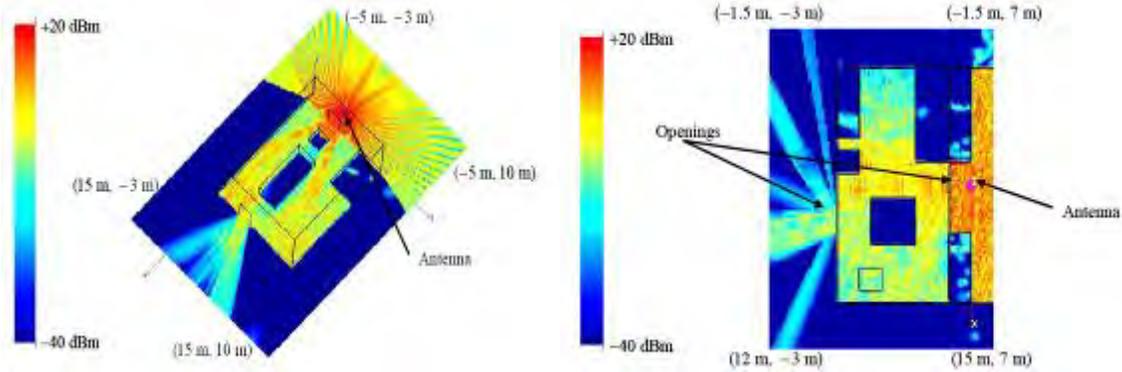


Figure 10. WLAN Propagation from Outside to Inside (left) within the Bridge (right) (from [11])

Although low-frequency sounds are more plausible to apply within ship compartments, lowering the frequency significantly may decrease the data transfer rate. Therefore, to establish a reliable, robust, and scalable network that can be used to reach-back with the operation center, more deployable relay nodes with higher frequencies are required. An operational procedure to relay

these nodes for different types of ships, and within compartments, has to be considered. One drawback for higher-frequency nodes will be positioning the BT members within the ships, especially below the main deck.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WIRELESS NETWORKS USED ONBOARD SHIPS WITHIN MIO AND BOARDING

A. OVERVIEW

In the last decade, there has been a significant evolution in wireless technology, based on higher demands of mobility due to mass communication requirements. With developments in Internet and cellular systems, wireless technology has become a significant part of communities. Providing wireless Internet connection in almost every part of daily routines, takes precedence over regular wired Internet connections. While through an airport, driving a car, or walking in a downtown area, cellular networks or wireless access points provide Internet connections. These provide a fixed-end solution for coverage of remote devices, such as WAP or the cellular coverage of the service provider. Beyond these boundaries, connectivity fails. While moving onboard target vessels, even though connection can be established through satellite phones—especially in off-shore boarding—dispersion of BT members below the main deck causes a lack of connectivity. Several technologies have been developed to overcome the problem of fixed centralized network structures that do not provide flexibility of multi-hop connections. Multi-hop wireless connections can be categorized in four major sub-networks, as seen in Figure 11. (Mobile Ad-hoc Wireless Networks (MANET), Wireless Mesh Networks (WMN), Wireless Sensor Networks and Hybrid Wireless Networks) [17]. Current technologies that enable mobile multi-hop networking are shown in Table 4.

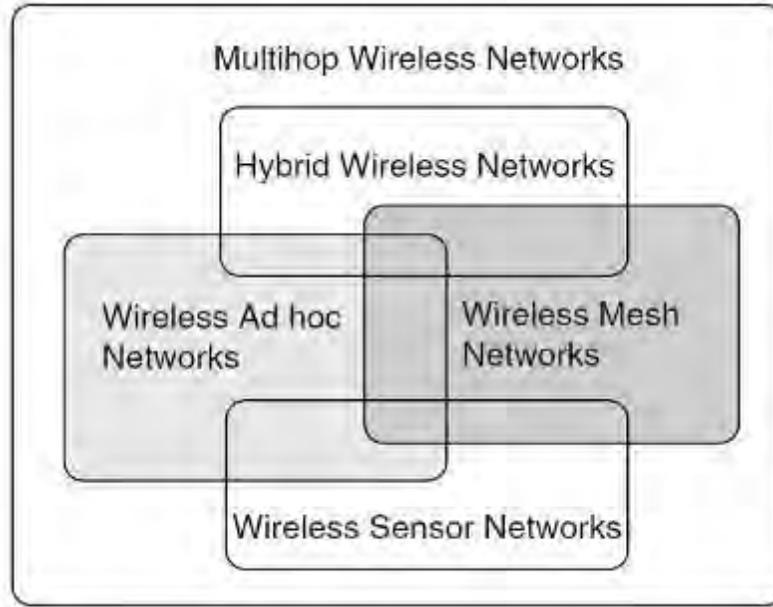


Figure 11. Classification of Multi-hop Wireless Networks (from [18])

Technology	Theoretical bit rate	Frequency	Range	Power consumption
IEEE 802.11b	1, 2, 5.5 and 11 Mbit/s	2.4 GHz	25–100 m (indoor) 100–500 m (outdoor)	~30 mW
IEEE 802.11g	Up to 54 Mbit/s	2.4 GHz	25–50 m (indoor)	~79 mW
IEEE 802.11a	6, 9, 12, 24, 36, 48 and 54 Mbit/s	5 GHz	10–40 m (indoor)	40 mW, 250 mW or 1 W
Bluetooth (IEEE 802.15.1)	1 Mbit/s (v1.1)	2.4 GHz	10 m (up to 100 m)	1 mW (up to 100 mW)
UWB (IEEE 802.15.3)	110 – 480 Mbit/s	Mostly 3 – 10 GHz	~10 m	100 mW, 250 mW
IEEE 802.15.4 (for example, Zigbee)	20, 40 or 250 kbit/s	868 MHz, 915 MHz or 2.4 GHz	10–100 m	1 mW
HiperLAN2	Up to 54 Mbit/s	5 GHz	30–150 m	200 mW or 1 W
IrDA	Up to 4 Mbit/s	Infrared (850 nm)	~10 m (line of sight)	Distance based
HomeRF	1 Mbit/s (v1.0) 10 Mbit/s (v2.0)	2.4 GHz	~50 m	100 mW
IEEE 802.16 IEEE 802.16a IEEE 802.16e (Broadband Wireless)	32 – 134 Mbit/s up to 75 Mbit/s up to 15 Mbit/s	10–66 GHz < 11 GHz < 6 GHz	2–5 km 7–10 km (max 50 km) 2–5 km	Complex power control

Table 4. MANET Enabling Technologies (from [19])

B. WIRELESS MESH NETWORKS

A wireless mesh network is a distributed, self-healing network that provides connection through relays over nodes within the network. Wireless

Mesh Networks (WMN) are used to provide reliable, scalable, and cost-effective communication in various areas. In contrast to wired/wireless centralized networks, node failures do not destruct network topology or connectivity. Various variables affect design of WMNs from power usage of nodes to antenna size of radios. Though WMNs leverage all OSI layers, Medium Access Control (MAC) mainly govern the communications within network through a common channel.

