



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**AD-HOC SENSOR NETWORKS FOR MARITIME
INTERDICTION OPERATIONS AND REGIONAL
SECURITY**

by

Theofanis Kontogiannis

September 2012

Thesis Advisor:

Alex Bordetsky

Second Reader:

John P. Looney

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 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Ad-Hoc Sensor Networks for Maritime Interdiction Operations and Regional Security			5. FUNDING NUMBERS	
6. AUTHOR Theofanis Kontogiannis				
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) Robust communications are key to the success of naval operations such as area surveillance, control, and interdiction. Communication and sensor networks allow the flow of data and critical information that is necessary for conducting an operation from both the tactical and strategic perspectives. In naval operations, the platforms are hardly stationary, as the networking infrastructure operates from a variety of platforms in motion on the sea, above the sea, and from space, in the case of satellite support. Sensor networks consist of nodes made up of small sensors that are able to monitor, process, and analyze phenomena over geographical regions of varying sizes and for significant periods. Some categories of these small, and sometimes low-cost, sensors are able to collect and transmit, or relay, sensor data about physical values (e.g., temperature, humidity, and sea state), or dynamic attributes of objects, such as speed, direction, and the existence of dangerous substances (e.g., radioactive materials and explosives). The objective of this thesis is to examine how unstructured sensor networks, known also as ad-hoc sensor networks, can effectively support maritime interdiction operations and regional security by providing reliable communications and flow of information.				
14. SUBJECT TERMS WSN, MANET, WMN, MIO, Regional Security, Wireless Network, Networked-Swimmers, UAV, USV, Buoys, Sensors			15. NUMBER OF PAGES 129	
			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

**AD-HOC SENSOR NETWORKS FOR MARITIME INTERDICTION
OPERATIONS AND REGIONAL SECURITY**

Theofanis Kontogiannis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 2001

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
September 2012**

Author: Theofanis Kontogiannis

Approved by: Alex Bordetsky
Thesis Advisor

John P. Looney
Thesis Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Robust communications are key to the success of naval operations such as area surveillance, control, and interdiction. Communication and sensor networks allow the flow of data and critical information that is necessary for conducting an operation from both the tactical and strategic perspectives. In naval operations, the platforms are hardly stationary, as the networking infrastructure operates from a variety of platforms in motion on the sea, above the sea, and from space, in the case of satellite support.

Sensor networks consist of nodes made up of small sensors that are able to monitor, process, and analyze phenomena over geographical regions of varying sizes and for significant periods. Some categories of these small, and sometimes low-cost, sensors are able to collect and transmit, or relay, sensor data about physical values (e.g., temperature, humidity, and sea state), or dynamic attributes of objects, such as speed, direction, and the existence of dangerous substances (e.g., radioactive materials, explosives).

The objective of this thesis is to examine how unstructured sensor networks, known also as ad-hoc sensor networks, can effectively support maritime interdiction operations and regional security by providing reliable communications and flow of information.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	MOTIVATION	1
B.	MARITIME INTERDICTION OPERATIONS (MIO).....	1
C.	AD-HOC SENSOR NETWORKS IN MIO: BACKGROUND	4
D.	THESIS OBJECTIVE	6
E.	THESIS OUTLINE.....	6
II.	LITERATURE REVIEW	7
A.	INTRODUCTION.....	7
B.	AD-HOC NETWORK CATEGORIES	9
1.	Mobile Ad-hoc Networks (MANETs).....	9
2.	Wireless Mesh Networks (WMN).....	10
3.	Wireless ad-hoc Sensor Networks (WSN).....	13
C.	SENSOR NETWORK DESIGN FOR MIO	19
1.	MIO Sensor-Network Design Philosophy	19
2.	Sensor Placement Problem in MIO	21
3.	Mobile Agent Routing.....	22
4.	Data Aggregation	24
5.	Area Coverage.....	25
III.	MIO NETWORK OPERATIONAL CONCEPT	29
A.	OPERATIONAL REQUIREMENTS FOR MIO NETWORKS	29
B.	ASSETS CONSISTING OF NODES IN A MIO NETWORK	34
1.	Boarding Team.....	35
2.	Swimmers - Divers	37
3.	Vessels	39
4.	Smart Buoys and USVs	40
5.	UAVs	49
6.	Land-Based Stations	56
IV.	EXPERIMENTATION FIELD	59
A.	CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX)	59
B.	SAN FRANCISCO BAY AREA	62
1.	Network equipment	62
2.	TNT/MIO 11–2 (May 6, 2011, event)	67
3.	TNT/MIO 12–2 (February 28, 2012 event).....	71
4.	Lessons learned	75
C.	FORT EUSTIS – RIVERINE AREA, VIRGINIA	76
1.	TNT/MIO 08–04 Experiment (September 08–12, 2008)	76
2.	TNT/MIO 09–02 Experiment (April 23–24, 2009).....	79
3.	TNT/MIO 09–04 (September 09–10, 2009).....	81
4.	Lessons learned	83
D.	NMIOTC, SOUDA BAY - GREECE	84

1.	TNT/MIO 09-04 (September 28–30, 2009)	84
2.	TNT/MIO 10-02 (June 12–14, 2010).....	86
3.	TNT/MIO 11-02 (June 9–10, 2011).....	89
4.	TNT/MIO 12-02 (June 12–14, 2012).....	95
5.	Lessons learned	96
E.	SUMMARY	96
V.	CONCLUSIONS	99
A.	CONCLUSIONS	99
B.	OTHER APPLICATIONS – POTENTIAL FUTURE RESEARCH.....	102
	LIST OF REFERENCES	105
	INITIAL DISTRIBUTION LIST	111

LIST OF FIGURES

Figure 1.	Armed boarding parties conducting MIO (Images from militaryphotos.net and wikimedeia.org).	3
Figure 2.	Network for the conduct of military operations (Image from VirginiaTech ECE department website)	8
Figure 3.	San Francisco Bay Area mesh network backbone (Image from CENETIX website).....	11
Figure 4.	A wireless mesh network interconnecting stationary and mobile clients (From [19]).....	12
Figure 5.	WSNs for geological data, ecosystem monitoring and weather forecasting (Image from Network Intell website)	15
Figure 6.	Multi-hop relay in a network (Image from Nomadic Technologies website).....	26
Figure 7.	Three-Dimensional Coverage Model (From [31]).....	27
Figure 8.	Voronoi diagram (From [31])	28
Figure 9.	Network Performance Monitor (From Solarwinds website)	34
Figure 10.	ARAM sensor (from [20])	35
Figure 11.	Glau software showing a spike in gamma-count rate (from [20])	36
Figure 12.	Networked swimmers for TNT 11–2 (Image from CENETIX website)	38
Figure 13.	Portable detector used by the swimmers for TNT 11–2 (Image from CENETIX website).....	38
Figure 14.	Transmitted video and videoconference between swimmers and experts during TNT 11–2 (From [20])	39
Figure 15.	SFPD Patrol Boat.....	40
Figure 16.	CBIBS deployment area (left) and sensor buoy (right) (Image from CBIBS website).....	41
Figure 17.	SHARC above and below the surface (Image from Liquid Robotics website).....	43
Figure 18.	BASIL buoy/USV (From [43]).....	44
Figure 19.	ARTEMIS side and top view (From [8]).....	46
Figure 20.	USV <i>Sea Fox</i> (From [44], [46]).....	47
Figure 21.	USV <i>U-Ranger*7</i> and sensor suite (From [47])	49
Figure 22.	UAV <i>Integrator</i> (From [48])	51
Figure 23.	<i>Fury 1500</i> UAV (From [49])	51
Figure 24.	Mini-Helicopter <i>Vellerofontis</i> (Image from CENETIX website)	53
Figure 25.	<i>SR200 VTOL</i> UAV (From [50]).....	54
Figure 26.	<i>APID 60 VTOL</i> UAV (From [51])	55
Figure 27.	SAAB’s <i>Skeldar V-200</i> with its onboard a vessel operator (From [52])	56
Figure 28.	SFPD relay node on San Francisco Port’s Pier 45 (From [20]).....	57
Figure 29.	Mobile Surveillance Radar (Image from Mathworks website).....	58
Figure 30.	CENETIX tools (Image from CENETIX website).....	60
Figure 31.	The CENETIX backbone: San Francisco Bay (left), Camp Roberts (right) (Image from CENETIX website).....	60

Figure 32.	CENETIX Observers Notepad (Image from CENETIX website).....	61
Figure 33.	Wave Relay equipment (Image from Persistent Systems website)	63
Figure 34.	Sector Antenna Array onboard SFPD boat.	63
Figure 35.	Node-Ping Graph	66
Figure 36.	Spectral diagram of ARAM as seen on laptop screen onboard SFPD boat.....	67
Figure 37.	TW-220 CheetahNet radio (Image from TrellisWare website)	69
Figure 38.	Live video streaming between SFPD boat and NPS (Image from CENETIX website).....	70
Figure 39.	SFPD patrol boat PLI (Image from CENETIX website).....	70
Figure 40.	PLI of <i>Marine 2</i> (blue) and <i>Marine 3</i> (green) during February 28, 2012, trial	72
Figure 41.	Live video streaming from <i>Marine 3</i>	73
Figure 42.	Network status on “Solar Winds” platform	73
Figure 43.	Bandwidth Monitor on Solar Winds platform	74
Figure 44.	Live video streaming from boarding team (left) and UAV (right) (Image from CENETIX website)	77
Figure 45.	Riverine-area mesh network (From [56])	79
Figure 46.	USV <i>Sea Fox</i> video streaming (Image from CENETIX website)	80
Figure 47.	Riverine network connectivity at 12.4 nm (Image from CENETIX website).....	81
Figure 48.	Sensing distance measurement between ME1 and ME2 and ARAM spectra diagram (Image from CENETIX website)	82
Figure 49.	Swimmer detection by ashore node (Image from CENETIX website)	83
Figure 50.	Large vessel: HS <i>ARIS</i> at NMIOTC	85
Figure 51.	Swimmer positions on PLI and a picture taken on the vessel hull (From [63]).....	86
Figure 52.	Swimmer video feed and positions on PLI (Image from CENETIX website).....	87
Figure 53.	UAV standoff detection results (Images provided by NMIOTC)	88
Figure 54.	Swimmers Location on PLI during large-vessel search (Image from CENETIX website).....	91
Figure 55.	Network performance statistics during large-vessel search (From [20]).....	91
Figure 56.	UAV–USV pursuit and sensor data (Images provided by NMIOTC).....	92
Figure 57.	Large-vessel search ad-hoc sensor network (From [38]).....	93
Figure 58.	Small-vessel search ad-hoc sensor network (From [38]).....	94
Figure 59.	Swimmer ad-hoc mobile, broadband, wireless-mesh network (From [38])	94

LIST OF ACRONYMS AND ABBREVIATIONS

AFCS	Automatic Flight Control System
AIS	Automatic Identification System
ANTD	Advanced Network Technologies Division
ARAM	Adaptable Radiation Area Monitor
ARDEC/JSAS	Armament Research Development and Engineering Center / Joint Situational Awareness System
C2	Command and Control
CBIBS	Chesapeake Bay Interpretive Buoy System
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CENETIX	Center for Network Innovation and Experimentation
CGYC	Coast Guard Yacht Club
COMINT	Communications Intelligence
DoS	Denial of Services
DTRA	Defense Threat Reduction Agency
E/M	Electromagnetic
EIRP	Effective Isotropic Radiated Power
EO	Electro –Optical
FOI	Swedish Defense Research Agency
GGB	Golden Gate Bridge
GPRS	General Packet Radio Service
GPS	Global Positioning System

GSM	Global System for Mobile Communications
Hellas-Sat	Hellenic Satellite System
IDS	Intrusion Detection Systems
IED	Improvised Explosive Devices
IEEE	Institute of Electrical and Electronics Engineers
IR	infrared
ISR	Intelligence, Surveillance and Reconnaissance
LAN	Local Area Network
LEO	Low Earth Orbit
LLNL	Lawrence Livermore National Laboratory
LOS	Line of Sight
MANET(s)	Mobile Ad-hoc Network(s)
MIO	Maritime Interdiction Operations
MOB	Mobile Operation Base
MPU3	Man Portable Unit GEN3
MPU4	Man Portable Unit GEN4
NATO JCBRN COE	NATO Joint-Chemical-Biological-Radiological-Nuclear Defense Center of Excellence
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NMIOTC	NATO's Maritime Interdiction Operational Training Centre
NOAA	National Oceanic and Atmospheric Administration
NOC	Network Operation Center

OTC	Officer in Tactical Command
PC	Personal Computer
PLI	Position Location Information
PRND	Preventive Radiological and Nuclear Detection
PTT	Press To Talk
QoS	Quality of Service
RF	Radio Frequency
SA	Situational Awareness
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SFPD	San Francisco Police Department
SHARC	Sensor Hosting Autonomous Remote Craft
SIGINT	Signal Intelligence
SNR	Signal to Noise Ratio
SOF	Special Operation Forces
TNT	Tactical Network Topology
TOC	Tactical Operation Center
UAV(s)	Unmanned Aerial Vehicle(s)
UK	United Kingdom
UMV	Unmanned Maritime Vessel
UN	United Nations
USV(s)	Unmanned Surface Vehicle(s)
VPN	Virtual Private Network
VTOL	Vertical Take-Off and Landing

WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WMAN	Wireless Metropolitan Area Networks
WMD	Weapons of Mass Destruction
WMN(s)	Wireless Mesh Network(s)
WSN(s)	Wireless Sensor Network(s)

ACKNOWLEDGMENTS

I would like to thank firstly the Hellenic Navy, for providing me the great opportunity of studying and expanding my academic knowledge in the Naval Postgraduate School.

I would like to thank my advisors, Professor Alex Bordetsky and Commander (USN) John P. Looney for their help and guidance during the construction of this thesis. Their contribution was more than valuable, helping my research to be a unique experience for me.

I have also to express my thanks to Professor Ioannis Koukos of Hellenic Navy Academy, Mr. Eugene Bourakov of the Naval Postgraduate School, Mr. Antoine Burcham of Liquid Robotics and Mr. Antoine Martin of Unmanned Vehicle Systems Consulting for their valuable help and advice when I asked them.

I would also like to thank my parents, Evangelos and Ekaterini, for what they have done and offer to me so far.

Last but not least, I would like to thank my beloved fiancé and future wife, Andreana, for all of her support and patience during my presence and studies at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Since the beginning of this century's sudden outburst of international terrorism, the countries of the North Atlantic Treaty Organization (NATO) have been involved in a concerted effort to eradicate all aspects of terrorism. Several countries (e.g., the United States of America [USA] and the United Kingdom [UK]) are working hard to thwart all aspects of terrorism, including those that threaten the free and safe movement and distribution of goods over the seas. Addressing these maritime challenges requires a large commitment of resources because of the vastness of the seaways, which remain a critical element in militaries' lines of communication and businesses' efficient flow of commerce. Related to the terrorism challenge is piracy. There are some areas in the world where pirate activity remains common (e.g., the Indian Ocean east of the Horn of Africa, the South Coast of Nigeria, and the Strait of Malacca); hence, there are several ongoing, coordinated anti-piracy naval operations. In many ways, the term Maritime Interdiction Operations (MIO) applies well to these efforts to thwart terrorism and piracy on the world's seaways.

B. MARITIME INTERDICTION OPERATIONS (MIO)

A Maritime Interdiction Operation (MIO) is a naval operation that makes use of coercive measures to delay, disrupt, or even destroy enemy forces or provisions on the way to an area of interest—which can be a battle area or an area that represents a potential threat environment—before the enemy does any damage against friendly forces [1], [2]. According to the NATO's operational document for MIO [3], “a Maritime Interdiction Operation (MIO) encompasses seaborne enforcement measures to intercept the movement of certain types of designated items into or out of a nation or specific area. MIOs are normally restricted to the interception and, if necessary, boarding of vessels to verify, redirect or impound their cargoes in support of the enforcement of economic or military sanctions.”

As long as commerce has traveled across the world's waterways, piracy has been a challenge. Today, some parties, whether countries, small segments of society (e.g., the militia in Somalia), or individual crews refuse to comply with international law and threaten security and peace, not only in a particular region, but, in some circumstances, on a worldwide scale. Confirming that these countries or parties are violating international law or international mandates (e.g., United Nations [UN] resolutions) or enforcing sanctions or embargoes may require a complex set of maritime operations. Sanctions may include constraining or denying of supplies or other trading privileges, and even the liberty of moving people out of a particular area. The military objective of a sanction is to impose a selective barrier to control or prevent the traffic of products, persons, or services to or from a particular area. Usually the enforcement of a sanction requires support by a combination of military operations by air, land, and sea. Naval forces usually conduct MIOs during sanction enforcement by attempting to reduce the flow of prohibited items and prevent potential enemy actions in the area of interest. Various factors such as the environment, maritime assets, personnel, the sophistication of the adversary, and logistics affect, positively or negatively, the MIO objective [3].

While an embargo can be established by a country unilaterally, usually it is the United Nations that authorizes the use of such force with a UN Security Council resolution. Apart from the authorization of the UN, a country can use national assets (e.g., ships and planes) to impose an embargo in order to defend against a threat to peace and security as defined by international law [3].

MIO assets normally are eligible to execute the following actions:

- Vessel interrogation for various reasons that do not have to do with navigation safety.
- Documentation and cargo examination.
- Boarding (i.e., embarking an armed party to conduct searches of a vessel).
- Diverting of vessels that refuse to comply with the sanctioning force's directions.

- Seizure of vessels and their cargo if they do not divert as ordered by sanctioning forces [3].



Figure 1. Armed boarding parties conducting MIO (Images from militaryphotos.net and wikimedia.org).

MIOs are an integral part of antiterrorism and anti-piracy operations. MIOs also contribute to short-term and long-term regional security, since they result in the control of all maritime traffic. Additionally, MIOs are used to detain illegal or dangerous cargo transported by ships and to prevent illegal immigration. The transportation of illegal immigrants by vessels from one region to another concerns many nations. Several seaways are used for this illegal activity (e.g., the Mediterranean Sea is a human-smuggling route from Africa and the Middle East to Europe, and the Persian Gulf and Arabian Sea is used as a route from the coasts of Iran and Pakistan to the Arabian Peninsula). It is easily understood that effective surveillance of the seas and execution of MIOs is necessary to significantly constrain these phenomena.

Over the past decade, maritime operations have changed considerably, due to the desire to counter asymmetric threats. These asymmetric threats can be weapons of mass destruction (WMD), radioactive and biologically hazardous material, improvised, explosive devices (IEDs), etc., that can be used during a terrorist attack and, despite their usually insignificant dimensions, can cause disproportionate catastrophe and death. The

threat of these small and lethal weapons requires naval forces to adjust operations quickly and effectively to prevent devastating attacks. An aspect of this adjustment is the rapid development and use of reliable sensors and communications networks in austere environments to enhance friendly forces' ability to detect and interdict these threats while they remain in a remote area (i.e., offshore). Consequently, the means (e.g., communication and networking systems, sensors) to facilitate the execution of MIO and regional security operations have to be evolved.

C. AD-HOC SENSOR NETWORKS IN MIO: BACKGROUND

Unambiguous, robust communications are vital to the success of naval operations such as area surveillance, control, and interdiction. Communications and sensor networks allow the flow of data and critical information that is necessary for the conduct of an operation from both tactical and strategic perspectives. Sensor network communications are affected by several factors, such as the physical environment, network-systems quality, asset positioning, and the electromagnetic environment. Conventional wireless networks have stationary networking infrastructure such as base stations (e.g., buildings and antennas) serving as gathering nodes for traffic emanating from mobile devices. These nodes interact with the base stations in a client/server fashion. When considering naval operations, the situation becomes more complicated: the platforms are hardly stationary, as the networking infrastructure operates from a variety of platforms in motion on the sea, above the sea, and from space, in the case of satellite support [4]. Thus, the objective of this thesis is to examine how unstructured networks are able to effectively communicate in naval operations despite the low coverage of their antennas. Such systems are known as sensor networks or ad-hoc networks.

Sensor networks consist of nodes made up of small sensors that are able to monitor, process, and analyze phenomena over geographical regions of varying sizes and for significant periods. Recent progress in sensor-network technology has led to the invention of small, low-cost sensors that are able to collect and transmit, or relay, sensor data about physical values (e.g., temperature, humidity, and sea state), or dynamic attributes of objects (e.g., speed and direction of movement), and the existence or absence

of substances (e.g., radioactive materials and explosives). These capabilities are useful applications in a number of other maritime operations (e.g., habitat and environment monitoring, healthcare, and military surveillance) [4]. As mentioned by Hans-Joachim Hof [5], the application of a sensor network customarily determines not only the sensor nodes' design, but also the design of the particular network comprising those nodes.

Surveillance is the primary aim of sensor networks used by the military. The purpose of surveillance missions is to collect or verify as much data as possible concerning the enemy's capabilities, positions, and intentions in order to have a detailed tactical overview, along with data about the area of operations. Since manned surveillance missions in forward-deployed areas often involve high risk for friendly forces, the assets assigned to the missions require a high degree of stealth and protection. With advances in sensor networks, many surveillance missions can be achieved with less risk; consequently, the deployment of unmanned surveillance missions, by exploiting wireless sensor networks, is crucial for military and other security-related missions. Nowadays, threats vary from bands and organized groups to unmanned vehicles able to operate above, on, and even below the sea surface. Combining the aforementioned situation with the potential of asymmetric threats such as radiological, biological, or chemical agents makes for a difficult security challenge.

Previous research examined the feasibility and constraints of applying modern sensor-networking technology on Aegean islands. The concept espoused providing information to the Hellenic Coast Guard to enhance situational awareness and decision-making capability [7]. This research was limited to an island-based network topology. In MIO, most sensors are employed on assets moving and operating on the sea surface, or in the air, in the case of unmanned, aerial vehicles (UAVs). Those dynamic conditions hinder reliable connection (i.e., cause range changes among nodes, or interference of physical obstacles between two network nodes) or even interrupt reliable connection among the sensor nodes of the MIO network and require the adoption of methods to facilitate and maintain area coverage. A military wireless-network design is highly affected by signal-propagation phenomena. Many architectures are tested and utilized to ensure that alternative routing and handling of data address potential problems and

drawbacks beyond the standards acceptable in civilian ad-hoc networks. Currently, terrestrial node cannot reach far into open seas; therefore, an aerial platform (e.g., a UAV) or other relay platform (e.g., smart buoys) [8] are a low-cost solution when there is no coverage by a land-based network, or low-earth orbit (LEO) satellite coverage is inadequate or unavailable.

D. THESIS OBJECTIVE

This thesis investigates the use of ad-hoc sensor networks to support maritime interdiction operations in a broad coverage area (i.e., a 50-nautical-mile radius or more). Specifically it investigates the following:

- i) How can be ad-hoc networks be used to robustly support MIO?
- ii) What quality of service (QoS) and survivability advantages do ad-hoc networks provide to MIO?
- iii) What are the limitations of ad-hoc networks supporting MIO?

This thesis develops a foundational understanding of how ad-hoc networks can effectively provide robust communications and flow of information during maritime interdiction operations. It also extrapolates on how these sensor networks potentially benefit other maritime operations.

E. THESIS OUTLINE

This thesis is organized as follows. Chapter I includes introductory material regarding the motivation, scope, and background for this research. Chapter II summarizes the literature review for the concept of the ad-hoc sensor. Chapter III analyzes the operational concept of a MIO ad-hoc sensor network. Chapter IV discusses experimentations on MIO ad-hoc sensor networks and the lessons learned. Chapter V presents the conclusions and potential areas of future research on this particular subject.

II. LITERATURE REVIEW

A. INTRODUCTION

Wireless communication technologies are undergoing rapid advancements. Since the beginning of wireless networking, two categories of wireless networks have emerged: infrastructure networks (e.g., local-area networks (LANs) and wide-area networks (WANs)) and ad-hoc networks. “Ad-hoc” is a Latin expression meaning “for this purpose.” “Ad-hoc networks” is a term referring to networks created for a particular aim. These networks are created on the fly for temporary use, and occasionally for extended lifetime use, depending on their desired role. Usually, ad-hoc networks consist of several workstations (e.g., desktop and laptop computers) or other wireless devices (e.g., cell phones and tablet personal computers) able to establish communications with each other for information exchange [9].

A wireless ad-hoc network is a decentralized type of network without a preexisting infrastructure (e.g., wired networks, routers, or access points) to support it, as in a managed (i.e., infrastructure) type of wireless network. Instead, each node is involved individually in data routing for the other nodes, resulting in a dynamic establishment of nodes that forward data according to the network’s connectivity. Additionally, ad-hoc networks are able to use *flooding* for data forwarding [10]. In the case of a limited or even non-existing network topology, flooding is the simplest form of information distribution through the network nodes [11]. Flooding in a network is the forwarding of data from a network node connected to a router to any other node connected to the router, except to the source node of this data [12]. Flooding is an algorithm that has application in several network scenarios, such as link-state advertisements in wireless multi-hop networks and query propagation in peer-to-peer networks [11].

An ad-hoc network typically refers to any network where the status of all devices is equal and they are free to connect with any other ad-hoc network device in their effective link range. An ad-hoc network makes use of an 802.11 or 802.16 standard mode

of operation established by the Institute of Electrical and Electronics Engineers (IEEE) for worldwide interoperability for microwave access (WiMAX). IEEE 802.11 refers to wireless, local-area networks (WLAN) communications in 2.4, 3.6 and 5 GHz ranges, and typically supports relatively short range wi-fi networks (e.g., home networks). The IEEE 802.16 standard refers to broadband, wireless, metropolitan-area networks (WMAN) in frequencies of 2–66 GHz and data rates of up to 100Mbps, in the case of a mobile nodes network. With the adoption of IEEE 802.16, the data transmitted by a node signal can reach distances of around 50 km (27 nautical miles) [13], [14], [15].

Wireless ad-hoc networks are classified by their application to the following categories [10], [16]:

- Mobile ad-hoc networks (MANET)
- Wireless mesh networks (WMN)
- Wireless sensor networks (WSN)

An example of an ad-hoc network for military purposes is depicted in Figure 2. The network nodes depicted include ships, air and land vehicles, remote sensors, and personnel. They communicate with each other through the network thereby enhancing information exchange during dynamic operations.

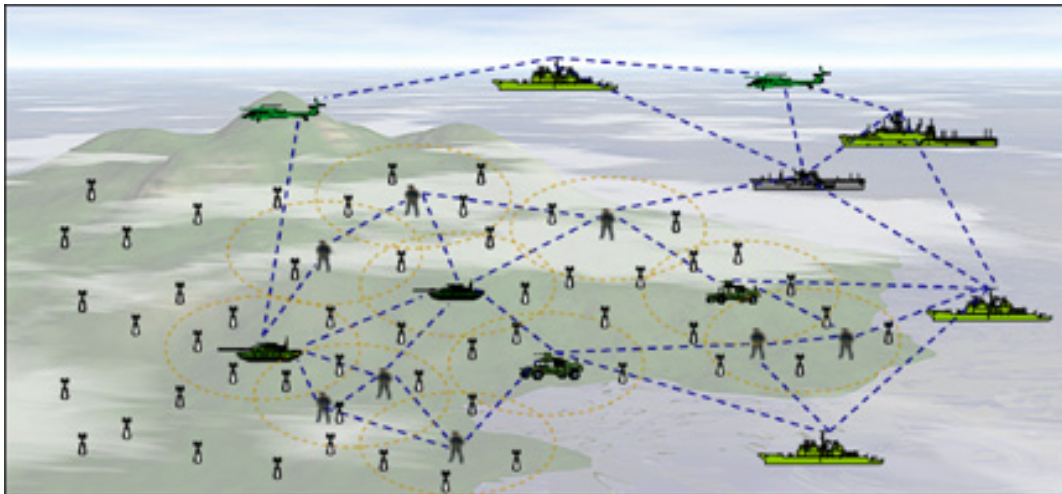


Figure 2. Network for the conduct of military operations (Image from VirginiaTech ECE department website)

B. AD-HOC NETWORK CATEGORIES

1. Mobile Ad-hoc Networks (MANETs)

Mobile, ad-hoc networks (MANETs) are not hinged on centralized and regulated connectivity. Because of the rapid evolution of wireless communication systems, the deployment of independent mobile users, e.g., the establishment of resistant, efficient, reliable, dynamic communication for emergency and rescue operations, and of course military networks, is necessary. A MANET, according to the Advanced Network Technologies Division of National Institute of Standards and Technology, is defined as “an autonomous collection of mobile users that communicate over relatively bandwidth-limited wireless links.” Due to the nodes’ mobility, especially during military operations, the network topology is rapidly altered through time in unforeseen ways. For example during a MIO, since the assets are typically mobile and afloat, the nodes change their location in the network for a variety of reasons, such as human decisions or environmental forces. MANETs are decentralized networks because all network activity, including topology discovery and message delivery, is individually conducted by each node. [16]

A wide variety of networks embody the principles of a MANET such as small, static networks limited by energy sources, to large-scale, mobile, highly dynamic networks. For all applications, MANETs make use of algorithms for efficient determination of network organization, link scheduling, and information routing. In a MANET, many factors significantly affect the viability of routing paths and message delivery in decentralized environments such as variable wireless-link quality, propagation-path losses, attenuation, multiuser interference, alterations of topology, and other factors. In the case of military operations such as MIO, MANETs must also address additional constraints such as connectivity, available bandwidth, energy availability, scalability, and security. Factors like latency, reliability, potential jamming, and restoration from possible node malfunction significantly affect the network’s design and performance. The network adjusts to overcome these factors by altering its routing paths. The potential of a MANET network to expand and get denser, for example, during a boarding phase of a MIO operation where several nodes, such as the boarding team,

vessels, UAVs, or buoys may be present, may result in latency increase and continual node disconnection–reconnection. [16], [17]

Military networks, such as networks for naval operations including MIO, are designed to operate in a way that ensures a low probability of intercept and/or a low probability of detection. Consequently, it is desirable for the nodes to radiate with the least possible power and reduce their frequency of transmission, depending always on operational needs, to decrease the probability of detection or interception. Any deviation in any of these requirements may lead to overall performance and credibility deterioration like interception of information flow through the network and potential malfunction of nodes that may lead to entire collapse of the network. [16]

2. Wireless Mesh Networks (WMN)

A wireless mesh network (WMN) is defined as a communications network consisting of radio nodes organized in a mesh topology. In a mesh topology, the nodes of the network have point-to-point connection with all other nodes of the network. Each node can transmit and relay data to other nodes. This helps ensure the flow of information through the network because the information can reach its destination through alternative paths [18]. An example of a WMN that supports MIO is used by the San Francisco Police Department (SFPD) to monitor maritime traffic at the San Francisco Bay entrance (see Figure 3). The infrastructure of this network is divided into two clusters. The first consists of three point-to-point connections between: (1) the Golden Gate Bridge node (GGB tagged white square in Figure 3) and the Lawrence Livermore National Laboratory (LLNL) node (in Figure 3 its abbreviation is LBNL), (2) LLNL and Alameda Island (the white square toward the bottom and right-center of Figure 3), and (3) Alameda Island and Yerba Buena Coast Guard Station (YBI NOC). Note that the red lines in Figure 3 depict the wireless communications link between the network nodes. The second link cluster consists of two nodes: the GGB connected to Coast Guard Yacht Club (CGYC) (Pier 45 on Figure 3) and to a SFPD patrol boat (not depicted in Figure 3). This second cluster is a mobile mesh network; the future vision is to connect all SFPD patrol boats and make them nodes in a mesh network.

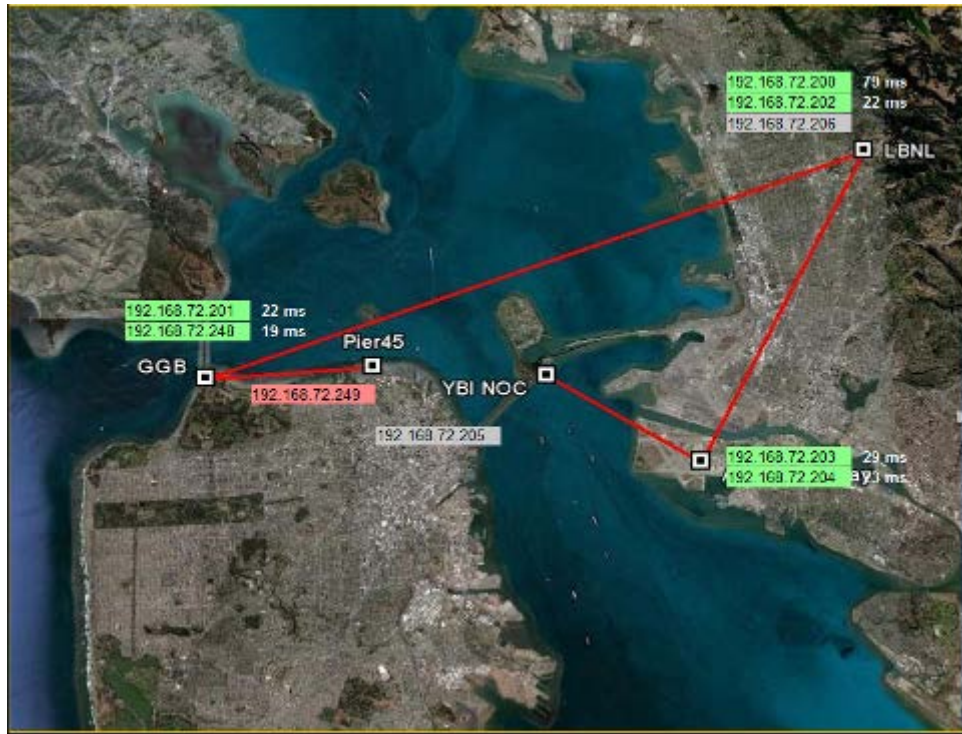


Figure 3. San Francisco Bay Area mesh network backbone (Image from CENETIX website)

Wireless mesh networks usually consist of mesh clients, mesh routers, and gateways. The mesh clients can be portable computers, cell phones, or other wireless devices, while the mesh routers forward traffic to and from the gateways, which are not necessarily connected to the Internet [18]. An example of a mesh network connecting stationary and mobile clients is depicted in Figure 4. WMNs can enable IEEE 802.11 and 802.16 standards. A characteristic that defines a WMN is that the nodes at the core of the network are forwarding the data to and from the clients in a multi-hop mode, resulting in a MANET formation. Apart from the multi-hop requirement, there are no other restrictions on WMN design. Hence, flexibility and versatility are significant WMN characteristics and advantages.

An advantage of a mesh network is its reliability and redundancy. In case a node is not able to operate, the rest of the nodes can overcome this situation by establishing and retaining communications among them, either directly or via one or more intermediate nodes [18], [19]. This is extremely useful for a WMN that supports MIOs,

since the connectivity through the network must be retained even though one or more participating nodes may fail, move out of range, or have its propagation path temporarily blocked. During MIO, nodes often experience the latter two challenges. WMNs have self-healing, self-forming, and self-organization attributes that are beneficial, not only for MIOs, but for military operations in general.

A WMN can be considered a special category of wireless ad-hoc networks. A WMN usually has a more organized configuration and can support dynamic and cost-effective connectivity over a particular and wide geographic area. The mesh routers can be mobile and move according to specific requirements occurring in the network (e.g., the requirements of nodes consisting of vessels that are moving on the sea surface during a MIO). Mesh routers do not usually face the resource constraints that network nodes may encounter because they are usually located within the network topology in such as way as to be supplied with the necessities (e.g., nodes ashore supplied with unlimited energy etc.). This results in an ability of mesh routers to have higher and more reliable performance. [18], [19]

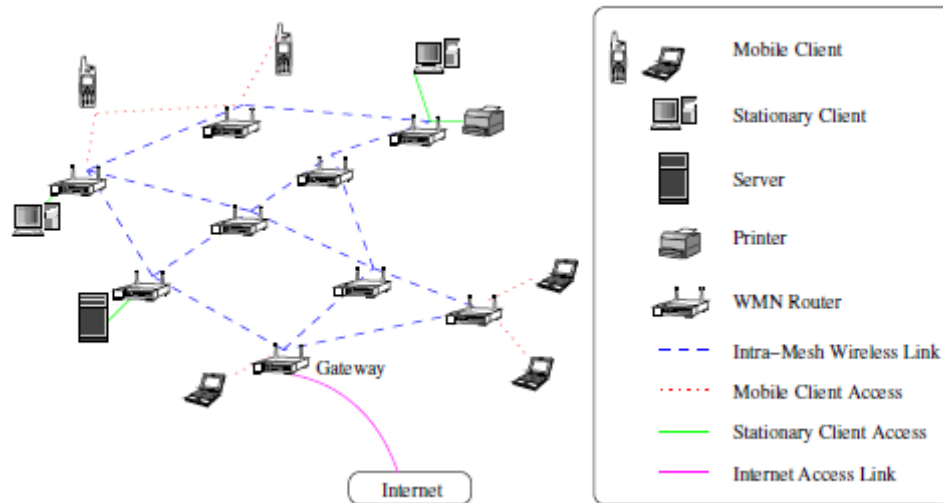


Figure 4. A wireless mesh network interconnecting stationary and mobile clients
(From [19])

Because of their flexibility and adaptability, WMNs can efficiently satisfy the requirements of multiple applications, such as broadband Internet access and mobile user

access and connectivity. Mesh connectivity significantly contributes to network performance enhancement, such as fault tolerance, load balancing, throughput, protocol efficiency, and reduction of effective cost. However, there are drawbacks of WMN that need to be taken under consideration, such as the determination of bandwidth that each subscriber of the network can receive, the security of the network, and the transmission power level that ensures connectivity among the network nodes. [18], [19]

3. Wireless ad-hoc Sensor Networks (WSN)

A wireless sensor network (WSN) is one of the most robust types of networks for wireless communications for both civilian and military use. In a WSN, communication is achieved and maintained with the use of spatially distributed autonomous sensor nodes capable of collecting information (e.g., communications, radar, video, etc.). WSNs typically have a significant number of wireless ad-hoc network features (e.g., the capacity for infrastructure-less setup and minimal dependence on network planning). These characteristics facilitate rapid WSN setup, especially where there is a lack of an existing network or where a fixed infrastructure network is infeasible due to various circumstances (e.g., networks used for tactical battlefield operations). There are both military and civilian WSN applications, such as the detection of an unauthorized person or asset intruding into an area of interest, object tracking, and fire detection. [21]

A wireless ad-hoc sensor network consists of a number of sensor nodes spread across a defined geographical area [22]. Each sensor node has wireless-communication capability and some level of intelligence (e.g., radar, meteorological sensors) for signal processing and dissemination of data. The characteristic that distinguishes WSNs from WMNs and MANETs is that the primary role of a WSN node is not just communication, but mainly data gathering by the sensor and dissemination through the network [22]. The following list contains examples of some wireless ad-hoc sensor networks; it is drawn from the NIST website:

- Military sensor networks for detection of enemy movements or other important phenomena like explosions

- Sensor networks for detection of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials or attacks.¹
- Sensor networks for detection and monitoring of environmental phenomena (e.g., ocean currents or sea states that may affect the conduct of an operation).
- Wireless sensor networks for surveillance and monitoring of navigational traffic in maritime channels or more expanded areas. For example, networks consisting of smart buoys on which radars are mounted for the monitoring of an area such as San Francisco Bay.
- Wireless-sensor surveillance networks for providing security in public places or other facilities monitored by police authorities or security companies

The capabilities of wireless ad-hoc sensor networks have a pivotal role in both civilian and military operations. Wireless sensor networks for geological data, ecosystem monitoring, and weather forecasting are depicted in Figure 5, below.