1. Challenges

In [18], challenges of WMN are discussed in detail. Important challenges that affect BT networking are described in the following sections.

a. *Throughput Degradation and Unfairness*

The theoretical upper limit of each node in random static WMN with ideal routing is $O(1/\sqrt{n})$, while the whole networks throughput is $O(1/\sqrt{n} \log n)$, where n is the number of nodes and O is the limit of the function [20]. Extending the network will significantly degrade throughput capacity; however, using IEEE 802.11 on a string topology—the current common protocol in use—the throughput degrades even more. Table 5 shows the degradation of throughput in a string topology with the increase of nodes within the network [18].

	<i>1 Hop</i>	<i>2 Hops</i>	<i>3 Hops</i>	<i>4 Hops</i>	<i>5 Hops</i>	<i>>5 Hops</i>
Normalized throughput	1	0.47	0.32	0.23	0.15	0.14
$\frac{1}{\text{Hoplength}}$	1	0.5	0.33	0.25	0.2	0.16

Table 5. Throughput Degradation in WMN (from [18])

Considering a possible extension of BT networking as more nodes are deployed, throughput will shrink to a level that will prevent data and/or voice exchange between members. During the design or network and operation phases of boarding, this challenge has to be taken into account.

Besides degradation, throughput fairness among nodes is another challenge.

A network is said to be exhibiting high throughput fairness if all nodes get equal throughput under similar situations of source traffic and network load. WMNs show high throughput unfairness among the contending traffic flows. [18]

Regarding throughput fairness, connectivity problems may pop-up during high density operations while multiple BT are members moving around.

b. Resource Management

Wireless nodes use batteries as energy sources. Depending upon the antenna size, and modulation and electronics onboard, nodes can use a specific bandwidth interval. Management of these resources is crucial to sustain a reliable and robust connection.

C. MOBILE AD-HOC NETWORKS

Mobile ad-hoc network is a dynamic decentralized wireless network that enables nodes to move around and extend the network through relays. Each node is involved in the routing, and provides the flexibility of a network to stretch toward the direction of the nodes. It does not require a fixed infrastructure similar to currently used wireless access points to manage networking between nodes. Instead, all nodes within the network act as a router and relay messages toward the destination. Sustaining connectivity between these mobile nodes challenges the network design. Moving nodes and routing tables change the network topology. In addition, movement of nodes agitates the link throughput and error rates. As discussed above in WMN, there is a tradeoff between routing/processing and energy consumption that directly restricts usage of nodes. Frodigh et al. analyzed mobile ad-hoc network characteristics and requirements to establish mobile ad-hoc networks in their research paper [21]. Characteristics and requirements that are relevant to the BT networking are summarized below.

1. Security

In a multi-hop environment, sustaining security triangle features, confidentiality, integrity and authentication (CIA) with non-repudiation, is essential in establishing a secure, reliable network. For security purposes, a best practice usage of a third-party certification authority among entities is the currently used mechanism, and a trust relationship among nodes has to be organized through a protocol [21]. Currently, commercial off-the-shelf technologies include such security precautions.

2. Routing

Spontaneous movement of nodes makes routing a challenging issue within MANETs. Depending on the network metrics, a best available path is chosen between end points by a routing algorithm. Calculated costs based on metrics can determine traffic paths. Major metrics that are used to calculate path costs include stability of nodes that define the uptime of nodes in a network, bandwidth/throughput, latency that defines the response time of a node, and power consumption. Protocols are divided into the following three groups [22].

a. Proactive

In proactive protocols, all information about routes to each node is stored in routing tables. Every change in topology is reflected to routing tables in a time interval. Keeping track of every change in the network will consume scarce bandwidth and power [21].

(1) Destination-Sequenced Distance Vector (DSDV). Each node maintains routes to every node within the network and required number of hops to destination node in its routing table. Periodic updates are broadcasted to nodes to keep their routing tables up-to-date. Since each node keeps records of the next hop for each destination node and number of hops, nodes can simply calculate optimized routes [21].

(2) Optimized Link State Routing Protocol (OLSR).

b. Reactive

In reactive protocols, only required routes are calculated and recorded.

(1) Ad-hoc On-Demand Distance Vector (AODV). It keeps records of routes like as DSDV protocol, except it does not keep records for all nodes. In case of creating a new route, the initiating node broadcasts a route request to its neighbors to find the route to end node. All nodes broadcast the request until the new node is found. During broadcast/flood each node records the new route [21].

(2) Dynamic Source Routing (DSR). In DSR routing source node embeds addresses of hops in the header of data packets. Intermediate nodes are only required to know the next hop towards the destination. If in routing a cache of node there is no record for next hop, a route request message is broadcast by that node. Either the destination node or the next hop node will unicast back [21].

c. Hybrid:

Hybrid protocols use features of both proactive and reactive protocols. One of the known hybrid protocol is Zone Routing Protocol (ZRP) [22].

D. DIFFERENCES BETWEEN VMNS AND MANETS

Although both wireless networks look similar to each other, they differentiate in various ways. One of the major differences is mobility of nodes. MANET nodes are more mobile and dynamic compared to WMN nodes; therefore, network topology of MANET is highly dynamic compared to a static WMN topology. The mobility of nodes affects routing performance; therefore, “while the on-demand routing protocols perform better in wireless ad hoc networks, the relatively static hierarchical or table-driven routing protocols perform better in WMNs” [18]. The main differences between these two networks are shown in Table 6.

<i>Issue</i>	<i>Wireless Ad Hoc Networks</i>	<i>Wireless Mesh Networks</i>
Network topology	Highly dynamic	Relatively static
Mobility of relay nodes	Medium to high	Low
Energy constraint	High	Low
Application characteristics	Temporary	Semipermanent or permanent
Infrastructure requirement	Infrastructureless	Partial or fully fixed infrastructure
Relaying	Relaying by mobile nodes	Relaying by fixed nodes
Routing performance	Fully distributed on-demand routing preferred	Fully distributed or partially distributed with table-driven or hierarchical routing preferred
Deployment	Easy to deploy	Some planning required
Traffic characteristics	Typically user traffic	Typically user and sensor traffic
Popular application scenario	Tactical communication	Tactical and civilian communication

Table 6. Differences Between MANETs and WMNs (from [18])

E. INTERNET CONNECTION FOR MANETS

Mobile IP for MANETs is used to provide Internet connection to nodes. Mobile IP foreign agents are used as access points in a layered protocol to provide connection. In case one of the nodes within the MANET requires an Internet connection, the node uses its home IP address and registers with a foreign agent. Foreign agents then act as proxies for the Internet connection [21]. A layered scheme of the MIPMANET is shown in Figure 12.

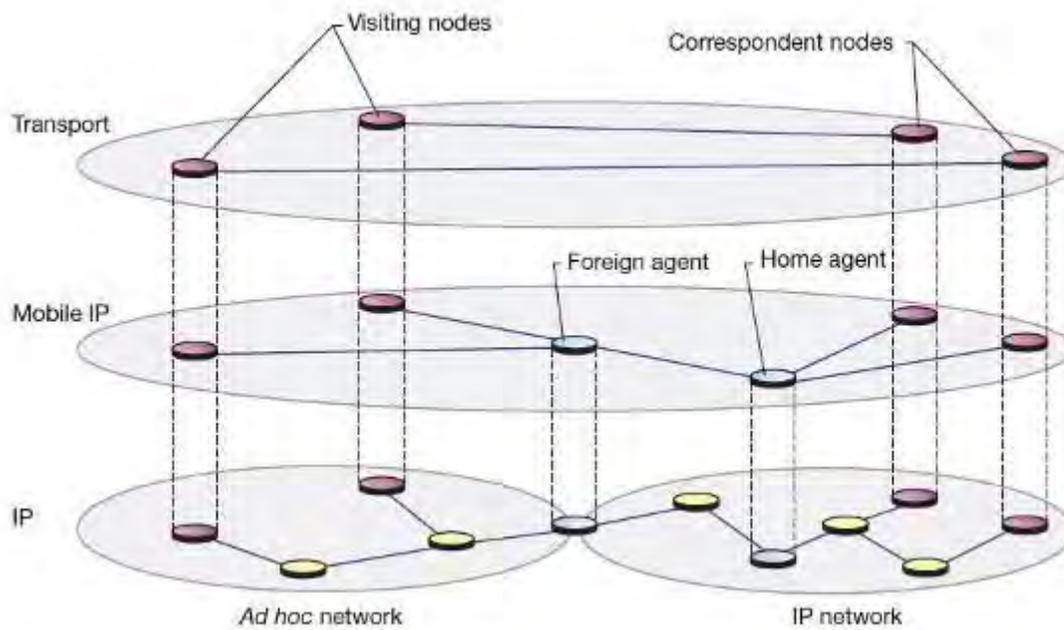


Figure 12. MANET Architecture for Internet Connection (from [21])

Using this layered approach enables nodes to have an Internet connection without inference of their regular network.

IV. EXPERIMENTATION FIELD

A. CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX)

The Center for Network Innovation and Experimentation (CENETIX) was founded in 2004 to conduct and lead research efforts in various areas such as tactical networking and collaboration, unmanned vehicles, sensors and situational awareness platforms. CENETIX integrates and manages a unique student-operated NPS Tactical Networking and Maritime Interdiction Operations Testbed [23]. Under the leadership of Professor Alex Bordetsky and Chief Engineer Eugene Borakov, CENETIX plug-and play test-bed extended from San Francisco to overseas partner sites in Germany, Sweden, Greece, Poland, Norway, and Czech Republic over time. Students and research associates in the Naval Postgraduate School (NPS) conducted various research and field experimentations in coordination with Lawrence Livermore National Laboratory, the U.S. Coast Guard, the U.S. Marine Corps, and the U.S. Special Operations Command.

One of the major research areas is to build and extend a network that will enhance situational awareness in Maritime Interdiction Operations. Within CENETIX, mobile Network Operations Center was built to manage collaborative efforts. After deployment of servers at the CENETIX operations center at NPS, a network was extended further to distributed nodes using a combination of current Internet backbone (VPN connection) and wireless mesh networks (Figure 13).



Figure 13. MIO Test bed, SF Bay , East Coast and Overseas (from [23])

All distributed nodes, either from internal networks of CENETIX or from the Internet that have a reach-back connection to CENETIX servers, are able to reach and share vital information through the CENETIX resource portal. System administrators simulating decision makers in the MIO can keep track of situational awareness nodes, while observing interactions among all nodes. Distributed nodes can share files, pictures along command and control channels, as well as instant video, via appropriate tool (Figure 14).

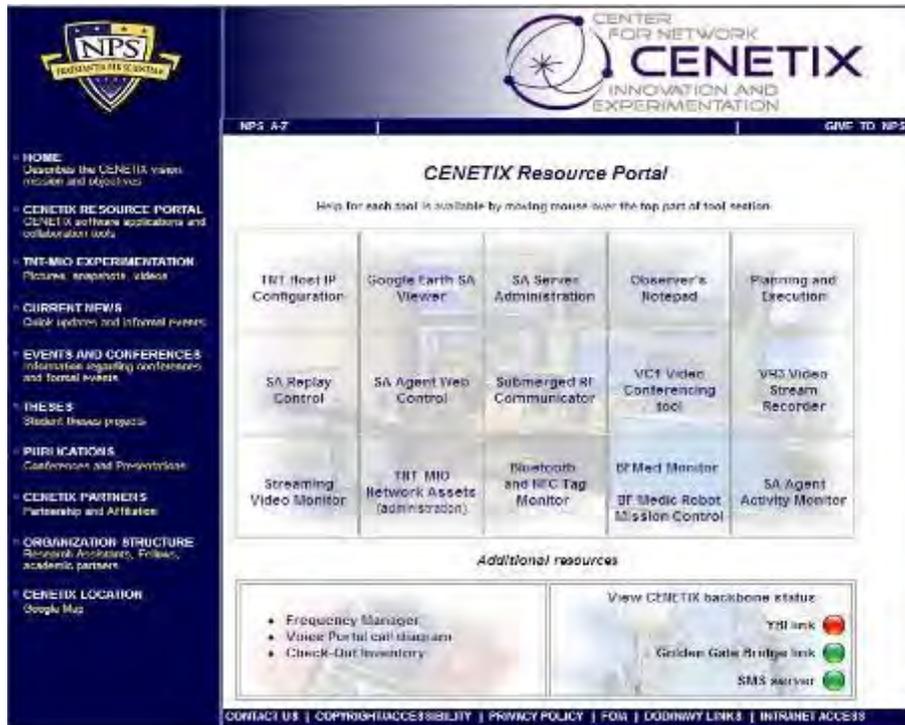


Figure 14. CENETIX Resource Portal (from [24])

As part of a Joint Interagency Field Experimentation (JFIX), in accordance with the U.S Coast Guard, Defense Threat Reduction Agency (DTRA), LLNL, and the Office of Naval Research (ONR), the CENETIX team conducted Maritime Interdictions Operations (MIO) Weapon of Mass Destruction Intelligence Surveillance and Reconnaissance (WMD-ISR) experiments in August 10–15, 2014 in Alameda, CA.

B. MIO WMD-ISR EXPERIMENTS IN ALAMEDA, CA (AUGUST 10–15, 2014)

1. Objectives of Experiment

Focus points of the experiment were [25]

- Establish and test Cutter-to-Boarding Team Network
- Establish and test Boarding Team On-The-Move Network
- Integrate MIO and counter WMD-ISR techniques

2. Scenario

To observe and measure most realistic values, the following scenario was developed based on current operational procedures. A suspected vessel shielded radiological/nuclear material or residue is to appear in SF Bay area. A harbor pilot boat detects the signature by stand-off detection sensor and reports to the authorities. The Operation Center starts to track target vessel movement, and concurrently shares/exchanges information visually with off-shore forward deployed fast patrol unit. Further analyzes of suspected target and its crew reveals strong affiliation to the San Francisco urban area that leads the Operation Center to shift a high threat level. Special Forces with technical units are tasked to conduct WMD-ISR ashore, while an offshore patrol boat is deployed to shadow the target vessel. After rendezvous of the target vessel with a large vessel, a cutter (simulated) is dispatched in the area with Boarding Team onboard to conduct a VBSS onboard large vessel. Boarding Team members are equipped with wearable broadband wireless units and stand-off detection sensors besides their weaponry. Instant data, voice, and video connections between Operations Center, the Cutter, the fast patrol boat, and the boarding team is crucial to carry out the mission with minimum risk. Also during boarding, divers are needed to conduct a search in the hull of the ship at sea [25].