¹ This kind of sensor networks has a lot of applications during MIO operations since one of the main scopes of MIO is the detection of the CBRNE materials and the prevention of their illegal transportation.



Figure 5. WSNs for geological data, ecosystem monitoring and weather forecasting (Image from Network Intell website)

WSN are classified according to two characteristics: individually addressable nodes and network data aggregation. For example, a sensor node of a network deployed at sea for surveillance should be individually addressable in order to detect and track a target within its coverage area and relay this information to the rest of the network. On the other hand, in a case where other data such as sea state or temperature is needed, perhaps addressability is not important since any node in the area is able to respond. The ability of a sensor network to aggregate collected data, results in a reduction in the number of messages that will be distributed across the network nodes. [22]

Generally, the function of an ad-hoc sensor network relies on the needs that lead to the concept of this particular network. The following roles are important in a significant number of networks [22]:

- Determination of values at a particular location. More specifically, a given sensor node is not necessarily comprised of one sensor type; rather, it can be comprised of different types of sensors, each with a different sampling

rate and measured values. For example, in a MIO network, one sensor node might detect a vessel, another node might collect information for the classification of a vessel, another might sense the presence of hazardous material (e.g., CBRNE) on the vessel, and a final camera sensor might transmit real-time pictures to other nodes of the network.

- Detection of an event of interest, including reporting data about the event's emergence, and estimation or evaluation of the event's parameters. An example is a sensor network designed for traffic monitoring, where police authorities can detect a vehicle moving on a highway and estimate its speed and direction.
- Classification and identification of a detected object. In a network for sea-area surveillance, it is important to correlate a detected vessel with other sources of information such as that provided by the Automatic Identification System (AIS). AIS is required on all vessels over fifteen meters and it broadcasts identification data (e.g., vessels name, departure and destination port etc.) about the vessel it resides on; hence, a contact detected by a node with a radar sensor can amplify the contact with classification information such as merchant vessel or warship.
- Tracking of an object of interest. For example, in a network like the above that is used for the classification and identification of a target, tracking a suspect vessel during its movement through a geographical area is covered by the network. This function is important, since the continuous tracking of a suspicious vessel gives the opportunity for friendly forces to be aware of its position at any time and to interfere when judged necessary by superior authorities. [22]

In all four roles above, the most significant requirement of the sensor network is that the necessary data be distributed to the proper end users. In most cases, the relay of data among the nodes is done under extremely tight time constraints. For example, the detection of a suspect vessel in a maritime surveillance network should trigger immediate

feedback to the authorities (e.g., coast guard or naval forces) responsible for the area. This feedback allows the authorities to take or adjust actions appropriately.

A wireless ad-hoc sensor network, specifically one designed for MIO, requires the following [22]:

- A significant number of sensors. The deployment of many sensors on the sea surface or in the air may be required as events unfold; hence scalability is a major factor.
- Energy consumption: A network designed to facilitate MIO operations, or other naval operations, requires that the majority of sensor nodes are placed in remote areas where maintenance to those nodes may be difficult. An example is a smart buoy node in a sea area: the lifetime of that node depends on the battery life or fuel cell, thus the minimization of energy consumption is necessary.
- Network self-organization. The significant number of nodes and their potential deployment in unprotected and non-friendly locations necessitates that the network have self-organization capabilities, since manual configuration may not be possible. Furthermore, some nodes may stop operating for a variety of reasons, such as destruction or malfunction. Additionally, other nodes may join the network according to the nature of the operation. Consequently, the network must be able to readjust itself whenever necessary to preserve functionality. Even though individual nodes may get disconnected from the network, reliable connectivity has to be preserved at a high level.
- Querying ability. During a MIO, an individual node or a group of nodes may need to be queried (e.g., if hazardous material is detected) for information collected within its assigned region. According to the amount of data fusion performed at a node, there is a potential for the node to face difficulties due to the transmission of a large amount of the data across the network. This situation requires that data from a particular area be

collected by various local sink nodes,² these nodes may create and relay summary messages. A query may be directed to the closest node to the specific location's sink node.

- Collaborative signal processing: One significant difference between WSNs and MANETs is that the objective of a WSN is not only communication preservation among the network nodes, but also the detection/classification of some events of interest (e.g., detection of explosives during the boarding of a suspicious vessel). Data fusion from multiple sensors contributes to improved detection/classification performance during military operations, even though it may result in network architecture limitations, since it requires data transmission and messages control. [22]

Nowadays, with the availability of low-cost, short-range radios along with progress in wireless networking, wireless ad-hoc sensor networks have several applications. Every node can be equipped with various sensors, such as radar, acoustic, infrared, video camera, and radiological. These sensor nodes may be organized in clusters that report local-event detections to the other nodes of the cluster. Nodes in the cluster then fuse the data to form a local estimate. One node can be eligible to operate as the cluster master and fitted with a longer-range radio using a protocol such as IEEE 802.11 or 802.16. The cluster-master node is able to produce a global estimate and report the results to other clusters or to the end node of the network. The concept of cluster master promotes cost and energy efficiency, since long-range radios are expensive and often have excess energy consumption rates compared to typical sensor nodes in a WSN [22], [24].

² A sink node in a WSN is a node where the data collected by other sensor nodes is forwarded. The appropriate placement of a sink node positively affects the energy consumption of the WSN and its potential operating life. In some cases the end node of the network can form a sink node [23].

C. SENSOR NETWORK DESIGN FOR MIO

Ad-hoc networks usually do not have a fixed network infrastructure like that of cellular-phone networks; consequently, rapid deployability and adaptability are advantageous attributes, particularly in the case of networks designed for MIO, and more generally for naval operations. As Seapahn Meguerdichian et al., precisely describe in their article about exposure in wireless ad-hoc networks, [25] “integration of inexpensive, power efficient, and reliable sensors in nodes of wireless ad-hoc networks, with significant computational and communication resources, allows better exploitation of the attributes of this kind of network.” Previous research [6] analyzes multi-objective, evolutionary algorithms for sensor-network design; this can be applied to MIO networks as follows (borrowing heavily from [6]).

1. MIO Sensor-Network Design Philosophy

As Lam Thu Bui et al [6] describe, a wireless sensor network typically consists of a significant number of sensor nodes, individually processing and executing simple algorithms and exchanging information with each other and a fusion center via wireless communications channels. Sensor networks are used for monitoring and possible control of units during military operations (e.g., surveillance, regional security monitoring, hazardous-material detection, etc.). When designing a network to support MIO and regional security monitoring operations, the lifetime maximization and information that can be extracted from the network are put in balance with energy consumption, latency, and deployment cost.

Sensors of WSNs for MIOs and naval operations can be distributed randomly in austere environments, such as open seas with rough conditions, or in particularly well defined positions, such as a sensor network for surveillance of a maritime channel, such as the SFPD mesh network (Figure 3). In all cases, the sensor nodes are coordinated to obtain continuous communication through the network, exploiting the multi-hop phenomenon with several clusters and cluster heads. Cluster heads are powerful sensor nodes with higher battery capacity and processing capability than that of conventional sensor nodes.

The sensors of the MIO or security network capture the data (e.g., radioactive-hazard detection), process it, and relay it to the other nodes or to a base station³, if it is within communications connectivity range. Each specific application defines the data reporting frequency and the sensor's number that processed the data. Some issues that affect and define the whole design of a MIO sensor network are the following:

- *Fault tolerance* is a significant factor during the network-design phase because the sensor nodes are susceptible to potential malfunction and may run out of energy, since they are not supplied with limitless power.
- There are enough limitations on the energy, processing, and storage capacities of the sensor nodes depending to the role and nature (e.g., node equipped with radar requires consumes much more energy than a node with a camera or CBRNE sensor) of each particular network node.
- *Scalability* is significant, since a MIO and other dynamic military tasks have the potential to require a rapid change in the number of participating assets and nodes.
- Topology changes have to be considered, since the mobility of some nodes during MIO may result in difficulties in the communications among other nodes (e.g., because of distance, physical obstacles, or electromagnetic environment).
- Since environmental noise and other propagation effects (e.g., scattering and ducting) affect all communication and sensor-systems performance, it is well understood that data transmission through the network has to overcome the above phenomena.
- *Survivability* of a MIO network has to be examined thoroughly because sensor networks are data centric: the loss of a few nodes may cause severe degradation of the network and lead to operational failure [6].

³ A base station can be the end node of the network where all the data is gathered, processed, and evaluated and can be either on a ship or on land.

2. Sensor Placement Problem in MIO

Theoretically, sensor placement should be based on some optimal node locations that maximize the flow of data stream (e.g., characters, voice, and video data, etc.) through the network. In practice, however, a MIO poses significant optimization limitations due to constantly changing node positions, and range and propagation path challenges. In a MIO, it is not necessary to maintain connectivity among all nodes, but it is among those nodes that have a critical role in the delivery of information to the desired end node. The main factors affecting node positioning are the following:

- The *detection probability*, which indicates the efficiency of the sensor network to detect a target.
- The *deployment cost*, which depends on the sensor numbers. In the case of a homogeneous network, the cost is proportional to the number of sensors. As MIO networks are heterogeneous (i.e., their nodes have different capabilities and roles), the deployment cost is given by the equation $C = \sum_{i=1}^n C_i T_i$, where n is the number of nodes, C_i is the cost of a node of type i , and T_i is the number of nodes of type i .
- Since the nodes of the network transmit data, *energy consumption*, depends on the distance that data is transferred between the nodes and the sink. The energy consumption of the network is calculated as the total energy consumed at each individual node. In a MIO network, where some nodes are portable and cannot be supplied with infinite power (i.e., they are dependent on batteries, fuel cells, or solar panels), energy consumption is a key factor.

There is much research investigating the sensor-placement problem from detection and coverage perspectives (for example, see Kar and Banerjee [2003] [26], Jourdan and De Weck [2004] [27]). While each research project has much the same scope, they have different approaches to the problem. For example, one project examines the placement problem for grid coverage, developing an iterative sensor-placement algorithm for optimal area coverage. Other researchers approach this problem from the

perspective of enhancing the detection of scattered targets in a particular area. Regardless of their approach, all researchers aim to reduce sensor numbers through simultaneous optimization of coverage, connectivity, and asset lifetime. A method used by Ferentinos and Tsiligridis (2007) is the selective activation of network sensors. Some nodes work as cluster heads to get optimal energy consumption and application requirements, such as uniformity of sensor measurements, while addressing connectivity limitations [6], [28].

3. Mobile Agent⁴ Routing

Obviously, data transmission among the sensor network nodes, uses, apart from energy consumption network bandwidth. This situation results in possible delays in information relay and network-performance reduction. For this problem, a mobile agent is used to fuse the data according to operational needs. The agent-routing problem aims to compute mobile agent routes to ensure maximum detection accuracy and minimize energy consumption and path-loss effects. More specifically,

- Detection accuracy is calculated as the sum of the detected signal energies of all nodes along the route. Ensuring higher detection accuracy lets the sink extract appropriate conclusions about target data, such as type and location. For example, during the boarding phase of a MIO, a reliable sensor for IED detection can inform the end node (e.g., the officer in tactical command [OTC]) of the presence or absence of explosive materials in the investigated vessel. This leads to a decision by the OTC regarding the need for further evaluation and actions.
- Because of free-space propagation, there is signal attenuation in each link of the mobile agent route that deals with path loss, and this has to be addressed—actually minimized—to obtain the required communication to support the MIO. The path loss of a route is equal to the sum of path loss along each link of the route. According to Friis’s free-space propagation

⁴ A Mobile Agent is a hardware unit with high communication and processing capabilities employed to traverse the network (e.g., aerial or ground vehicles or even light nodes able to hop through the network) when data gathering and network maintenance is required. Continuous presence of these agents during network operation is not required [29].

model, the relation between the power P_{rj} received by sensor j and the power P_{ti} transmitted by sensor i is given by the following equation (2.1):

$$P_{rj} = \frac{P_{ti} G_{ti} G_{rj} \lambda^2}{4\pi^2 d_{ij}^2 \beta}$$

Equation 2.1: Friis's free-space propagation model [6]

where G_{ti} is the gain of transmitting sensor antenna i , G_{rj} is the gain of the receiving sensor antenna j , λ is the wavelength of the transmitted signal, d_{ij} the distance between the two sensors, and β is the system loss factor. The path loss of the wireless link in dB is given by the following equation (2.2)

$$PL_{ij} = 10\log(P_{ti} / P_{rj})$$

Equation 2.2: Path loss of the wireless link in dB [6]

Also, the total path loss through a path is the sum of the path losses of each individual link along the path, given by the following equation (2.3):

$$PL(P) = \sum_{i=0}^{l-1} PL_{n_i, n_{i+1}}$$

Equation 2.3: Total Path loss [6]

where l is the total number of nodes along the path.

- The energy consumption of a route, like the sensor-placement problem, is equal to the total energy consumed by each sensor of the route during data processing and transmission.

There are several advantages to using mobile agents in a WSN. Some of those advantages are latency reduction during data transmission, autonomous operation,

information retrieval in balance with energy consumption, and simultaneous data processing. Mobile-agent applications include target detection, localization, classification, and surveillance of an assigned area. The determination of route (i.e., the sequence and number of sensors, that a mobile agent follows defines the accuracy of detection, energy consumption, and path loss of the route [6].

4. Data Aggregation

Data aggregation is the process by which data from multiple sensors is gathered to address and eliminate unnecessary transmissions, providing the flow of information through the network and the arrival of this information at the end node. The main scope of data aggregation is to congregate the most crucial data from the sensors and make it available to the end node in an energy-efficient mode with minimum-possible data latency. This process is useful, not only for MIO networks, but for every military WSN because during a military operation, there is a significant and sometimes rapidly increased flow of data based on the development of events during an operation. It is absolutely necessary to transmit the data from some of these events; however, some data may not have much importance at a particular moment. For example, in a MIO network during the vessel-seizure phase, perhaps the information that needs to reach the end node soonest is video pictures taken by the boarding team, and not information about atmospheric conditions in the area. Data-aggregation algorithms are very important, since they contribute to network lifetime and data-accuracy enhancements that are related to energy efficiency. The energy efficiency of a WSN depends on various factors, such as network architecture, data-aggregation mechanisms, and underlying routing protocols [30]. More specifically:

- *Data accuracy* relies on the applications of the sensor network. For example, during target detection, its location estimation at the sink determines data accuracy [6].
- *A data aggregation* is considered energy efficient if it maximizes network functionality (e.g., energy consumption increases the lifetime of network nodes ensuring the robust flow of information through the network). Using

the hypothesis that all sensors have the exact same role, energy-consumption minimization of each sensor has to be applied. [30]

- *Network lifetime* is the number of data aggregation rounds that it takes until a predefined percentage of sensors cannot operate any more, due to their available-power depletion.[6]
- *Latency* is the delay occurring in data transmission, routing, and data aggregation. Actually, latency is defined as the intermediate time between the transmission of the generated data from a node and its reception at the network's end node [6].

5. Area Coverage

Wireless sensor networks, either for MIO or for other military purposes, aim to monitor and cover their pre-assigned area. Coverage is one of the most important factors and is a measure of network quality of service (QoS). The coverage area of the network is defined as the fraction of the whole assigned area and that which is covered by the totality of network sensor nodes. Coverage, network lifetime, and deployment cost are the most significant factors for the area-coverage problems of a sensor network. It is easily understood that to ensure the coverage of a particular area by a sensor network, each location of interest in the monitoring region has to be within the effective range of at least one sensor. This situation is achieved with the activation of a subset of sensors, which results in the coverage of every location of interest while other sensors of the network that do not possess vital data can hibernate to conserve power. So the collected data can be relayed from the sensor node to the sink with successive relays through the array of network nodes [6]. An example of a network where the information from a source node arrives at the destination node with successive relays is depicted in Figure 6.

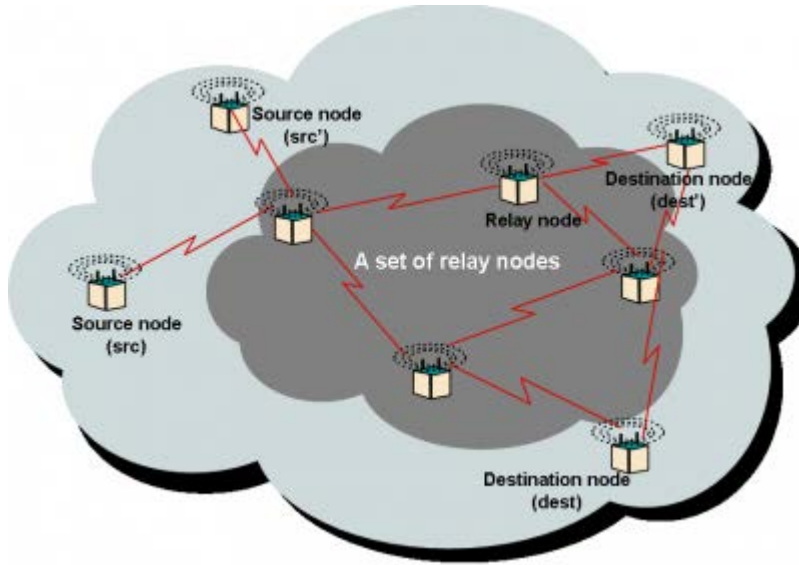


Figure 6. Multi-hop relay in a network (Image from Nomadic Technologies website)

The model that is usually used in order to define and depict a sensor node's coverage area is a disk in two dimensions or a sphere in three dimensions. Any point within the area is considered covered by the sensor node. In reality, the coverage area differs, since the presence of obstacles cannot be excluded. For a MIO, obstacles to coverage are often islands, large vessels crossing the area of interest, and even environmental conditions such as fog. These may interfere with the line of sight (LOS) between two or more nodes. Obstacles affect the propagation of radio frequency (RF) signals (for communications) and electromagnetic (E/M) signals (for sensors such as radars). This happens because obstacles may absorb or reflect the signal depending on the nature of the obstacle; obstacles render the area behind them invisible to the sensor node. Some research on the coverage problem uses a two-dimensional field as its model. Even though it is much easier to develop algorithms for a two-dimensional versus a three-dimensional model, the extracted results may not be sufficient for many real-world environments. Real coverage issues are predicated in three dimensions, since the nodes of a network can be deployed on land, sea, underwater, in the air, or in space. [31]. A model of a three-dimensional coverage diagram is depicted in Figure 7.