3. Experiment Setup

To establish communication links between the experiment field and NPS CENETIX servers, we established a VPN gateway between the Coast Guard Base in Yerba Buena Island (YBI), San Francisco Bay, and NPS CENETIX Operations Center. To coordinate efforts and to observe/manage experiments, a portable network operations center was established onboard USNS Cape Orlando. Sector Antenna Arrays were mounted on a YBI tower, and onboard SFPD boats and the Coast Guard Cutter to extend the network (Figure 15). Initially, we tried to maintain a direct line-of-sight between YBI and USNS Cape ORLANDO; however, the container in-between prevented us from having a direct

link. We deployed SFPD Boats in-between to relay communications (Figure 15), and unique IPs were assigned to all nodes. The YBI tower node was configured to be the gateway for all distributed nodes. A quad radio router, with an omnidirectional sector antenna, provided a robust connectivity between mobile nodes.



Figure 15. Link between YBI Tower and USNS Cape ORLANDO



Figure 16. Sector Antenna Array Onboard SFPD Boat (from [26])

4. Boarding Team Networking

After extending the network to USNS Cape ORLANDO, we established our experimental set-up onboard to USNS Admiral Callaghan that was moored on the next pier. USNS Admiral Callaghan was simulating the target vessel. As discussed in earlier chapters, the propagation of EM waves below the main deck is unpredictable. Therefore, to have a better understanding of how the ship structure affects BT communication, we split decks in segments based on fragments and direct line-of-sight. In Figure 17, Deck-1 segments can be seen.

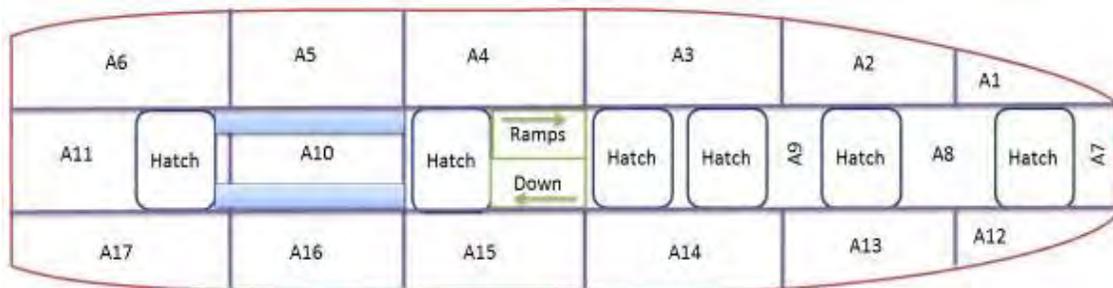


Figure 17. USNS Admiral Callaghan Deck-1 Measurement Segments

Based on current operational requirements and procedures of BTs, we made our measurements in two phases. In the first phase, after BT members

were onboard the target vessel, they split into three groups, each consisting two members. Each team initially moved to a specific location to secure the ship. The first team moved to the bridge, the second team gathered the crew in the mess room, and the last team moved towards the engine room to take control of the steering gear, the auxiliary engine room, and the main engine room. After securing the ship in the second phase, the BT leader directed the group in the engine room to search the ship. They searched the ship from the main deck down to the orlop deck. Two different wireless mobile ad-hoc networks (Wave Relay and Trellis Ware) and one wireless mesh network (Virtual Extension) were tested.

5. Evaluated WMN/Mobile Ad-Hoc Systems

We have evaluated two types of MANETs and one WMN.

a. *Wave Relay Mobile Ad-Hoc System*

The Wave Relay Mobil Ad-Hoc System is designed and developed by Persistent Systems as a solution for communication links between on-the-move nodes. It provides peer-to-peer scalable networks that enables data, voice, and video communication between on-the-move nodes. Man Portable Unit 4 (MPU4) provides connectivity by seamless OSI Layer-2 Ethernet which enables to plug-and-play cameras, video recorders, IP sensors and various devices. The radios in our lab have 2.3–2.5 GHz frequency range. Specifications of MPU4 are provided in Figure 18 [27]. Wave relay radios can be configured through an interface in the web browser. Some specifications and measurements, such as Signal-to-Noise Ratio (SNR) and Bandwidth usage, can be observed from the control interface.

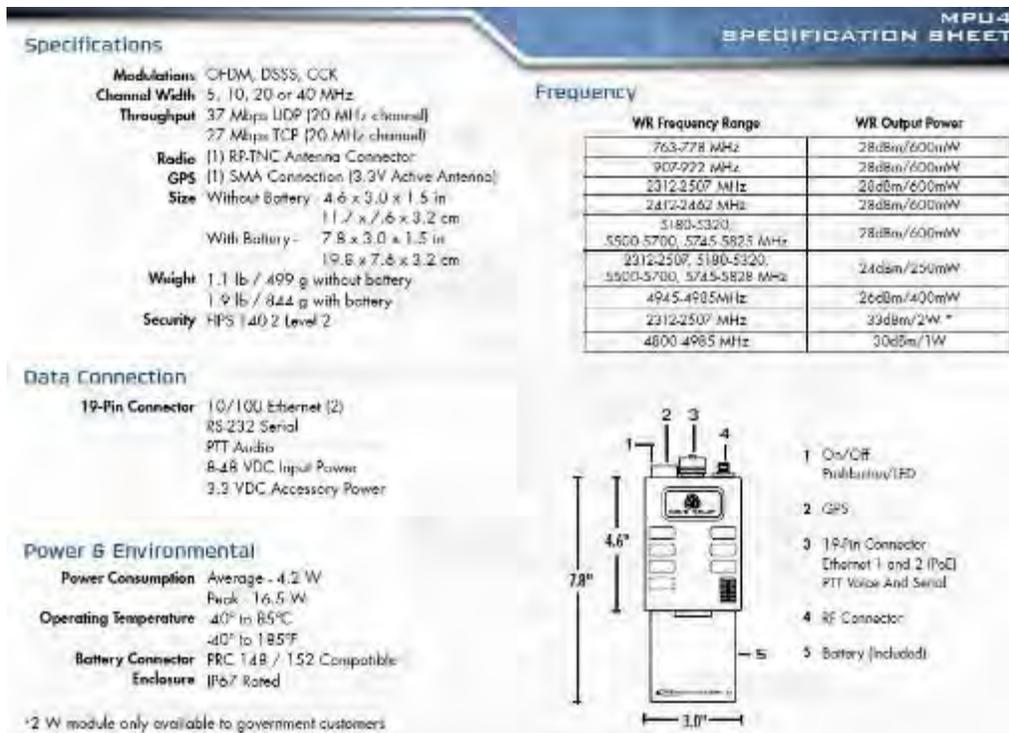


Figure 18. MPU4 Specification (from [27])

b. Trellis Ware Mobile Ad-Hoc System

The second commercial mobile ad-hoc radio that we used was CheetahNet’s tactical network radio TW220. It is a handheld portable unit designed to establish voice/video/data network up to eight point-to-point nodes. According to Trellis Ware Inc., it is specifically designed to operate in the harshest environments such as MIO, mine coverage, and robotics. Specifications of MPU4 are provided in Figure 19 [28].



Figure 19. TW-220 Performance Parameters (from [28])

c. *Virtual Extension Wireless Mesh System*

Virtual Extension's VEmesh network is a low power, low frequency wireless mesh network that is designed for sensor networking. VEmod with its RF part communicates with the network via RS232, RS485 or DALI interface. The main drawback of sensor networks when the size of the network is getting bigger is the power and computing consumption of routing algorithms. According to Virtual Extensions' data sheet, VEmesh is optimized for wireless mesh networks via "synchronized-flooding" technology that enables nodes to re-transmit every message they receive. So in order to send a message, initiating node sends it to all neighbor nodes, and all nodes retransmit the message until all nodes have received it. By this way all nodes are covered without any excessive routing process that consumes energy and processing time. This multi-path propagation maximizes network throughput against interference. Besides, there is no theoretical limitation for the number of nodes in WMN. Figure 20 displays a picture of nodes that illustrate four hops, with an obstruction

on the way. According to the specification sheet of VEmesh, theoretical data rate is 50 Kbps, and frequency range is 902–928 MHz [29].

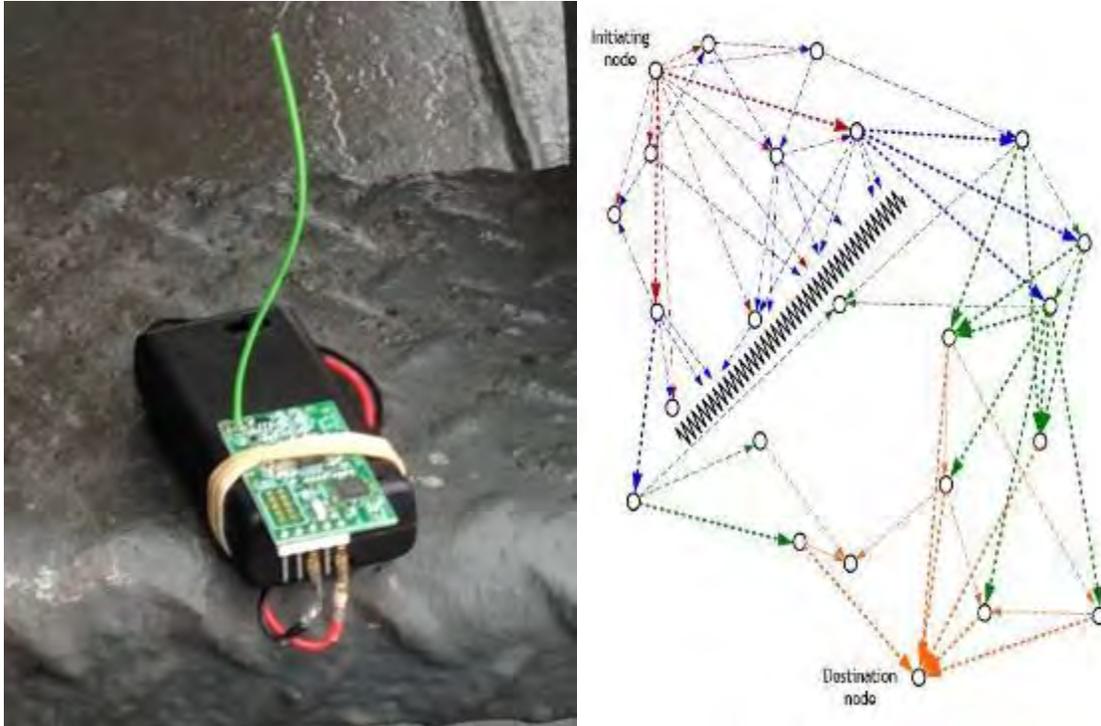


Figure 20. VEmesh Node and 4 Hops Networking Through and Obstacle (from [29]).

d. Measurement Tools Used

To observe network performance and node behavior, we used Solar Winds Network Management and Performance tool, Qcheck Network Performance Measurement tool, and two laptops each with two Ethernet cards to host two local area networks. To observe instant changes in connectivity of nodes, we used a Node Ping Graph tool, which is an interface that provides pings concurrently to multiple IPs with their response time.



Figure 21. Qcheck NPM Tool(left) and Node Ping Graph Tool (right)

We mounted one Trellis Ware node and one Wave Relay node to two laptops on each side, and then created a common background domain to merge these two local area networks. As discussed above, for the measurement of the first phase of boarding to secure the ship, BT members split into three groups and dispersed from the bridge to engine room. To observe the behavior of the on-the-move nodes, we measured TCP, UDP throughputs, SNR, Upload, and Download Bandwidths of nodes in-between stations and recorded the values. We also made radio checks to observe/control voice communications. Regarding the previous research of propagation of EM waves within ship compartments, we chose stations at the preface of poor network metrics. We set bridge, mess room, hatch to second deck, steering gear compartment, auxiliary engine compartment, and main engine compartment as our stations, respectively, from the upper decks to the lower decks. Figure 22 and Table 7 show stations on the blueprint of the ship, and the results of the wave relay mobile ad-hoc system, respectively.