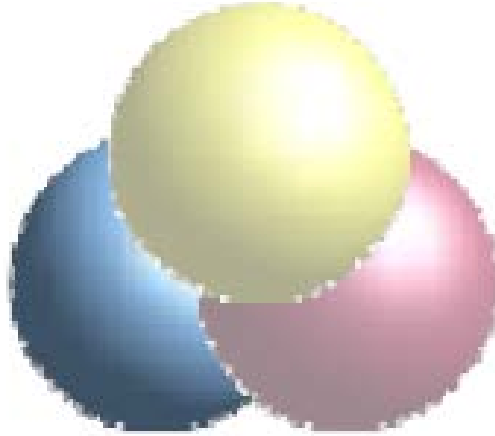


Figure 7. Three-Dimensional Coverage Model (From [31])

Apart from two- and three-dimensional models for the determination of a sensor-network coverage area, a “Voronoi diagram” is frequently used during network studies. The Voronoi diagram for a sensor network consists of polygons depicting boundaries around each sensor, such that every point within a sensor’s boundary is closer to that sensor than any other sensor in the network. Voronoi diagrams are used by researchers to detect potential shadow areas in coverage and extract deployment protocols to control sensor movement. The vector-based algorithm forces network sensors to alter their position to fill a coverage hole in any of their Voronoi polygons. The Voronoi-based algorithm directs a sensor towards a coverage gap [31]. A Voronoi diagram is depicted in Figure 8.

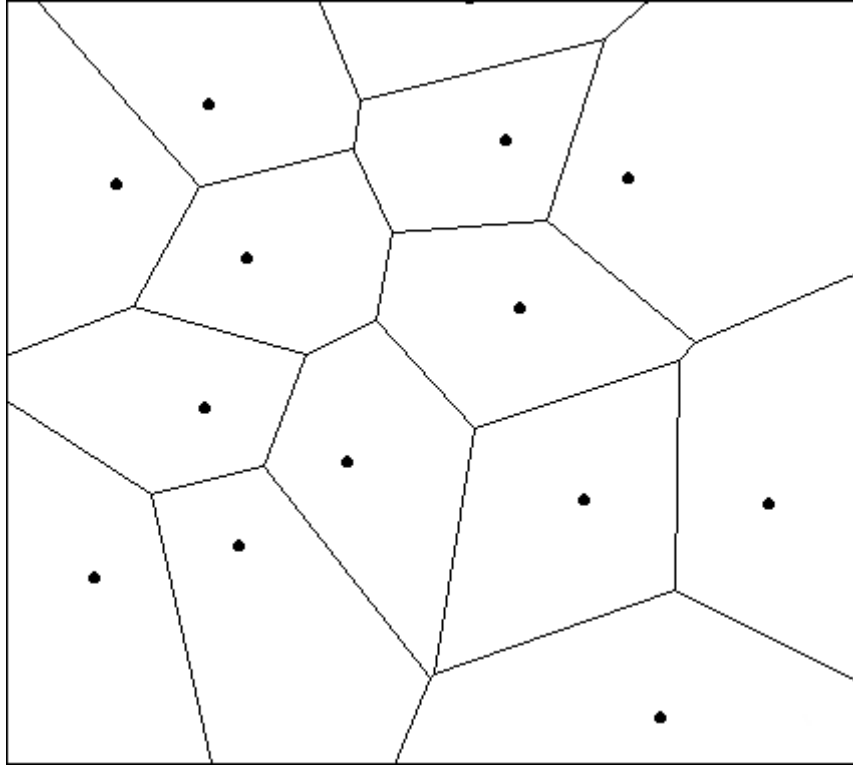


Figure 8. Voronoi diagram (From [31])

The sections above make it clear that the design and concept of an ad-hoc network for MIO and regional security operations needs significant forethought and examination. Operational requirements need to be put in balance with asset availability and effective cost, not only for network construction but also its functioning (e.g., maintenance and energy consumption). The progress over the last decade in sensing and communications technology gives opportunity and flexibility for the accomplishment of this scope, since there are a huge variety of methods and means that can be employed for the construction of those networks.

III. MIO NETWORK OPERATIONAL CONCEPT

A. OPERATIONAL REQUIREMENTS FOR MIO NETWORKS

A network designed for military and general regional security purposes has to provide reliable communications among the participating nodes and facilitate the flow of information—voice, video or data—during the operation. Moreover, network adaptability is critical to allow adjustments based on current circumstances and future operations demands that may affect the network (e.g., node positioning and increases in the amount of data transmission requirements).

In MIO and other regional maritime security operations, the majority of the nodes are not stationary, but move and operate on the sea surface or in the air. This attribute burdens the network and affects performance. Moreover, as in all military operations, the flow of data may increase excessively during an operation's execution, hence network adaptability is key to ensure tactical success by enabling all necessary information to reach the end node of the network. That end node can then relay the information wherever needed. Since the flow of information can be high enough, the network must have the capacity to support the amount of communication and provide sufficient transmission speeds as well as security and reliability of information flow.

The network for a MIO must consist of various kinds of sensor nodes. Some nodes must be equipped with radar devices for ensuring the surveillance and monitoring of an area within their effective range; other nodes need a camera to transmit real-time pictures/video; others may have electro-optical (EO) and infrared (IR) equipment for better surveillance and target classification at night. Equipment used for detection of CBRNE material is necessary for MIO and regional security operations. For example, the boarding team during the sweep phase of a MIO may transmit real-time video from the suspect ship from helmet cameras while simultaneously transmitting information from CBRN sensors. In the case of maritime security in an expanded area, the presence of

nodes whose role is just to relay the data to the end node (multi-hop) is essential. The number and the type of nodes of the network are highly related to the area of interest and potential threat.

Previous research [32] makes a precise analysis of the attributes that a network designed for a MIO must have. According to Stavroulakis, some critical factors that affect network performance are the sufficiency and portability of equipment, since MIO teams must employ portable devices when embarking on a vessel during the boarding phase of a MIO, and the network might need to scale up because of environmental challenges, such as electromagnetic interference and weather conditions.

As mentioned above, the power capacity and consumption of a node, whether portable or deployed on the sea surface during an operation, is a significant factor that affects the design of the network and the planning and execution of the operation. During the design phase, there must be consideration for this issue and alternative solutions in case some nodes become depleted of energy. For example, the boarding team must carry additional power-supply devices such as batteries for the equipment, or other assets must be placed in such an array that a node that runs out of energy is covered by another node, facilitating the uninterrupted flow of information.

In the case where multiple boardings are required, the deployment time (i.e., transport and set up) of the network equipment used by the team affects mission success because slow MIO operations can cause a host of mission problems (e.g., increased surveillance requirements of waiting ships and health/sanitary problems arising of waiting ships). Furthermore, the dimensions of the equipment may affect network overall performance. For example, it is obvious that portable equipment must be within a particular size and weight to be carried and used by the boarding teams. In regional security operations when nodes are on buoys that are deployed temporarily to facilitate networking, they must have a shape and weight that allows for storage and timely, satisfactory deployment from a ship or aircraft.

Another critical factor in operation execution is the effective range for direct communication between two nodes of the network and the overall effective transmission

range with the multi-hop effect exploitation. During MIO and regional security operations, a primary goal is the interdiction of dangerous material before they reach a vital area (e.g., port or population center). Moreover, during MIO execution, the command post in tactical command may need to keep a safe distance from the seized vessel to avoid damage in case of explosion or bio-hazardous emissions from the cargo. The effective communications range of each node (i.e., the per hop transmission range) that a node covers relies on several factors, such as frequency, transmission power, antenna gain, signal-to-noise ratio (SNR), height of antenna, and atmospheric conditions. The effective communication range significantly affects the number of nodes required to ensure the uninterrupted flow of data and, consequently, the total cost of the network construction and management burden. Theoretically the range within which two nodes can communicate is derived by the following Friis propagation model fundamental equation (3.1):

$$\frac{P_{rj}}{P_{ti}} = \frac{G_{ti}G_{rj}\lambda^2}{4\pi^2 d_{ij}^2 \beta}$$

Equation 3.1: Friis propagation model fundamental equation [6]

where P_{rj} is the power of the received signal at node (j) sensitivity, P_{ti} the transmission power of node (i), G_{ti} is the gain of transmitting sensor antenna i, G_{rj} is the gain of the receiving sensor antenna j, λ is the wavelength of the transmitted signal, R_{ij} the distance between the two sensors (i), (j), and β is the system-loss factor. Ad-hoc network nodes usually communicate within line of sight (LOS), and their communications range is calculated by the following equation (3.2):

$$R_{LOS} = 1.23(\sqrt{h_1} + \sqrt{h_2})$$

Equation 3.2: LOS communications range [33]

where R_{LOS} is the range measured in nautical miles, and h_1 , h_2 the height of each node antenna from sea level, measured in feet. The height of the antenna depends on the location of the node, for example, if the node is on a ship, we may have an antenna height

of 50ft or more; if we have a small boat it will not exceed 15 ft; and in the case of a buoy, the antenna is likely to be at most 6–7 ft tall. However, despite those calculations, current ad-hoc networks nodes have limited ranges, unless they make use of the SATCOM or WiMAX standard, rarely exceeding 4 km (2.2 nautical miles), depending on the factors mentioned above and affected significantly by energy-availability constraints. So, to avoid a high-density vertices network⁵ that may be costly, somewhat difficult to deploy, and may require the nodes within the transmitting area to be silent so as not to corrupt transmission [34], the assets should be able to transmit data as far as possible. However, the data will be transmitted to the end node of the network by using the multi-hop effect through the nodes. Willis and Kikkert developed a model showing that communication between two nodes separated by 10 km (5.4 nautical miles) is not only feasible, but reliable as well. However, their model considered a frequency of 40MHz and an effective isotropic radiated power (EIRP) equal to 1 Watt transmitted over irregular terrain, an attribute that the sea surface terrain does not have except in rough seas [35]. A distance of 5.4 nautical miles is highly desirable for networks designed for MIO and regional security operations, since a non-excessive number of nodes can cover a wide area.

A fact affecting the communication of the maritime nodes is the mobility of the majority of the assets, since they are not permanently stationed. This constant movement on the sea surface and in the air results in continuous increases or decreases in node separation. However, for avoiding the potential of limited or even no communication among some nodes, making the arrival of information to the end node impossible, an option of implementing alternative equipment that provides vertices with Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS) or satellite communications has to be considered. Also a potential employment of WiMAX or IEEE 802.16 standard in the networks can dramatically increase the communications range among nodes, and consequently the network coverage, since the transmitted signal can reach at distances beyond LOS to around 50 km (27 nautical miles) with high data rates up to 100 Mbps [14], [15]. Moreover in order to simplify the communication of the

⁵ High-density vertices networks are networks composed by a large amount of nodes gathered in a small area. The number of the network nodes is disproportional to the area where the network operates.

nodes, such as transceiver-antenna alignments in the case of directional antennas, omnidirectional antennas should be used instead of directional.

Since MIO take place at sea, the equipment used must have resistance to sea conditions such as humidity, temperature changes, water, and salinity. For example, the equipment used by swimmers and divers who check the hulls of suspect ships obviously needs to be waterproof. Furthermore, the equipment must be tolerant of the vibrations caused by sea waves. Assets such as buoys that are deployed for network facilitation and/or surveillance have to retain stability on the sea surface regardless of the sea state.

Another factor to consider during the network design phase is the electromagnetic interference that affects network nodes, not only with external/out-of-network assets such as radar and radio transmission from ships, but also the mutual interference among nodes. Since there may be multiple vertices equipped with radar, their transmission can cause problems to the communication within the network. During the execution of a MIO, the presence of ships equipped with radar transmitting under high power may cause burdensome electromagnetic interference. Addressing this problem entails defining transmission sectors for radars, lowering/managing output power, or, if necessary, using means of communications other than the network [32].

A significant requirement for ad-hoc sensor networks supporting MIO and regional security operations is the security of information distributed through the network. Since there is no physical connection between nodes, and data is distributed over the air using electromagnetic waves, there is the potential that the transmitted information may be intercepted by anyone within a node's transmission range. The network is also vulnerable to cyber attacks, such as malicious codes resulting in denial of services (DoS) or even the collapse of the entire network. IEEE 802.11 provides security to the network with the use of open or shared key authentication and static wired-equivalent privacy (WEP) keys. Security of the ad-hoc sensor network can be enhanced with the use of a virtual private network (VPN) and intrusion-detection systems (IDS). A VPN tunnel encrypts the transmitted data additionally to the WEP encryption. VPN can be used as well for the encryption of WiMAX (IEEE 802.16) standard communications. [21], [36].

For ensuring continuous and reliable functionality during an operation, a network operation center (NOC) should be established, not necessarily in the area of operations. The NOC assists in managing and monitoring the network. A primary function is monitoring all the participating nodes to ensure that they are connected to the network and working properly. If monitoring uncovers problems in the network, then the NOC assists in providing solutions whenever necessary. Another role of the NOC is to provide accessibility to new users/nodes on the network, an attribute necessary for MIO networks that alter the number of participating nodes. The NOC can make use of several applications for network management such as fault management/service restoration, trouble-ticket administration, configuration management, security management, performance management and accounting management [37]. A picture of network performance monitoring used by a NOC is depicted in Figure 9.

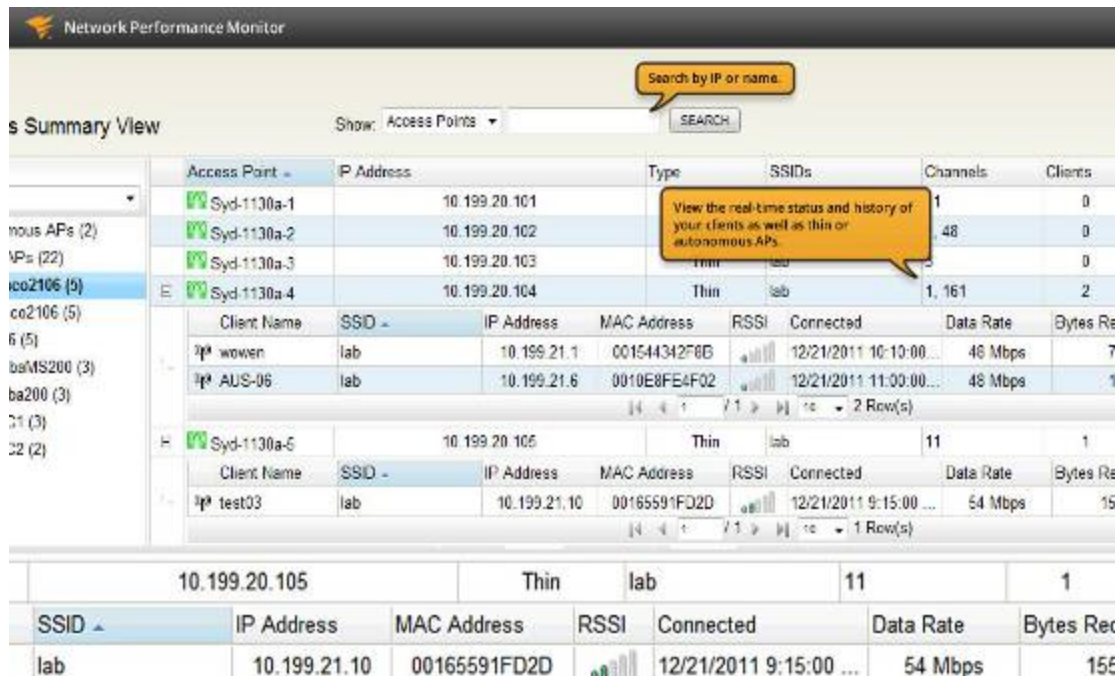


Figure 9. Network Performance Monitor (From Solarwinds website)

B. ASSETS CONSISTING OF NODES IN A MIO NETWORK

MIO and naval operations related to regional security generally take place at sea, either close to coastal areas or far away from shore on the open sea. It is obvious that the

majority of assets used for the conduct of an operation will be deployed at sea or in the air. However, the use of shore-based stations cannot be excluded, especially when the operation evolves near a coast. The assets that may carry nodes of a MIO ad-hoc sensor network are the boarding team (in the equipment carried by the team), surface vessels (ships or boats), aerial vehicles such as UAVs, unmanned surface vehicles (USVs), buoys, swimmer or diver equipment, and shore-based nodes, whether mobile (e.g., trucks equipped with sensors and antennas or personnel with equipment) or stationary (e.g., a headquarters, an antenna, or a sensor for relaying data to other nodes).

1. Boarding Team

During a MIO, a team may board a suspicious vessel. Apart from inspecting the ship's documentation (i.e., manifest) and crew (e.g., checking the crew and passenger list against watchlists), the team may search for the presence of illegal and dangerous material in the cargo such as CBRNs or IEDs. The data from sophisticated sensors can be transmitted from the boarded ship to another station for evaluation. For the detection of this material, the team has to carry appropriate sensors as they search the ship. A sensor that may be carried by the boarding team is the adaptable radiation area monitor (ARAM) developed by Lawrence Livermore National Laboratory (LLNL). According to NPS-LLNL field-experiments and student studies, ARAM is already integrated into the mesh network of SFPD patrol vessels in San Francisco Bay Area for long-term data capture and analysis. The ARAM system makes use of commercial constituents and software developed by LLNL for preventive radiological and nuclear detection (PRND) for MIO [20]. An ARAM sensor is depicted in Figure 10.



Figure 10. ARAM sensor (from [20])

The LLNL software processes the detection signal from the sensor, providing a diagram of the gamma-count rate or gamma-energy spectrum, and with the use of “Glau” software, stores the gathered data and produces spectrum files that are available to users of the network, informing them about the existence of radiological material [20]. A diagram of a gamma count rate with the use of Glau software is depicted in Figure 11.