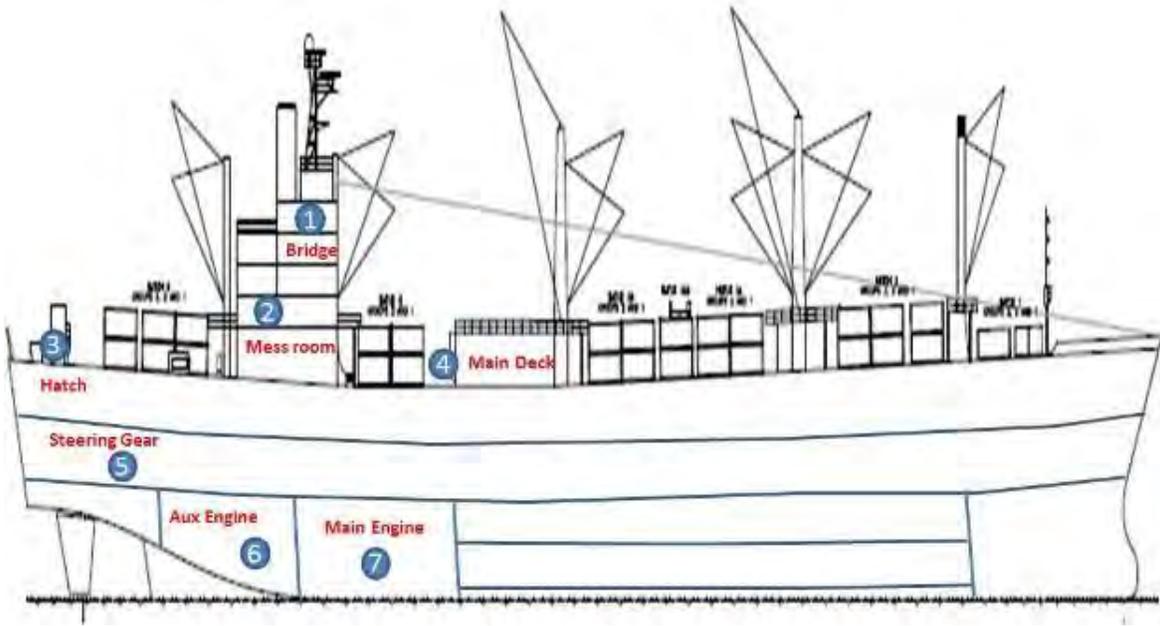


Figure 22. Phase-I (Securing the Ship) Measurement Stations

Stations	TCP Throughput (Qcheck)	UDP Throughput (Qcheck)	SNR (dB) (WR)	Upload Bandwidth (Solarwinds)	Download Bandwidth (Solarwinds)	Ping Response Time
2-4	1.017 Mbps	1.16 Mbps	39	1.76 Mbps	2.58 Mbps	84 ms
1A-2	81.484 Kbps	154.95 Kbps	8.5	N/A	N/A	N/A
1B-2	1.3 Mbps	168.5 Kbps	14.4	1.4 Mbps	1.24 Mbps	6 ms
2-3	911.47 Kbps	356.19 Kbps	15.20	1.93 Mbps	2.73 Mbps	10 ms
1-3	192.45 Kbps	579.7 Kbps	15.7	2.28 Mbps	1.10 Mbps	24 ms
3-5	2.778 Mbps	1.153 Mbps	37.8	3.07 Mbps	1.85 Mbps	10 ms
3-6	N/A	N/A	1-3.7	N/A	N/A	N/A
5-7	1.798 Mbps	610 Kbps	34.04	961 Kbps	2.19 Mbps	6 ms
6-7	2.9 Mbps	1.8 Mbps	34.73	2.69 Mbps	2.27 Mbps	6 ms

Table 7. Measurements of First Phase for Wave Relay

After measurements of (phase-I securing the ship), we measured and observed the network performance during the second phase of boarding (search of the vessel) based on our segments mentioned earlier. Since the main deck is

an open space, we were able to measure network parameters; however, when we moved down below deck, wave relay nodes started to fade within 20 meters. This was an expected situation due to high frequency and OFDM modulation technique used by Wave Relay system. On the other hand, Trellis Ware System TW-220 radios were functional below the main deck. We followed patterns of segments as shown in Figures 23–26, and continued to follow all other decks below the main deck to observe peer-to-peer network performance metrics.

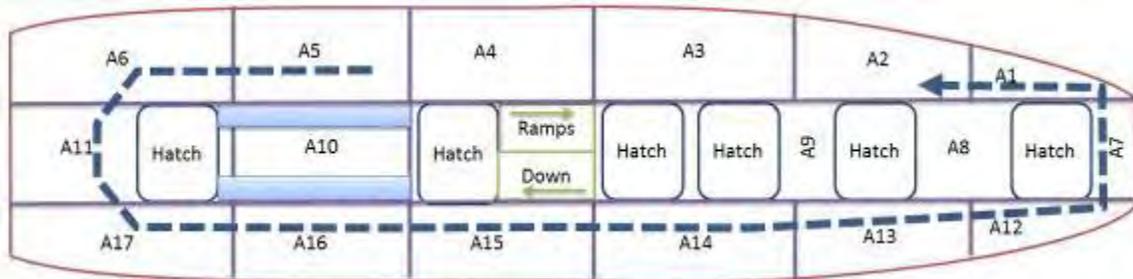


Figure 23. Main Deck Search Pattern

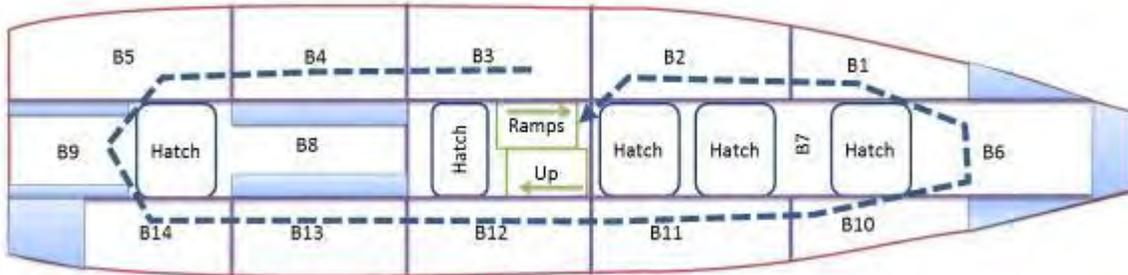


Figure 24. Second Deck Search Pattern

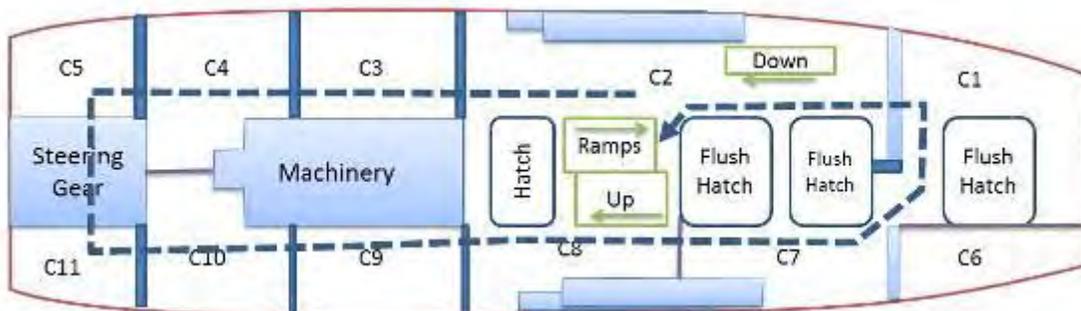


Figure 25. Third Deck Search Pattern

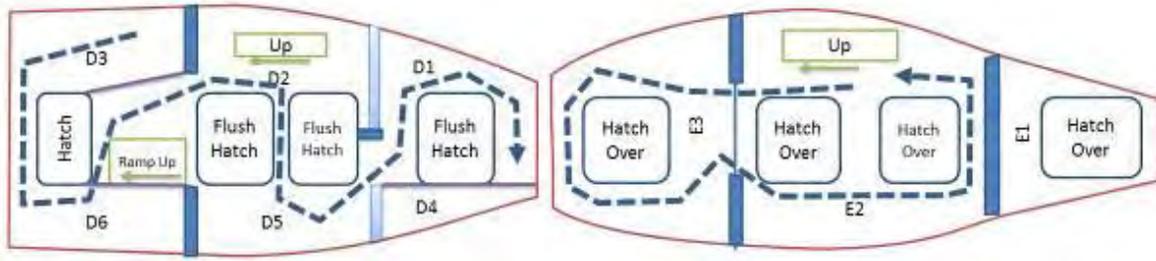


Figure 26. Fourth (left) and Fifth (right) Decks Search Pattern

Measurements for the main deck are shown in Table 8.

Stations	TCP Throughput (Qcheck)	UDP Throughput (Qcheck)	SNR (dB) (WR)	Upload Bandwidth (Solarwinds)	Download Bandwidth (Solarwinds)	Ping Response Time
A4-Bridge	1.4 Mbps	274.72 Kbps	27.28	2.82 Mbps	2.62 Mbps	82 ms
A4-A11	1.212 Mbps	246 Kbps	34.11	1.74 Mbps	2.57	6 ms
A4-A17	N/A	N/A	34.66	N/A	N/A	N/A
A4-A14	1.91 Mbps	1.050 Mbps	35.2	1.61 Mbps	1.14 Mbps	13 ms
A4-A13	824.75 Kbps	609 Kbps	35.36	2.57 Mbps	1.17 Mbps	16 ms
A4-A12	998 Kbps	752 Kbps	21.3	1.23 Mbps	715 Kbps	16 ms
A4-A7	705.2 Kbps	523 Kbps	18	689 Kbps	188 Kbps	18 ms

Table 8. Measurements of Main Deck-1

After having point-to-point measurements regarding EM propagation within the vessel, we investigated patterns to relay nodes in a way to sustain reliable communication. During the first phase, to extend the network from the bridge to the main engine room, we deployed VEmesh and Wave Relay Trellis ware nodes, as seen in Figures 27 and 28.

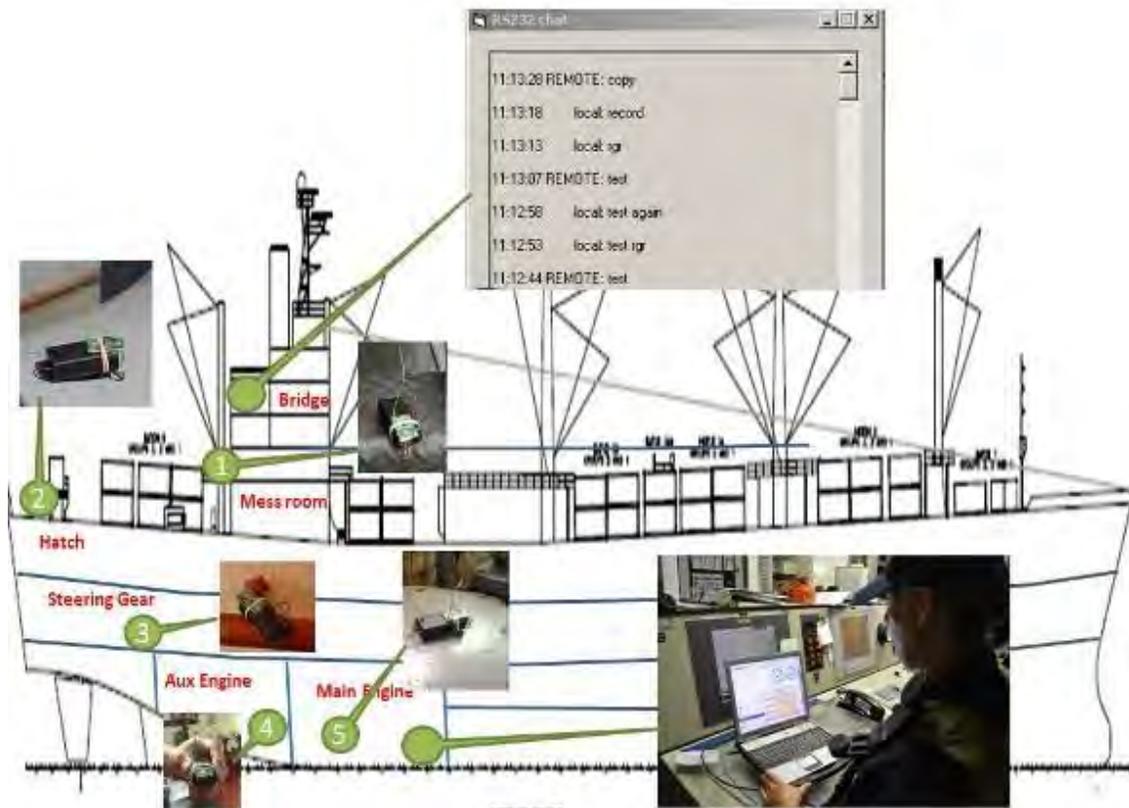


Figure 27. Virtual Extension Mesh Network

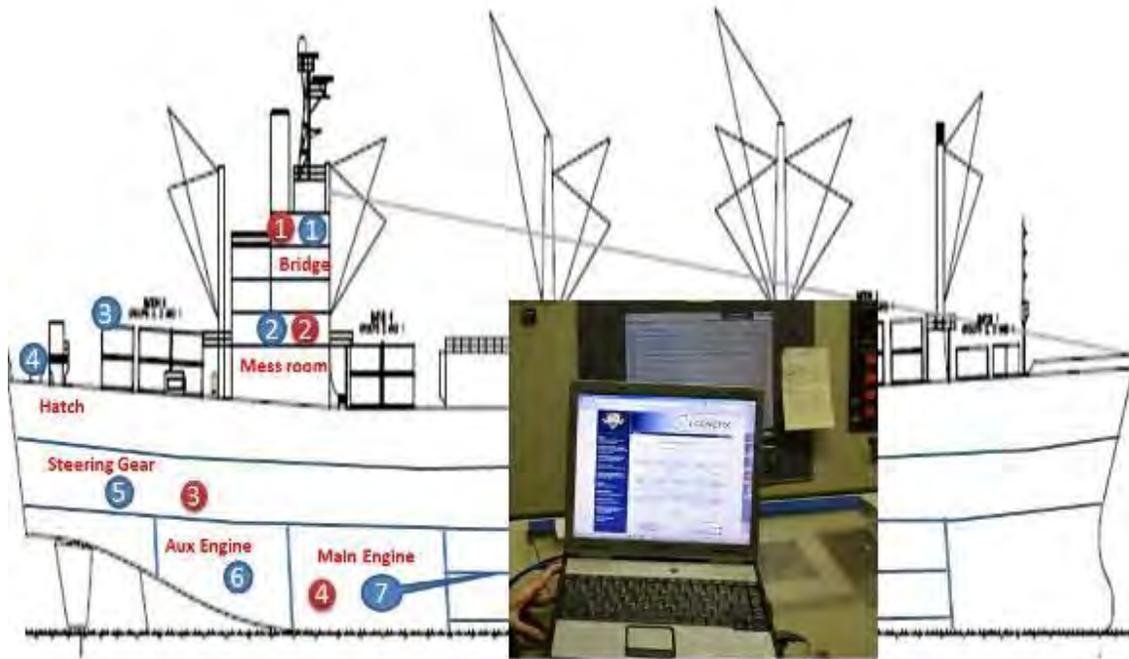


Figure 28. Wave Relay (blue nodes), Trellis Ware (red nodes) Networks

Based on our network we built, Table 9 displays the measurements we gathered.

Stations	TCP Throughput (Qcheck)	Packet Loss Rate(%)	Received Bandwidth (Solarwinds)	Transmitted Bandwidth (Solarwinds)	Node Response Time	Approx. Distance
2-4	147.358 Kbps	0	10.4 Kbps	57 Kbps	302 ms	20 m
2-5	171.455 Kbps	29	59 Kbps	7.862 Kbps	595 ms	25 m
2-6	104.535 Kbps	0	48.3 Kbps	4.742 Kbps	701 ms	20 m
2-7	29.165 Kbps	23	118 Kbps	5.684 bps	1013 ms	23 m
Mess-Main Deck	148.783 Kbps	0	4227 bps	4040 bps	524 ms	10 m

Table 9. Measured Metrics of Network

We extended the network down to the engine room via deployable nodes, and measured the network metrics to get a better understanding of communications below the main deck.

For the wave relay network, we deployed five nodes in-between the bridge and the main engine to keep data communications alive. We observed that boarding team members were able to download the CENETIX website and establish a communication to the server from the main engine compartment. Regarding the higher frequency used by Wave Relay nodes and propagation of waves within ship compartments as discussed in Chapter II, we deployed our nodes close to openings within the ship. We deployed only two TW-220 radios to keep voice communications alive between the far edge nodes, as seen in Figure 28.