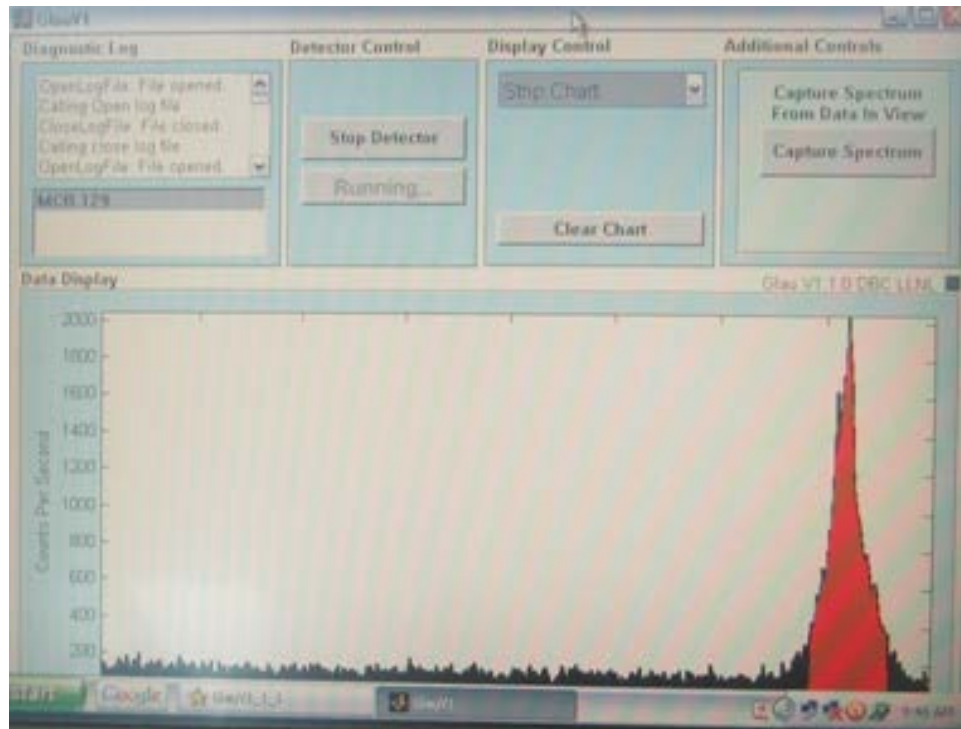


Figure 11. Glau software showing a spike in gamma-count rate (from [20])

Furthermore, the boarding team can have video and voice equipment to transmit real-time pictures from the ship to other nodes of the network to assist scientist in properly and efficiently identifying the source material. The exchange of information can be enhanced through text chatting between the boarding team and other participants in the network such as CBRN subject matter experts. All data gathered—picture, video, and sensor data—from the CBRNE detection sensor can be transmitted from the suspect ship through the network with the communications equipment carried by the boarding team.

2. Swimmers - Divers

During MIO and regional security operations, the deployment of swimmers or divers in the area of interest may be required to investigate the hull of a seized ship or conduct a security check on an object floating in the area of interest for assessment as a potential threat. Swimmers should be able to transmit real-time pictures through the network via video and voice devices. They may also be able to detect with portable sensors whether a suspicious object contains CBRNE material and transmit that data for further evaluation by a subject matter expert brought into the network. Obviously the equipment carried by a swimmer must be waterproof. During the TNT MIO 11–2 (June 2011) and TNT MIO 12–2 (June 2012)⁶ experiments, networked swimmers were employed as part of the experiment and successfully transmitted video, voice, and data from a portable WMD detector [38]. Networked swimmers for the TNT 11–2 experiment are depicted in Figure 12. The portable detector used by swimmers is shown in Figure 13, and a snapshot of transmitted video and a videoconferencing window between the swimmers and remote experts is shown in Figure 14.

⁶ The subject of TNT MIO 11-2 and 12-2 experiments was the “Networking and Interagency Collaboration On Maritime-Sourced Nuclear Radiological Threat Detection and Interdiction”. These experiments were conducted with the cooperation of NPS/LLNL, NATO Maritime Interdiction Operational Training Center (NMIOTC), NATO Special Operation Forces (SOF) Headquarters–Belgium, NATO Joint Chemical–Biological–Radiological–Nuclear Defense Center of Excellence (NATO JCBRN COE), Swedish Defense Research Agency (FOI), and the University of Bundeswehr and Armament Research Development and Engineering Center/Joint Situational Awareness System (ARDEC/JSAS).



Figure 12. Networked swimmers for TNT 11-2 (Image from CENETIX website)



Figure 13. Portable detector used by the swimmers for TNT 11-2 (Image from CENETIX website)



Figure 14. Transmitted video and videoconference between swimmers and experts during TNT 11–2 (From [20])

3. Vessels

Apparently, ships and boats can form almost any type of node in a MIO network. With the communication and detection equipment that they may have available onboard, they are able to operate as a communications relay node, and as a sensor node that distributes data such as video or radar, IR, or EO pictures of the area where the ship is deployed, and/or data concerning meteorological and atmospheric conditions. They can also operate as the end node of a network that gathers, processes, and evaluates all data collected by the other nodes of the network. A ship acting as an end node can be the flagship of a group or division of ships that execute MIO or other naval operations. An important advantage of ships acting as nodes is the fact that they do not have the energy constraints that other assets/nodes, such as buoys and UAVs, face. With the variety of detection and communication means onboard, they can collect and transmit data in

several ways to the desired destination, even to nodes that are not necessarily part of the network. Also, ships have the ability to repair potential equipment failures because of trained and specialized crew members; making them highly important to network performance. Ships may also carry and deploy, according to operational requirements, additional nodes, such as the boarding team (even though the team itself cannot be considered a node), swimmers, buoys, UAVs and USVs. An SFPD patrol boat that constitutes a node in the SFPD mesh network in San Francisco Bay Area is shown in Figure 15.



Figure 15. SFPD Patrol Boat

4. Smart Buoys and USVs

MIO and regional maritime security operations require the involvement of several types of assets. The extent of the area of operations may vary in scale from small areas (e.g., a maritime chokepoint encompassing a few square miles) to large area (e.g., surveillance of an expanded area for the detection and interdiction of a suspect for acts of piracy vessel at the Horn of Africa). Obviously the coverage of a wide area is much more complicated than that of a small area. The wider the area, the higher the number of assets/nodes required to reliably cover the area with a sensor network. The number of

vessels/units deployed for an operation's needs is not limitless and it is affected by several factors such as unit availability, operational evolution, assignment priorities, weather conditions, and, of course, cost. To avoid the employment of a significant number of ships and UAVs as nodes, the use of buoys as communications-relay nodes or sensor nodes can be an acceptable and cost-effective solution.

Buoys are widely used as sensors for the monitoring and gathering of meteorological, oceanographic, and atmospheric data. They transmit this data to several users through satellite or GSM/GPRS communications. An example of a buoy network is the National Oceanic and Atmospheric Administration's (NOAA) Chesapeake Bay interpretive buoy system (CBIBS) that has been deployed in the Chesapeake Bay area since 2007 — see Figure 16 [39].

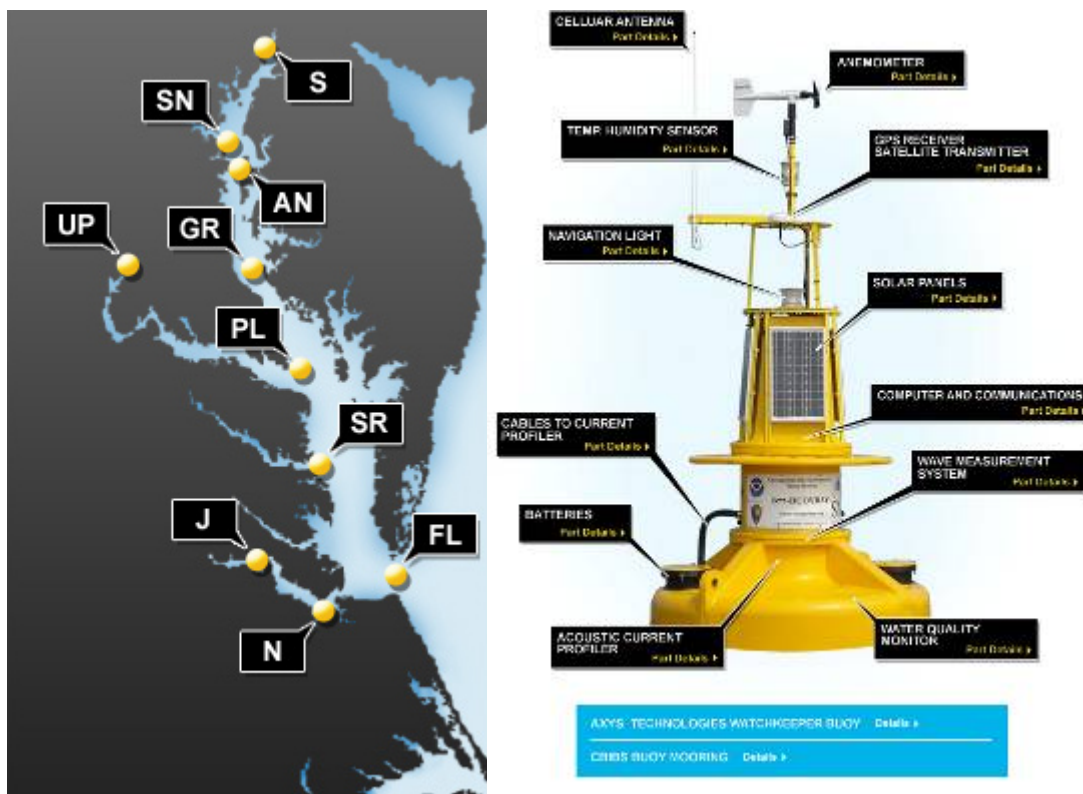


Figure 16. CBIBS deployment area (left) and sensor buoy (right) (Image from CBIBS website)

Since buoys are regularly used as sensors for environmental monitoring purposes, they are also able to work as sensors for naval operations. Apart from radar and environmental sensors, cameras and EO/IR devices can be installed, and with the use of the communications equipment, the data collected by sensors on buoys can be distributed throughout a wireless network. The combined use of sensor buoys, ships, and air assets can reliably and effectively cover a wide area. A buoy with a camera can transmit real- or near real-time pictures of the area around it. That data may facilitate decision making by a headquarters responsible for the area of interest. For example, a target detected by radar (perhaps installed on a buoy) is difficult to classify if there is no other information or intelligence about it. The camera allows the participants in the network to see the detected target and provide more data towards identifying it. Hence, by taking advantage of sensor buoys as nodes in a MIO or regional security network, the continuous monitoring of a wide area can be achieved.

There are several ways that buoys can be used in a MIO network. Apart from monitoring a particular area, the buoys may have only a communications relay role during an operation. In a MIO network, the buoys can be placed permanently in position for the specific operation (e.g., as a communications relay node during the boarding phase), or can float and move towards an area (at very low speeds of around two knots). However, a moving buoy is considered an USV or unmanned maritime vessel (UMV).

A buoy/USV that could be used as a node in an ad-hoc sensor network is the Wave Glider sensor-hosting, autonomous, remote craft (SHARC) developed by Liquid Robotics, Inc. SHARC is a buoy and USV that is able to travel, patrol, or remain stationary. It is equipped with solar panels to collect, transform, and distribute solar power to installed sensors. SHARC's propulsion system is passive and works with the glider and fins that operate seven meters below the surface. The glider ensures system stability on the surface and converts wave energy to movement giving the SHARC a speed of up to two knots, according to sea state. SHARC is highly reliable in retaining its stability and operations in rough weather. It has been tested during a 22-ft sea state and winds of 50 knots off the Alaskan coast [40]. Figure 17 shows how SHARC looks on and below the ocean's surface.



Figure 17. SHARC above and below the surface (Image from Liquid Robotics website)

The MIO-related systems and sensors that have been installed on a SHARC are the global positioning system (GPS), AIS, cameras, and meteorological sensors. Some subsurface sensors that have been installed include a camera, and acoustic and oceanography sensors. It has satellite and local communications capabilities for the transmission or relay of collected data. From the energy perspective, apart from the solar panels that can give 80 Watts of power, it is equipped with rechargeable batteries with 665 Watt-hours autonomy for the systems supply needs. A significant attribute of the SHARC is its minimal visual and radar signature that make it difficult to be detected by enemies and potential saboteurs [41], [42]. With the proper communications equipment, SHARC can be a significant part of a MIO network, as a sensor node or just for communications relay. Its ability to move lets it take a position among the nodes of a MIO network to ensure the uninterrupted flow of data, as it was explained in Chapter II concerning the Voronoi diagram (see Figure 8). Due to its dimensions and weight, shipboard storage of a SHARC and temporary deployment according to operational demands is feasible. A matter that should be examined is the potential for mounting CBRN sensors and surveillance equipment such as radar on it, to transmit information about CBRN materials and emissions, and a real-time radar picture of its area to the other nodes of the network. However, this has to be examined in balance with the energy

consumption rates of the sensors. Moreover, the mounting of heavy equipment with heights more than six feet may significantly affect the stability of the SHARC.

A buoy/USV that can be also used capable of acting as a node of a MIO sensor network is the *BASIL* self propelled buoy developed by a French company “ACSA Underwater GPS.” *BASIL*, like the SHARC, can be stationed in a particular position or navigate to desired locations or patrol patterns. However, it is not as resistant to rough sea conditions as the SHARC, since its maximum operation limit is sea state 3. Its maximum speed approaches three knots and its duration of autonomous operations is around eight hours. Its propulsion system is electrical. The navigation modes of *BASIL* are manual, route following and station keeping. Due to its dimensions (3.4 x 1.5 x 1.2 meters) and weight (380 kg), it can have large payload capable of holding several sensors on it such as cameras, CBRNE sensors, and network communication equipment. Since the current system design allows up to eight *BASIL* USVs to be controlled together, dynamic coverage of an area and multiple simultaneous sensor measurements can be achieved. However, the autonomy of eight hours with the electric propulsion system does not allow a long-term deployment of *BASIL* like the respective of SHARC. So *BASIL* is more likely to be deployed close to ports for the security enhancement of the area [43]. A picture of *BASIL* is depicted in Figure 18.



Figure 18. *BASIL* buoy/USV (From [43])

The main disadvantage of using a buoy as a sensor node in a MIO ad-hoc sensor network is the energy constraints and lack of mobility that this type of platform has. The solar panels and the battery that a buoy has for energy needs face difficulties in supporting the continuous operation of a radar system or other surveillance equipment, such as EO/IR systems, that consume significant power. A possible solution for this problem has been developed by SignalGeneriX, a Cypriot Company, in cooperation with Hellas-Sat (Hellenic Satellite System) and the Maritime Institute of the Eastern Mediterranean; it plans to construct a novel multipurpose, energy-autonomous, smart buoy named ARTEMIS that is able to operate in harsh weather at sea and relay data gathered by a variety of environmental and security sensors. ARTEMIS's dimensions and weight exceed those of a SHARC; it is eight meters tall and is made of aluminum for minimization of movement and maximization of the oscillation period. ARTEMIS has a hybrid power system consisting of both solar panels and a diesel power generator. According to requirements, the buoy is able to switch from the one power system to the other to satisfy energy needs. This system allows the buoy substantial autonomy even with radar use. Additionally, for saving energy, ARTEMIS can perform "sleep and wake up" and "hibernation" modes when there is no operational requirement. ARTEMIS has two platforms where sensors can be adjusted, one above and the other below the surface. According to ARTEMIS project representatives, this buoy "can house from one to hundreds of off-the-shelf analogue and digital sensors, meeting the needs of different demanding environmental, search and rescue, security and military applications." These attributes render it a useful tool in a MIO or regional security network when mounted with the appropriate sensing and communications equipment [8]. ARTEMIS's side and top view are depicted in Figure 19.

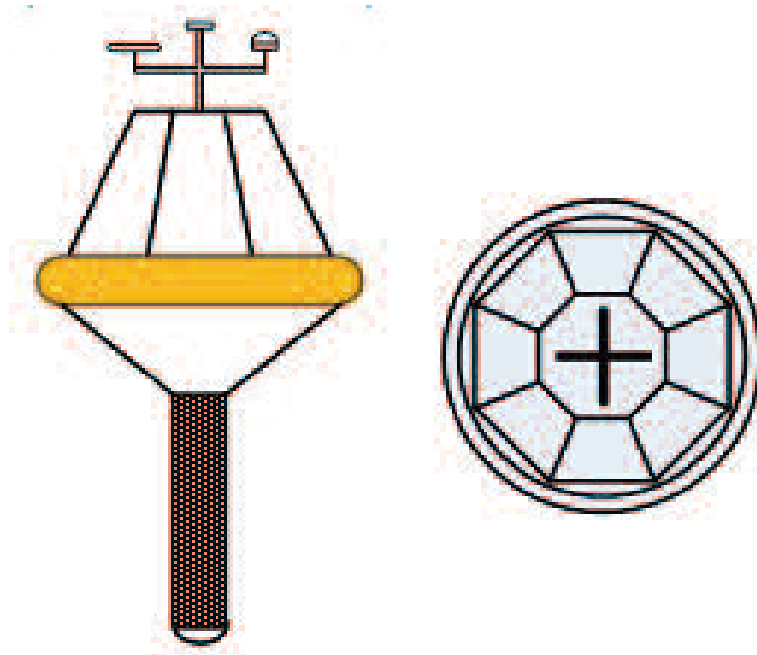


Figure 19. ARTEMIS side and top view (From [8])

One disadvantage of buoys as nodes in a MIO network is the exposure of the sensors and communications equipment to rough conditions, especially when a buoy is placed permanently at sea. The equipment has to face temperature alterations, humidity, salinity, and winds. Obviously, maintenance of a buoy is necessary, but the further away it is from the coast, the more difficult it is to maintain and repair it.

Besides buoys, USVs such as small remote-control or autonomous navigation boats can be employed as nodes of an ad-hoc MIO network. These small craft can be equipped with a wide array of sensors for the investigation of items floating at sea that swimmers or staffed units may be hesitant to approach. When such an item is detected during an operation, the small USV can be deployed by another unit (e.g., a warship conducting a patrol) to examine it at close range and transmit data to other nodes that can remain aloof from the potentially dangerous object. The small dimensions of many current USVs allow for their storage and deployment from a wide array of vessel such as destroyers and patrol boats.

Not only are there small remote-control craft, but USVs with dimensions like the SFPD patrol boats (see Figure 15) have been developed and can be employed as nodes of a MIO network. A *Sea Fox* USV participated in many TNT MIO network experiments that are described in chapter IV. The *Sea Fox* is a USV developed by “Northwind Marine” company. Based on a 17 ft rigid hull inflatable boat (RHIB), the *Sea Fox* is a semi-autonomous, high-speed USV capable of conducting unmanned Intelligence, Surveillance and Reconnaissance (ISR) operations. It can contribute to Force Protection, Riverine, and Port Security missions, to name a few. *Sea Fox* carries Command and Control, Communications and Intelligence (C3I) systems. Its typical configurations provide wide bandwidth video, IR and remotely controlled video camera and floodlights, and an announcing system. Additionally, *Sea Fox* has operated with radar, sonar, CBRNE detectors and swimmer detection systems. With those systems the USV is able to provide other nodes of the network, through wireless RF relays, a remote, real time picture (e.g., video or IR) of potential threats, thereby simultaneously increasing safety and situational awareness during potentially high threat operations [44], [45]. The 17 ft *Sea Fox* is 7 ft wide and weighs approximately 1300 kg. The command and control link for remote control operates at a frequency of 440 MHz and the communication equipment for the mesh network works at 2.4 GHz. The maximum speed of *Sea Fox* is around 35 knots [46]. USV *Sea Fox* is depicted in Figure 20.



Figure 20. USV *Sea Fox* (From [44], [46])

Another example of a USV that can be used as a node of MIO and Regional Security ad-hoc sensor network is the *U-Ranger**7 USV developed by “Calzoni Marine Handling and Lighting Solutions.” According to *U-Ranger**7 specification sheet, this USV is “able to operate as a stand-alone system or integrated in a higher level defense system.” *U-Ranger**7 is equipped with sensors such as radar, IR and video camera, and with its communication equipment, it can be remotely controlled and disseminate through the network the data collected by its sensors. Apart from the above sensors categories, CBRNE sensors can be integrated with it. According to Calzoni, the *U-Ranger**7 is designed to conduct ISR operations, patrolling, port protection, piracy interdiction and vessel escorting. It can also conduct search and rescue operations, and take over the role of a communication relay node in a network. The control modes of USV *U-Ranger**7 are autonomous, remote control, and manual. In the first case, the vessel moves according to a preplanned route and speed, all the while recording its position and collecting data by its sensors. In the second case, the USV is remotely controlled over a wireless communications link from a manned control console located ashore or on another at-sea platform. In the manual mode, the vessel is being driven by a person onboard, so it is no longer a USV, rather just a manned power boat. While the *U-Ranger**7’s maximum speed is 40 knots, it is capable of 12 hours of autonomous operations at a speed of 12 knots. These 12 hours of autonomy makes it highly desirable as a sensor network node for MIO. Moreover its size of 7 meters and weight of 1700 kg allows it to be carried by naval ships such as frigates, destroyers, auxiliary ships [47]. Figure 21 shows *U-Ranger**7 with its sensors.



Figure 21. USV *U-Ranger**7 and sensor suite (From [47])

5. UAVs

UAVs are “mini” airplanes and helicopters, and they are becoming prevalent in ongoing operations. As mentioned before, some sensor nodes can move in airspace, and conduct either surveillance or communications relay according to the needs and the topology of the network. Since staffed, large aircraft may be too expensive or vulnerable, UAVs offer a good option to participate in ad-hoc sensor networks.

UAVs can be equipped with several types of sensors, apart from their communication systems. A UAV is able to execute surveillance operations with radar or cameras, a task that is greatly enhanced by the altitude and speed that this type of asset can achieve. Besides the area-surveillance role, UAVs can relay information on a suspicious vessel within its assigned area by flying above it, discovering what kind of cargo this vessel carries, and assessing whether or not there are people on its deck, etc. The collected data can be transmitted to the other nodes of the network with the featured communications equipment. As in the case of the previously discussed assets, a UAV is able to perform the role of a communications-relay node—they are in fact the best asset for this role due to their antenna height. This antenna height, especially for fixed wing UAVs that can fly at high altitudes, enable them to establish communications with other nodes of the network in greater ranges than a surface assets can. Equation (3.2) explains this phenomenon. However, the communication-effective range does not rely only on node positioning, but also on factors relevant in equation (3.1). Consequently, the effective communications range, even though it is improved by increases in altitude, is

still limited to a few nautical miles, unless these assets have alternative communication systems like satellite communications or GSM/GPRS and WiMAX. Thus, appropriate positioning and assigned sectors for the nodes, even of UAVs, are required for uninterrupted flow of information through the network.

A fixed-wing UAV may be outfitted with CBRNE detectors, but it is difficult to take advantage of these sensors because aircraft cannot hover above and safely pass close enough to a target to detect CBRNE materials. Another disadvantage of fixed-wing UAVs is that they need space for launching and landing. This space is difficult for many ships to provide except for aircraft carrier type ships. Most of the current fixed wing UAVs operate from land-based stations, resulting in significant reduction in the time they can remain in the area of operations when far away from the coast. To address these problems, runway independent fixed wing UAVs or mini-helicopter UAVs are a convenient and reliable solution.

A runway independent UAV that can effectively form a node in a MIO sensor network is the *Integrator* developed by “Insitu Inc.” The *Integrator* is able to disseminate exceptional SA with its high quality imagery sensors and its long endurance. A significant attribute of this UAV is its versatility to accept payload integration according to each individual mission since the payloads are “plug and play.” The sensors that the *Integrator* carries are EO, IR and video cameras, and a laser rangefinder. These sensors can be removed and replaced with other type of sensors such as CBRNE detectors. With the current communications equipment, *Integrator* can communicate at distances over 55 nautical miles and its effective operational range is a radius of 550 nautical miles. Its dimensions (wing span 4.8 meters and length 2.2 meters) allow it to be carried and stored by a ship, but the launch and recovery system is a pneumatic catapult and Skyhook wingtip capture system respectively. Its endurance is 24 hours, which renders it a valuable tool for a MIO and regional maritime security operations. Its cruise speed is approximately 55 knots and the maximum operational ceiling is 15,000 ft. *Integrator* is guided by a control station from the ground or on a vessel at sea [48]. A picture of *Integrator* with its launch catapult is depicted in Figure 22.

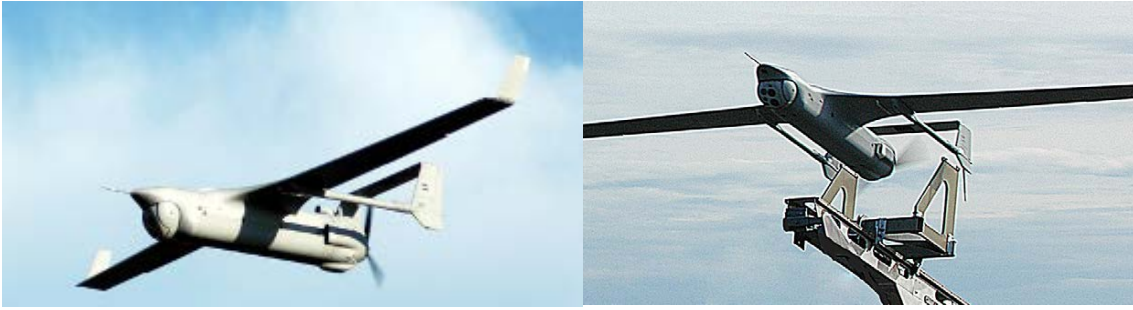


Figure 22. UAV *Integrator* (From [48])

Another example of a runway independent UAV that could serve as a node of an ad-hoc sensor network for MIO and regional security operations is the *Fury 1500* developed by “AME Unmanned Air Systems.” It has a very long effective operational range (1500 nautical miles) and it is designed mainly for ISR missions. Its endurance is more than 15 hours and its cruise speed and maximum altitude is 65–95 knots and 15,000 ft respectively. In a MIO network, the *Fury 1500* could form either a communications relay node or a sensor capable of disseminating through the network data collected by its own sensors such as video-camera, IR sensors, etc. It has a wing span of 3.7 meters and length 1.4 meters with maximum weight, including fuel and payload, of 150 kg [49]. A picture of *Fury 1500* is depicted in Figure 23.



Figure 23. *Fury 1500* UAV (From [49])

A fixed wing UAV like those just mentioned is not able to hover above a suspicious target in order to detect illicit material. This constraint is ameliorated by rotorcraft UAV such as mini-helicopters. A mini-helicopter is able to operate from a ship, can be carried and stored easily on a ship, and can hover above a suspicious target or floating object. Due to this latter attribute, a mini-helicopter can approach very close to a target in comparison to a fixed-wing UAV. A mini-helicopter can operate as a communications-relay node and can have CBRNE sensors and cameras for surveillance. A radar system is difficult to mount because of the mini-helicopter's small size and carrying capacity.

During the TNT MIO 11–2 and TNT MIO 12–2 experiments near the NMIOTC, described in chapter IV of this thesis, a mini-helicopter UAV named *Vellerofontis* was equipped with a nuclear-material detector, a surveillance camera, and a networking node. The UAV's role was the detection of radiological materials from above as suspect vessel on the move. The network equipment allowed the UAV to transmit detection data and video from a vessel in real time to the other nodes of the network. The employment of the mini-helicopter extended the range of the detection network during a pursuit of a suspicious vessel by friendly patrol forces [38]. This demonstrated that mini-helicopters are a responsive and capable asset to investigate the existence of dangerous materials or WMD onboard a vessel or floating object. With the use of a UAV helicopter as the node of a MIO network, the safety of personnel and units can be improved. Furthermore, UAV helicopters may form a communications-relay node, extending the range of the network and ameliorating its operational limitations. A picture of the mini-helicopter *Vellerofontis* with its equipment is depicted in Figure 24.



Figure 24. Mini-Helicopter *Vellerofontis* (Image from CENETIX website)

The *SR200* Vertical Take-Off and Landing (VTOL) rotorcraft UAV could be employed as a node of a MIO ad-hoc sensor network. *SR200*, developed by “Rotormotion LLC,” is equipped with a video camera and an EO/IR sensor. Other types of sensors like CBRNE detector are feasible. It has GPS for navigation purposes and location data transmission. The *SR200* can be controlled either manually by a ground station ashore or afloat, or automatically with an autonomous preplanned route. It is able to take off and land automatically with the use of GPS and an Automatic Flight Control System (AFCS). It utilizes an 802.11 telemetry system. The gathered sensors data is disseminated via the 802.11 system through the network. Its endurance is more than five hours and its operational speed approximately 50 knots. Its dimensions (2.8 and 3 meters length and main rotor diameter respectively) and weight (around 50 kg with the payload) allows its deployment from small vessels such as patrol boats [50]. A picture of *SR200 VTOL* UAV is depicted in Figure 25.



Figure 25. SR200 VTOL UAV (From [50])

Another VTOL UAV for MIO and regional security operations is the *APID 60* developed by the Swedish company “CybAero AB” in 2012. The *APID 60* is a state of the art UAV VTOL system consisting of the UAV, the network enabled control station and the payload system that can be EO, IR sensors, cameras, Synthetic Aperture Radar (SAR), Signal or Communications Intelligence (SIGINT or COMINT respectively), CBRNE sensors, communications relay equipment and loudspeakers according to user demands. It is also equipped with AIS for vessel identification. The *APID 60* UAV can fly either semi-manual remotely from the ground or ship-based control station or automatically according to a preplanned route. Its current data-link communication system can provide real time information to distances of 110 nautical miles. Similarly to *SR200*, the *APID 60* UAV is able to approach, land and lock-down on a ship’s deck automatically with the use of an automatic ship’s deck landing system. It is made from titanium, carbon fiber and aluminum, which renders it corrosion resistant and lightweight. Its length is 3.2 meters with a rotor diameter at 3.3 meters. It flies at speeds of 50 knots (cruise speed) with an endurance of six to eight hours and it has a maximum speed of 85 knots. Its total weigh with payload and fuel (gasoline or JP-5) is approximately 230 kg. This UAV can form a valuable tool for a MIO and many naval operations due to its

capabilities for payload and communications and permit stand-off detection and engagement with suspicious vessels [51]. A picture of the *APID 60* UAV is depicted in Figure 26.



Figure 26. *APID 60* VTOL UAV (From [51])

One other reliable VTOL UAV for MIO network support is the *Skeldar V-200* developed by “SAAB technologies.” It is able to carry several payload types such as radar, AIS, EO/IR and video cameras, and CBRNE detectors. It can be controlled remotely through a data-link at distances more than 55 nautical miles. Its maximum speed is 70 knots and its endurance more than 6 hours. Its overall length with the rotor is 5.2 meters and the maximum take-off weight is 230 kg [52]. A picture of *Skeldar V-200* with its onboard vessel operator is depicted in Figure 27.



Figure 27. SAAB's *Skeldar V-200* with its onboard a vessel operator (From [52])

6. Land-Based Stations

Apart from mobile assets in the sea or air, land-based stations can constitute nodes of a MIO or regional security network. These stations can be either stationary, such as buildings and sensors infrastructure (e.g., radars, communications antennas), or mobile assets, such as trucks equipped with surveillance and communications systems, or even people wearing sensors.

The use of land-based stations for MIO depends on the area of operations and its distance from the coast, which is related to the effective communication range among the network nodes. Land-based stations can form any kind of sensor nodes in a MIO and regional security ad-hoc sensor network. They can be equipped with surveillance systems such as radar, EO/IR devices and cameras, meteorological sensors, and communications equipment in order to relay to other nodes the data collected by them and from other sensor nodes of the network. For example, a node equipped with a radar device can execute surveillance of the area within its radar effective range and transmit the picture to other nodes of the network. In the case of dense islands in the area, e.g., the Aegean Sea in Greece, the establishment of a significant number of sensor nodes can increase the coverage of the network, thereby enhancing both surveillance and communication ranges. Kotsifas (2010) examined the construction of an island-based topology network for the

needs of the Hellenic coast guard. The network was intended to create more efficient surveillance and maritime situational awareness in the Aegean Sea for countering illegal immigration in this area [7].

A land-based node, such as a building, can form the end node of the network (e.g., a headquarters) where all data collected by other nodes is gathered, processed, and evaluated for further action. It can also transmit the data to other users who are not necessarily participants in the network. The advantage of a stationary, land-based node is that a variety of sensing and communications equipment can be installed. There are typically no space constraints and energy limitations, since the node is usually provisioned by the area's power-supply infrastructure or portable generators. A land-based, communications-relay node of the SFPD mesh network positioned at Pier 45 in San Francisco Port is depicted in Figure 28.



Figure 28. SFPD relay node on San Francisco Port's Pier 45 (From [20])

If a node for communications relay or some other role is required where there is no stationary asset, a mobile node, such as a vehicle, can be employed. The asset can collect data and relay it to other nodes of the network within its communication-systems range. A mobile surveillance radar, mounted on a truck, is depicted in Figure 29.



Figure 29. Mobile Surveillance Radar (Image from Mathworks website)

Obviously, there is a variety of platforms that can be used in an ad-hoc sensor network for MIO and regional security operations, and more coming on line every day. This leads to flexibility and performance and cost trade-offs. Furthermore, the continuous evolution of both communication and sensing systems contributes significantly to network design options and enhanced performance potential to meet current operational requirements. However, the fact that the nodes are located on different kinds of assets requires thorough examination of network design and of the equipment necessary for interoperability and data exchange throughout the network. As mentioned previously, ad-hoc sensor networks have already found application in real-life environments, and experiments are being conducted that employ all kind of assets to better comprehend how these networks can be utilized for MIO and regional security operations purposes.

IV. EXPERIMENTATION FIELD

A. CENTER FOR NETWORK INNOVATION AND EXPERIMENTATION (CENETIX)

As mentioned previously, a series of annual experiments are being conducted regarding ad-hoc sensor networks in support of MIO and security operations. During these experiments, useful conclusions about the benefits and potential drawbacks of this kind of network are extrapolated, resulting in a better understanding of the concepts behind them, and how to operate these networks to satisfy operational requirements. A series of experiments related to MIO were conducted under the aegis of NPS in cooperation with USA and non-USA organizations such as DTRA, LLNL, the Department of Homeland Security, and NMIO TC under the leadership of NPS's Professor Alex Bordetsky. A significant tool for the facilitation of experiment execution is the Center for Network Innovation and Experimentation (CENETIX).

CENETIX was founded in 2004 to facilitate research related to self-organizing tactical networking and collaboration. The research subjects that CENETIX studies are flexible and scalable wireless networks, network-controlled unmanned vehicles, sensors, and situational-awareness (SA) platforms. CENETIX incorporates and operates the NPS tactical-network topology (TNT) and MIO testbed. These "plug and play" experiment venues extends from NPS to Camp Roberts (California), the San Francisco Bay Area, Fort Eustis (Virginia), and the port authority areas of New York and New Jersey. These venues are connected via CENETIX's VPN to key experts at various centers of excellence in the USA and overseas [53]. CENETIX fields several tools that facilitate experiment execution and enhance the flow of data through network nodes. Users are able to communicate with each other via video-conferencing and text chat applications, and share video, voice, and data files through the Observers Notepad tool. Pictures of CENETIX tools, the CENETIX backbone (San Francisco Bay and Camp Roberts in California), and Observers Notepad are depicted in the following Figures (30, 31, and 32, respectively).



Figure 30. CENETIX tools (Image from CENETIX website)



Figure 31. The CENETIX backbone: San Francisco Bay (left), Camp Roberts (right) (Image from CENETIX website)

Observer's Notepad (nps-noc1).

Add comment:

Submit

Currently active:
fanis
NOC-CTX-STRATCOM

Chapter: SFPD_050611

X

New Chapter:

Date and Time	Comments	Attachment	Delete
5/6/2011 3:12:26 PM	EB: TW connectivity check from SFPD boat. Five TW units are posting their PLI to SA.	Replace Delete	X
5/6/2011 2:49:01 PM	EB: TW radio PLI posting is confirmed. On-board video feed was activated from NPS. Sensor data capturing file was initiated from NPS and successfully uploaded to Observer Notepad.	Replace Delete	X
5/6/2011 2:45:35 PM	LLNL Sensor update. File Spec-5-6-2011_14-54-51.xml is attached.	Replace Delete	X
5/6/2011 12:35:44 PM	EB: desktop sharing on 192.168.72.21 is confirmed from TNT network to allow start file capturing and video feed from remote.	Replace Delete	X
5/6/2011 12:26:32 PM	EB: SFPD boat route	Replace Delete	X
5/6/2011 12:13:34 PM	EB: be advised - boat video is off	Replace Delete	X
5/6/2011 11:59:39 AM	sfpd: Confirm video at NPS	Replace Delete	X

Figure 32. CENETIX Observers Notepad (Image from CENETIX website)

Since 2004, NPS, with the cooperation of LLNL, the United States Coast Guard, first responders in San Francisco Bay, New York, and New Jersey under the Department of Homeland Security, and USA federal and international academic and military agencies (e.g., NMIO TC and FOI), has conducted a series of TNT/MIO experiments. The main scopes of these experiments are: (1) network performance, (2) advanced sensors and collaborative technology assessment, (3) the detectability of CBRNE material, and (4) the establishment and preservation of ship-to-ship and ship-to-shore communications via tactical wireless network connectivity. The results yield high quality cooperation between command-and-control (C2) organizations and expert centers on a worldwide scale for the rapid detection, identification, and proper response of CBRNE threats in various geographical areas [54]. For the execution of these TNT/MIO experiments, systems such as sensors, vessels, UAVs, and USVs have been extensively used alongside actual security operators, and facilitated by off-the-shelf and specifically designed CENETIX

tools. TNT/MIO experiments have already taken place in San Francisco Bay, port authority areas of New York and New Jersey, riverine areas in Virginia, at the NMIOTC in Greece, and various locales in Germany, Poland and Sweden. Some of those experiments and the lessons learned during their execution are discussed below.

B. SAN FRANCISCO BAY AREA

The experimental mesh network of the SFPD in the San Francisco Bay Area is intended to monitor Bay Area maritime traffic and disseminate sensor data and coordination communications (e.g., video conferencing and voice transmissions) for the radioactive-material detection mission conducted from nodes on operating SFPD boats and stationary nodes (see page 11) to *expert centers* connected to this network. Next, the employment of patrolling marine boats (see Figures 15 and 34) from the Coast Guard and the SFPD—with simultaneous integration of network - enabled detection and classification by reach-back to experts — took place for the first time in 2010, during the TNT/MIO 10–2 experiment [55]. Since then, the San Francisco Bay mesh network has been a significant part of TNT/MIO 11–2 and 12–2 experiments and is characterized as long-term because its execution expands, usually on a weekly basis or more frequently throughout the year, compared to other portions of TNT/MIO experiments that last only a few days.