For the Virtual Extension Mesh Network, we deployed five lightweight nodes that were easy to deploy and carry. Boarding team member on-the-move below the main deck was able to communicate with the boarding team leader through command and control channels. We tested the system in all parts of the steering gear, the auxiliary room, and the main engine room. With only five relay nodes, BT members on-the-move had the flexibility to move around without any interference.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

The main concept of this thesis was to extend the boarding team network to cover the entire vessel using deployable mobile wireless relay nodes. Two different types of mobile ad-hoc networks and one wireless mesh network were tested. Experiments were conducted onboard the USNS Admiral Callaghan, a cargo ship designed to carry large vehicles, which is over 694 feet in length.

MANET (Wave Relay) with higher frequency performs well on the main deck; however, every 20 meters below the main deck a new node replacement was required to extend the network. Regarding propagation of EM, placing the nodes in the hatches provided a better distance and throughput. For the first phase of boarding seven (five relays, and two endpoints) high frequency nodes were used to extend the network from the bridge down to the main engine room. Connection to the CENETIX server was established during the experiment from the main engine room via high frequency nodes; however, to cover or search all of the ship, at least ten more nodes are required.

MANET (Trellis ware) with relatively lower frequency performs better onboard ship. With 4 nodes the entire vessel was covered during search phase. Yet only voice communication was established. Due to lower frequency data throughput was lower compared to higher frequency nodes.

WMN (Virtual Extension) nodes are much lighter than the other two nodes. With only five nodes, the bridge to engine room communication was established through RS-232. Though current packet size that can be transferred is small, the network can be used as a command and control channel between boarding team members. With its star topology, more than one team can communicate through a common channel.

Considering damage control units onboard warships and Special Forces in urban areas, findings of this research can be developed to enhance operational requirements in those areas.

To develop at least a baseline for Coast Guard and Naval Forces, this research can be extended to cover different types of ships as discussed in Chapter II. After examination of each different type of ship, operational guidelines with technical details can be published. Furthermore, experiments can be extended to vessels in operation—such as ferries carrying people—while their engines will certainly affect the network metrics. Performance of the integration of more than one system can be evaluated under different conditions. Comparison of the whole MIO network metrics will provide a better picture.

LIST OF REFERENCES

- [1] NATO, "Alliance Maritime Strategy," NATO, Brussels, Belgium, 2013.
- [2] International Maritime Organization, "Review of Maritime Transport," in *United Nations Conference on Trade and Development*, 2010, pp. 7–9.
- [3] S. P. Metaparti, "Maritime Security After 9/11: The Shipping Industry's Response to the Terrorist Threat," M.S. thesis, University of Hong Kong, 2004.
- [4] A. Walker. (2012, June 30). Breaking the Bottleneck: Maritime Terrorism and "Economic Chokepoints." [Online]. Available: <http://cimsec.org/breaking-the-bottleneck-maritime-terrorism-and-economic-chokepoints-part-1/1742>.
- [5] Compliant Boarding Definition. (May 2013). United Nations. [Online]. Available: <http://unterm.un.org/DGAACS/unterm.nsf/8fa942046ff7601c85256983007ca4d8/459f07c8c097f3958525775f00491aff?OpenDocument>.
- [6] Non-Compliant Boarding Definition. (January 2014). United Nations. [Online]. Available: <http://unterm.un.org/DGAACS/unterm.nsf/8fa942046ff7601c85256983007ca4d8/2c92ac48c72c5e08852577890069de38?OpenDocument>.
- [7] Different Types of Ship in the World Merchant Fleet. International Chamber of Shipping. [Online]. Available: <http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade/different-types-of-ship-in-the-world-merchant-fleet>. Accessed August 23, 2014.
- [8] H. G. Nguyen and M. Baker, "Characteristics of a Maritime Interdiction Operations Unmanned Ground Vehicle," Space and Naval Warfare Systems Center, San Diego, 2012.
- [9] Department of Navy Office of Chief of Naval Operations Headquarter Operations and U.C. Guard, "Navy tactic, techniques, and procedures," Washington, DC, 2008.
- [10] F. Michel, "Maximizing and Improving Situational Awareness with Global Positioning System Data in the Maritime Domain," M.S. thesis, Department of Information Technology Management, Naval Postgraduate School, Monterey, 2009.

- [11] A. Chaabane, "Propagation Modeling of Wireless Systems in Shipboard Compartments," M.S. thesis, Naval Postgraduate School, Monterey, 2005.
- [12] Knife-Edge Effect. ATIS. [Online]. Available: <http://www.atis.org/glossary/definition.aspx?id=4047>. Accessed August 23, 2014.
- [13] N. Bowditch, "American Practical Navigator," in *Chapter-7 Dead Reckoning*, Bethesda, Maryland, National Imagery and Mapping Agency, 2002, p. 99.
- [14] N. Kothari, B. Kannan and M. B. Dias, "Robust Indoor Localization on a Commercial Smart-Phone," Carnegie-Mellon University, Pittsburgh, Pennsylvania, 2011.
- [15] B. Cook, G. Buckberry, I. Scowcroft, J. Mitchell and T. Allen, "Indoor Location Using Trilateration Characteristics," University College London, U.K.
- [16] 9-1-1 Service. FCC. [Online]. Available: <http://www.fcc.gov/911/enhanced/> Accessed August 23, 2014.
- [17] Y. Zhang, J. Luo and H. Hu, "Chapter-1 Preface," in *Wireless Mesh Networking*, Auerbach Publication, 2007, p. 2.
- [18] B. Manoj and R. R. Rao, "Wireless Mesh Networks: Issues and Solutions," in *Wireless Mesh Networks*, Auerbach Publications, 2007, p. 6.
- [19] J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges," *Journal of Communications Network*, vol. 3, pp. 60–66, July 2004.
- [20] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Transaction on Information Theory*, vol. 46, no. 2, pp. 388–404, March 2000.
- [21] M. Frodigh, P. Johansson and P. Larsson, "Wireless Ad Hoc Networking—The Art of Networking Without a Network," *Ericsson Review*, no. 04, 2000.
- [22] J. Ishmael. (2009). Wireless Mesh Network. [Online]. Available: http://www.cse.chalmers.se/minema2009/slides/minema2009_WirelessMeshNetworks.pdf. Accessed June 23, 2014.

- [23] A. Bordetsky and N. David, "TNT Testbed for Self-Organizing Tactical Networking and Collaboration," Naval Postgraduate School.
- [24] Center For Network Innovation and Experimentation. (n.d.). Naval Postgraduate School. [Online]. Available: <http://cenetix.nps.edu/cenetix/>. Accessed June 28, 2014.
- [25] A. Bordetsky, "Maritime Interdiction Operations WMD-ISR," Naval Postgraduate School, Monterey, CA, 2014.
- [26] T. Kontogiannis, "Ad-Hoc Sensor Networks for Maritime Interdiction Operations and Regional Security," Naval Postgraduate School, Monterey, CA, September 2012.
- [27] P. Systems, *Man Portable Unit (MPU4)*. New York: Persistent Systems.
- [28] *TW-220 Cheetah Net*. T.W. Technologies, San Diego, CA, 2008.
- [29] *VEmod ST31-4.0 Standart Module for Wireless Mesh*, Virtual Extension, Israel, 2013.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California