1. Network equipment

The SFPD mesh network utilizes the Wave Relay ad-hoc networking system provided by Persistent Systems, LLC. The infrastructure of the mesh network uses two man-portable units, GEN4 (MPU4) and GEN3 (MPU3), the quad radio router, and the sector-antenna array, as depicted in Figures 33 and 34. The quad radio router is interconnected with the 5-GHz sector antenna-array system. This antenna is omnidirectional with a high gain value. Due to its significant vertical beam, it provides robust connectivity between naturally unstable network nodes, like those deployed for maritime operations [56].



Figure 33. Wave Relay equipment (Image from Persistent Systems website)



Figure 34. Sector Antenna Array onboard SFPD boat.

More specifically, Wave Relay technology is a highly evolved and flexible MANET solution, able to adjust to terrain irregularities and environmental conditions that tend to degrade wireless network performance. Wave Relay based MANETs provide

connectivity enhancement that preserve communication among the network's mobile nodes. The routing algorithm that Wave Relay uses allows a significant number of meshed-device to be dynamically incorporated into the network. Wave Relay's system provides sufficient connectivity changes among the nodes during the network operation and is able to retrieve, with the use of a routing protocol, alternative pathways for connectivity preservation. A significant advantage of this technology is the network's rapid scalability (consisting of a large number of mobile nodes)—a significant requirement for MIO and regional security networks. The Wave Relay technology is able to perceive node movement through the network – movement that causes network performance and connectivity fluctuations – and to route the data traffic via the current highest capacity path, thereby ensuring the best possible information flow and dissemination through the network [57].

Due to its peer-to-peer routing, the Wave Relay nodes can communicate directly with each other without the need of relays through an Internet gateway. Wave Relay provides the network with fault tolerance, resulting in the continuous functionality of the network, since there is no single node that the network relies on to transfer data. Independent of the potential failure of a node, the network maintains its operation. This continuous functionality is achieved through multichannel devices that ensure routing via alternative channels, multiple routes for increased reliability, and utilization of multiple redundant paths for system connectivity [57].

The MPU4 supports peer-to-peer network topology, multiple video streams through the network, and real-time position location and serial data transmission to participating network nodes. With the high data bandwidth that it uses, it is able to provide up to 37 Mbps of throughput. The MPU4 supports voice (up to sixteen press-to-talk (PTT) channels), video, and data communications. To provide real-time position information, it is connected to the GPS. Location information is then transmitted over the network where monitoring/visualization is displayed via the Google Earth application. The MPU4's effective range with the use of an omnidirectional antenna is approximately two nautical miles. The MPU4 uses high-density lithium-ion rechargeable batteries that allow it to operate up to fourteen hours. Its average power consumption is four Watts,

with peaks of eighteen Watts. There are seven editions of MPU4, classified by their operational frequency, which fluctuates (with specific bandwidths) from 700 MHz to 5.9 GHz. MPU4, due to its convenient dimensions, can be wearable, an attribute necessary for SOF teams that may operate during MIO [58].

The MPU3, as well as the MPU4, is designed for a human to carry and for permanent mounting on assets (e.g., UAVs, vehicles etc.). It provides with the data flow, from and to it, real-time SA, tactical voice (up to sixteen PTT channels), video, and data link. The MPU3 has an integrated GPS receiver to provide real-time position location and, similar to MPU4, it is able to provide up to 37 Mbps of throughput at an effective range of two miles with its omnidirectional antenna. Its peak transmission power is 2 Watts. The MPU3 can be either battery powered or cable powered by 8–48 VDC. Its average power consumption is 4 Watts. The operation frequency depends on the edition and fluctuates between 700 MHz and 5 GHz [59].

The quad radio router ensures deployment flexibility, fault tolerance, and network scalability. It can support up to four wireless radios that all take place in routing and can be mounted. Its power consumption is approximately 16 Watts and it is cable (either to battery or other power source) power supplied. Like the MPU4 and MPU3, it has an integrated GPS receiver and provides up to 37 Mbps of throughput. It is interconnected with the sector antenna array to communicate with the other nodes. The quad radio router with sector antenna array constitutes the sector antenna array router that is mounted on the SFPD patrol boats. The system operates at 5 GHz (there is also an edition that operates at 2.4 GHz) and its theoretical effective range is around ten miles (line of sight). According to the Persistent Systems' specification sheet for the sector antenna array router, it has been tested at 8.5 miles delivering 8.5 Mbps of throughput. The array consists of three independent antennas, each one with 120° coverage, that combine to provide high gain (10 dBi x 3 sectors) 360° horizontal coverage. Because of the significant vertical beam, a wide vertical area is covered too. With the use of the three antennas that individually cover an area of 120°, interference minimizing and network

capacity augmentation are achieved since the RF signals are directed toward the destination. This particular attribute ameliorates system reception as well ensuring the nodes connection [60], [61].

In addition to the Wave Relay systems (Quad Radio Router with Sector Antenna) for the TNT MIO experiments, the SFPD boats (*Marine 2* and *Marine 3*) are equipped with the ARAM sensor presented in Chapter III (Figure 10) for the detection of radiological material, and with a video camera for picture transmission through the network. Aboard each patrol boat is a laptop that interconnects all systems and uses some of the CENETIX SA tools. Through the use of the laptop, the user onboard can be aware of the network status (e.g., which nodes are connected) through the node-ping graph (see Figure 35), transmit and receive video, and use Observer's Notepad to communicate with other nodes by text chat, uploading files (e.g., voice, video, and data) and transmitting the spectral data derived by ARAM sensor detections. The spectral data as appears on a laptop screen is depicted in Figure 36.



Figure 35. Node-Ping Graph

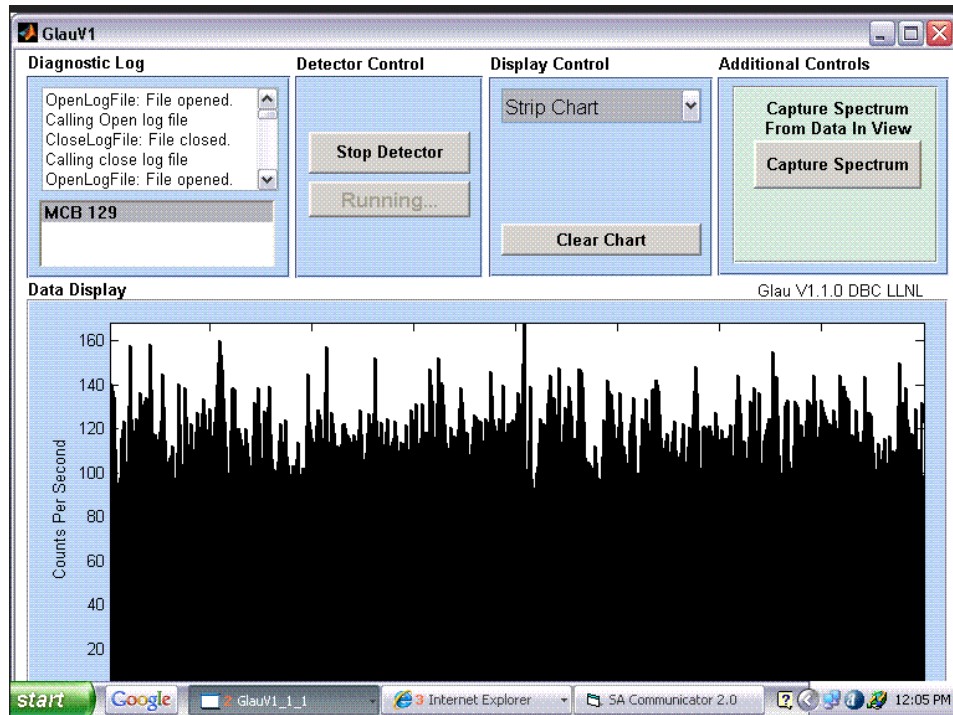


Figure 36. Spectral diagram of ARAM as seen on laptop screen onboard SFPD boat

The Golden Gate Bridge (GGB) node is equipped, apart from the Wave Relay Quad Radio Router with Sector Antenna, with a camera, continuously monitoring the traffic in the vicinity, and is remotely controlled via the CENETIX VPN. The relay node at the Coast Guard Yacht Club (CGYC), which was initially placed on Pier 45 in San Francisco Port (see Figures (3), (28)), provides meteorological data to the network. The overall performance and status of the network is monitored by the CENETIX NOC in NPS.

2. TNT/MIO 11-2 (May 6, 2011, event)

The TNT/MIO 10-2 experiment conducted in 2010 entailed the first use of the SFPD patrol boats (*Marine 2* and 3). The San Francisco Bay portion of both the 10-2 and TNT/MIO 11-2 experiment included the participation of the USCG, SFPD, and Alameda and Contra Costa county sheriffs' patrol boats. The main scopes of those experiments were the following:

- Familiarization of boarding teams with SA sharing.
- Exchange of real-time video and information with the Health Department's radiological experts.
- Small boat with mounted sensor search pattern effectiveness testing (i.e., testing which drive-by patterns were most effective in detecting radiological materials on a queue of pleasure craft).
- Network connectivity limitations due to range (e.g., in the case that the target vessels location causes the boarding team to operate at the limits of the network coverage).
- Tracking of patrol vessels through position-location information (PLI) based on GPS–Google Earth tool network monitoring.
- Generation of alerts and spectra reception by NPS, LLNL, and expert centers [38].
- ARAM sensor performance according to the radiological source location (distance and height) onboard the vessel.
- Examination of motion and sea-state effect on detector performance.

As part of TNT/MIO 11–2, a San Francisco Bay experiment took place on May 06, 2011. During this event, one SFPD boat was employed and a Trellis Ware TW-220 CheetahNet radio was integrated for testing with the Wave Relay system onboard the patrol boat. The test explored voice and data communications from a moving vessel to a shore node (NPS in this case) [20]. The TW-220 CheetahNet, according to Trellis Ware technologies website, is a wideband, networking radio that is able to support voice, video and data communications, and PLI simultaneously. It provides scalability and it is completely self-configuring. The TW-220 can provide data rates up to 2 Mbps and support up to eight hops among the nodes of an ad-hoc network. Its transmission frequency fluctuates between 905–925 MHz and also between 1775–1815 MHz with transmission output power of approximately 2 Watts [62]. A picture of TW-220 CheetahNet radio is depicted in Figure 37.



Figure 37. TW-220 CheetahNet radio (Image from TrellisWare website)

The aim of this experiment was achieved: PLI was visible at the shore station. The itinerary that the SFPD boat followed was depicted on GPS–Google Earth tracking tool. Live-streaming video was transmitted from the boat (Figure 38) to NPS. The crew onboard the patrol boat uploaded ARAM sensor-detection data on the Observer Notepad application making the spectra visible at the remote NPS node (fig. 36). The patrol-boat's itinerary is depicted by the blue line in Figure 39.



Figure 38. Live video streaming between SFPD boat and NPS (Image from CENETIX website)

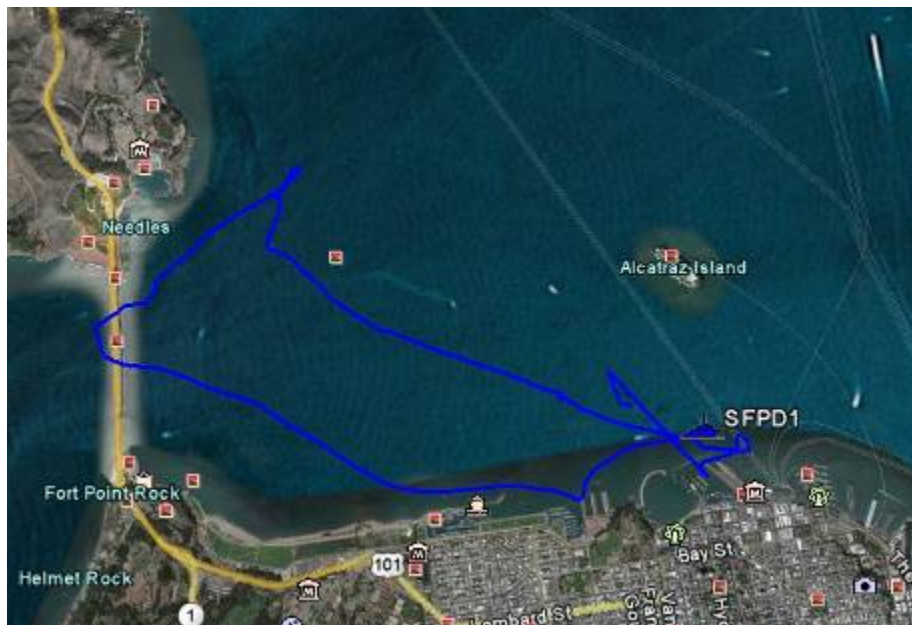


Figure 39. SFPD patrol boat PLI (Image from CENETIX website)

3. TNT/MIO 12–2 (February 28, 2012 event)

The TNT/MIO experiment continues in the San Francisco Bay Area in 2012. This portion of TNT/MIO 12–2 is taking place throughout the year on a weekly basis and with the same aim as TNT/MIO 11–2. For TNT/MIO 12–2 and the NPS Department of Information Sciences’ course on telecommunications and NOCs (IS4926), an NPS student team, including the author, participated both on the scene aboard SFPD patrol boats, and remotely from network operations centers at NPS’s CENETIX lab and Camp Roberts. In February 2012, tests of network-management techniques for the TNT/MIO mesh network were conducted to comprehend network capabilities and performance. During this experiment, two SFPD patrol boats (*Marine 2* and *Marine 3*) were employed. The main scope of this event was testing the hardware and software operations aboard the patrol boats that enabled the NPS CENETIX NOC to receive ARAM-detection measurements and live-streaming video derived by the boats’ cameras. Node behavior and cluster overall performance was captured.

The team aboard the two patrol boats checked the network behavior and status through the node-ping graph on the boats’ laptop screens (Figure (35)). The SFPD boats were connected with the NPS CENETIX NOC through the GGB node (Figure (3)). Information exchange and co-ordination between the boats themselves and the NOCs was achieved with the use of Observer’s Notepad. Observer’s Notepad was used for information exchange regarding network and node status, directions by the NOCs, and ARAM-detection data uploading. One insoluble problem was the malfunction of *Marine 2*’s camera, resulting in video streaming only from *Marine 3* through the VC1 conferencing application during the trial. As long as the patrol boats were connected to the GGB node, there was PLI through the GPS–Google Earth tool. The boat routes are depicted in Figure 40: with the blue line is for *Marine 2* and the green line is *Marine 3*. The crisp, straight lines indicate that no PLI position data was received.

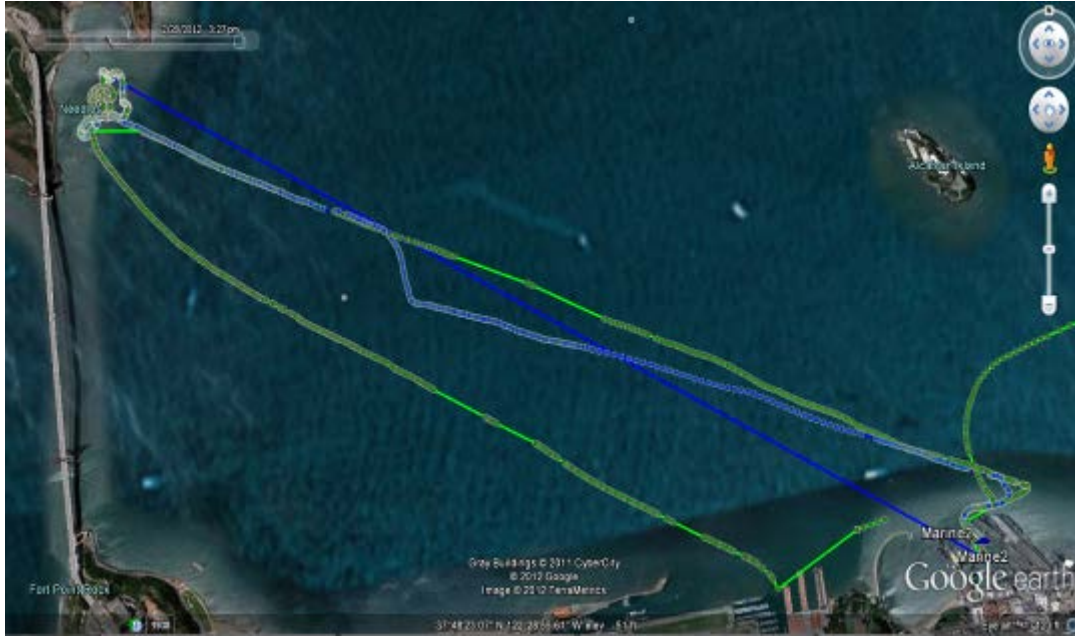


Figure 40. PLI of *Marine 2* (blue) and *Marine 3* (green) during February 28, 2012, trial

Figure 40 shows that for part of the trial, *Marine 2* was disconnected from the network because of technical problems. Once these problems were addressed, there was connectivity throughout the rest of trial. Initially, the two boats transited to a location north of the GGB node that is known, from previous experiments, to receive a strong signal level from the GGB node. During the transit and while on station there, live video streaming from *Marine 3* (Figure 41) and ARAM-detection spectra uploading through Observer's Notepad were successful. Prior to arrival at this position, *Marine 2* was not able to connect to the network. After fixing this problem, the network's overall status as captured by the NPS NOC through "Solar Winds"⁷ network monitoring is depicted in Figure 42. The green circles indicate successfully operating connections, and the red circles indicate no connection to the network. As depicted, the *Marine 2* video has a red circle since it never worked during this trial.

⁷ Network performance and general network management is based on the network performance monitoring software tool provided by Solarwinds Inc.

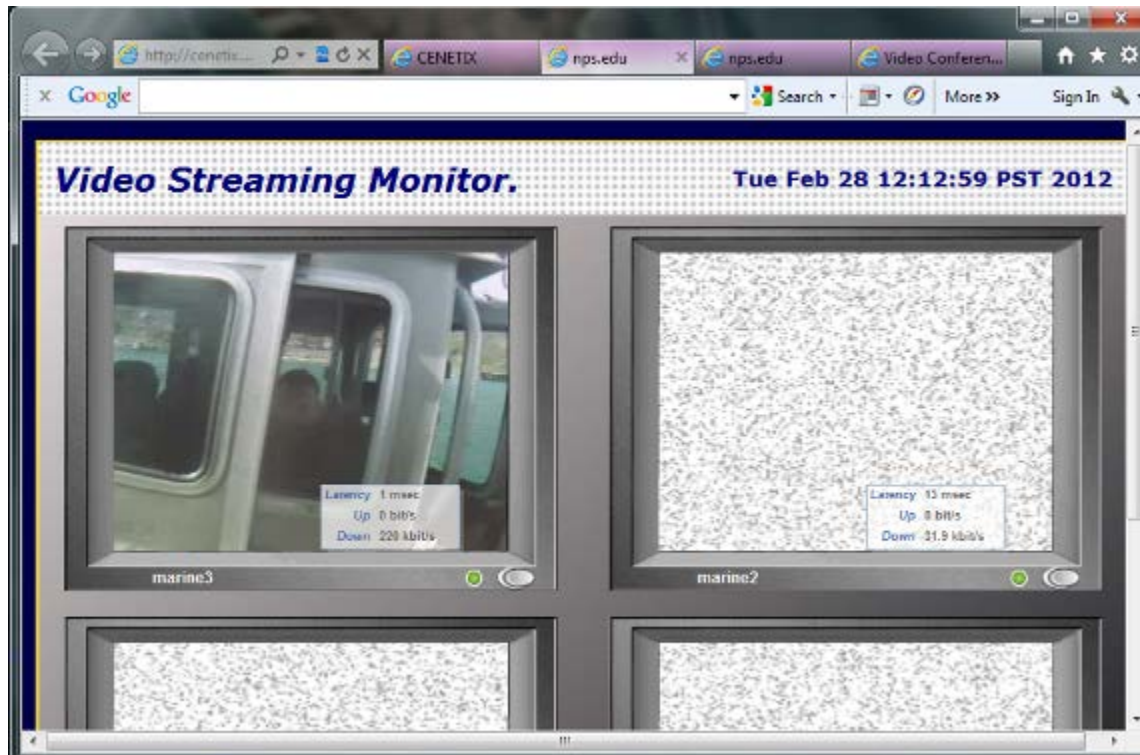


Figure 41. Live video streaming from *Marine 3*

SolarWinds Network Monitor

File Nodes Events Tools View Help

Add Refresh Print Events Page Chart Trace Ping Browse Tools Settings Help

	Node	Response Time	Packet Loss	Status	Since last change
●	192.168.72.21 Marine Laptop (2)	30 ms	48 %	Node Up	1 minute
●	192.168.72.22 Marine Laptop (3)	33 ms	7 %	Node Up	13 minutes
●	192.168.72.245 Marine Video (2)	no response	100 %	Request Timed Out	1 hour, 15 minutes
●	192.168.72.246 Marine Video (3)	24 ms	4 %	Node Up	25 minutes
●	192.168.72.254 Golden Gate Bridge Video Camera	22 ms	0 %	Node Up	6 days, 2 hours, 5 minutes
●	192.168.99.1 NOC NPS GATEWAY	0 ms	0 %	Node Up	1433 days, 2 hours, 52 minutes
●	192.168.99.1 NPS Switch at CENETIX	0 ms	0 %	Node Up	1 hour, 24 minutes
●	192.168.99.112	4 ms	4 %	Node Up	5 days, 19 hours, 53 minutes
●	192.168.99.116	4 ms	4 %	Node Up	52 minutes
●	192.168.99.118	4 ms	0 %	Node Up	21 days, 21 hours, 57 minutes
●	192.168.99.153 Cenetix MGT station	0 ms	0 %	Node Up	26 days, 19 hours, 50 minutes
●	192.168.99.155 CENETIX Server	0 ms	0 %	Node Up	1 hour, 21 minutes
●	192.168.99.180	4 ms	0 %	Node Up	5 days, 19 hours, 53 minutes
●	192.168.99.2 CR_GATEWAY	5 ms	0 %	Node Up	26 days, 19 hours, 52 minutes
●	192.168.99.213 SONY 2	1 ms	0 %	Node Up	581 days, 23 hours
●	192.168.99.216 NOC VIDEO	3 ms	0 %	Node Up	26 days, 19 hours, 52 minutes
●	192.168.99.216 CR Tower/Camera	5 ms	0 %	Node Up	26 days, 19 hours, 52 minutes
●	192.168.99.8 VPH Cisco 3015	0 ms	0 %	Node Up	1433 days, 2 hours, 52 minutes

SolarWinds Network Monitor

Network Performance Monitor

NetPerfMon Database Maintenance

SNMP Graph

Bandwidth Gauge

MS Browser

Security

Miscellaneous

Help & Web

Figure 42. Network status on “Solar Winds” platform

After staying at the north side of the GGB, the two boats were directed to move to the vicinity of Alcatraz Island. This area is experimentally proven to have low signal coverage from the communications nodes. The goal of this movement was a network-status check with one mobile node inside and the other outside the GGB node coverage area. *Marine 2* moved to the weak or no coverage area and *Marine 3* remained around 0.5 nautical miles behind to maintain connectivity with the GGB node. Observations showed that *Marine 3* preserved its connectivity while sailing close to the Alcatraz area because *Marine 2* was the intermediate node between *Marine 3* and the GGB, relaying interactively the data (multi-hop). The team aboard the patrol vessels checked node status during this phase with the node-ping graph on their laptop screens; however, without having any indication for data relay or not. The data rate gauged from *Marine 2* during the aforementioned phase was approximately 3.4 Kbps for uploading and 125 Kbps for the download—a significantly low performance level for networking connectivity (Figure 43).

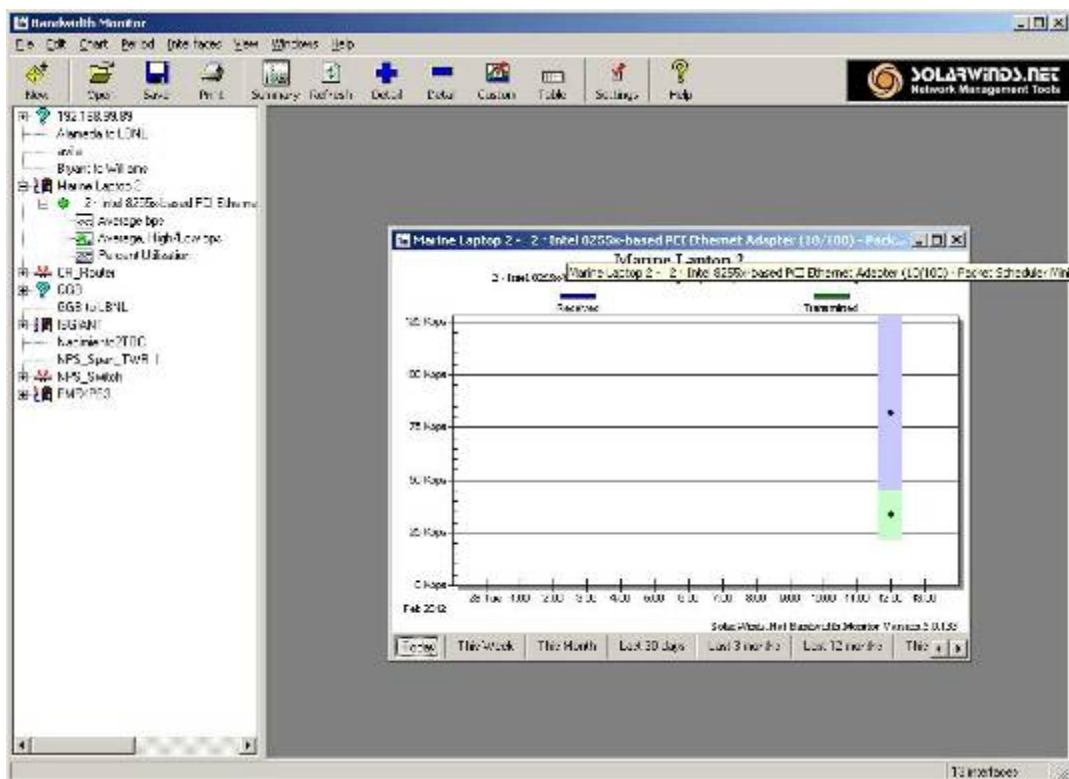


Figure 43. Bandwidth Monitor on Solar Winds platform

4. Lessons learned

During the San Francisco Bay portion of the TNT/MIO experiments, the potential contribution of ad-hoc sensor networks to MIO and regional security operations is obvious. Most importantly, data that leads to achieving SA of complex events is disseminated throughout the network with the use of man and small vessel/craft transportable equipment (i.e.; relatively small and light weight), such as Wave Relay and Trellis Ware radios. These systems allow for the delivery of information around the participating nodes and to expert centers via VPN connections through the commercial Internet. The use of the commercial Internet is only a surrogate for likely military or other official government or alliance networks. Additionally, PLI from the patrol boats, or any asset capable of transporting a node, can be provided to the end node. Hence, these systems allow the flow of human communications, both voice and text, real-time video, still pictures, detailed sensor data from sensors about the presence of illicit material, and the material's exact location onboard a suspicious vessel.

It is clear that mobile nodes—in this particular case, the patrol boats— have to maneuver promptly to retain direct or indirect connectivity to enable the flow of information. This situation can be applied as well to boarding teams and other mobile assets, as described in Chapter III. When a node is operating in a low- or no-coverage area, the employment of a relay node ensures the smooth flow of data, as shown in the February 2012 events.

During the experiment's execution, detector performance was affected, though not dramatically, by the sensor's proximity to the radiological sources, the motion of the two boats, and source's strength. Moreover, LOS is a critical factor for connectivity preservation. For example, the boats, when berthed in the San Francisco Port cannot be connected to the network, since the GGB node is out of their LOS. Furthermore, since the mesh-network environment is a non-constant variable (e.g., due to potential position alterations) that affects overall performance in the establishment of local NOCs in nodes, like the respective on SFPD boats that are giving information about the cluster nodes status, provides the network with added flexibility and adaptation. However, the

adaptation of local NOCs does not require a central NOC replacement, since the central NOC is responsible for all network monitoring and actions in case of a situation that affects the network operation.

C. FORT EUSTIS – RIVERINE AREA, VIRGINIA

To better understand and exploit ad-hoc sensor networking in MIOs, experiments have been conducted with the Port Authority of New York and New Jersey and in the riverine area of the James River adjacent to Fort Eustis, Virginia [56]. The following experiments were conducted as portions of TNT/MIO 08-04, TNT/MIO 9-2, and TNT/MIO 9-4.

1. TNT/MIO 08–04 Experiment (September 08–12, 2008)

The TNT/MIO 08–04 took place between September 8th and 12th, 2008 and was divided in two portions. The first was conducted in ports under the cognizance of the Port Authority of New York and New Jersey on September 8 and 9, and the second was executed in the riverine area of Hamptons Roads. The scope of this experiment was the exploration of new sensors, networking, and SA solutions that could contribute to detection, interdiction, and tracking of ships and boats that may pose a radiological threat in coastal, populated areas. The experiment included cooperation and data sharing with a node in Sweden. The equipment used to create the ship-to-shore wireless networks was Wave Relay. A total of eighteen Wave Relay devices (three were man-portable) were used on both mobile and stationary nodes during the New York portion of the experiment. The networks were integrated into a satellite communications (SATCOM) system at the port authority’s emergency-operations center, to provide Internet connectivity to reach-back centers in California, across the USA. This replicated conditions likely found in austere areas where public Internet access is unavailable. This satellite-to-ad-hoc network enabled mobile tactical nodes (e.g., Wave Relay systems mounted on boats and a UAV) to provide live-streaming video and other information transmissions to strategic nodes. [56]

The New York–New Jersey portion included two phases. During the first phase, boarding operations and searching for radiological material on a “suspicious” vessel were

conducted. During the second phase, detection of illicit material aboard two small vessels in a harbor was conducted by patrols with radiological detection systems onboard. In both phases, the participants, acting as investigators, needed to transmit in real time SA and spectral information to all centers (e.g., emergency operations centers and centers of excellence for radiological incidents). During the first phase, the boarding team managed to detect the radiation source and transmit the spectra to the expert centers through the network. They also transmitted live streaming video to assist in evaluation the spectra. Moreover, information sharing through the Observer's Notepad was continuous. Simultaneously, a UAV successfully transmitted aerial video of the suspicious vessel [56]. A snapshot of the video streams from the boarding team onboard the suspect vessel and the UAV is depicted in Figure 44.

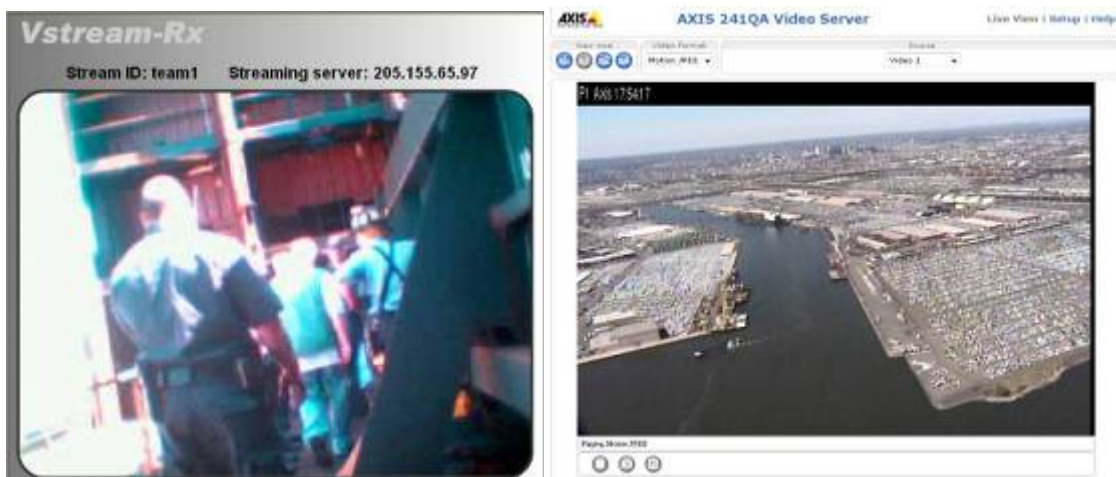


Figure 44. Live video streaming from boarding team (left) and UAV (right) (Image from CENETIX website)

During the second phase, the moving small security vessels used Wave Relay equipment to form a mesh network to transmit SA, video, and sensor detection data. The boats during this phase were moving in a coordinated manner in order to maintain connectivity and data transmission to the SATCOM node. This was accomplished by using the multi-hop capability by assigning a boat to act as a communication relay node. The patrol boats succeeded in intercepting the suspicious vessel that was carrying a

radiologic source, and had that source properly and expeditiously identifies by a remote expert based on the real time transmission of spectra files and video [56].

The second portion of the experiment took place in a riverine area of Virginia. The scope of the riverine scenario was the testing of wireless-networking support of high speed small-boat interdiction, waterborne-radiation detection, and data dissemination (e.g., video, SA, radiological) for security-operations. During the riverine phase, connectivity between two nodes was achieved at a distance of more than seven nautical miles. There were tests at this distance between the tactical-operation center (TOC) node and a remote semi-fixed node (i.e., the node was temporarily set up on a tripod to act as a deployable relay node to extend the network around a nearby bend in the river) set up on an adjacent riverbank. This set up was designed to measure the performance of this LOS link using different kinds of antennas. For sector-antenna array to sector-antenna array trail, the throughput was 8 to 10 Mbps. The 23 dB-directional-panel antenna to sector-antenna array yielded a throughput of 17 to 20 Mbps, and with the connection through two directional-panel antennas, the throughput reached 33 Mbps. Using the multi-hop effect, data was disseminated at a distance of fourteen nautical miles. The Google Earth visualization showed the TOC the boat positions and the link status between them. Furthermore, the network performance was tested while the boats were operating at high speeds. The Wave Relay nodes on the maneuvering boats were able to maintain live streaming video connectivity with no degradation, even when the small boats were operating at forty knots and experiencing significant turbulence on the water [56].

During the first day of the riverine experiment, two boats acted as boarding vessels and two others played the targets. The boarding vessels transmitted video and radiation spectra from the targets. Also during the boarding phase, biometric data was obtained from the crew of the target vessel and successfully transmitted to expert centers. On the second day, connectivity under high mobility conditions was tested along with radiation sensor performance, and spectra and biometric data dissemination through the network. The boat to shore connection reach out to seven nautical miles direct-distance, and fourteen nautical miles distance with one boat acting as a relay node—see Figure 45 for a depiction of the Google Earth PLI tool [56].

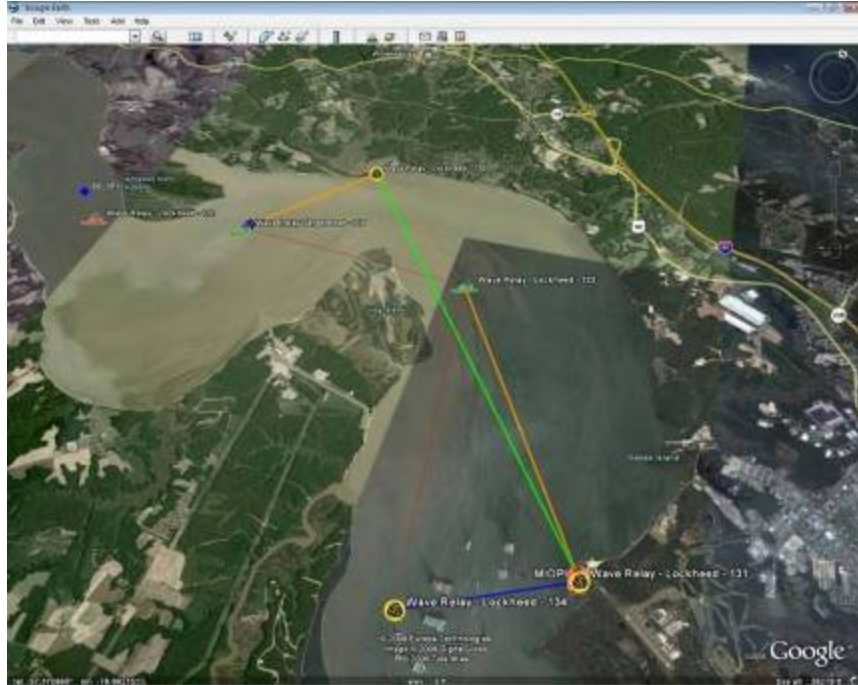


Figure 45. Riverine-area mesh network (From [56])

The aims of the TNT/MIO experiments in New York/New Jersey and Virginia were accomplished. There was robust communication, exploitation of Wave Relay systems among vessels and a UAV in multiple security situations. The nodes managed to transmit through the network live video, SA information, voice and text data, and radioactive source spectra files in real time to remote expert centers even at while conducting high speed operation—like those often occurring in security missions. Also the use of relay nodes proved that network coverage can be significantly increased, as in the case of fourteen-nautical-mile connectivity with multi-hop exploitation. Moreover, results showed that the use of a high-gain antenna, like that of Wave Relay systems, can dramatically affect network performance at a given distance.

2. TNT/MIO 09–02 Experiment (April 23–24, 2009)

The experiments in the riverine area continued in 2009. The riverine portion of TNT/MIO 09–02 took place between April 23rd and 24th, 2009. During this experiment,

a mobile operation base (MOB) was formed by a patrol boat that brought networked swimmers into the area. The mission of the swimmers was to tag a target vessel for vessel monitoring. Additionally, personnel-detection sensors and video cameras connected to Wave Relay devices were placed on the riverbank along the target vessel's expected route to detect illicit activities (e.g., smuggling items or people to or from the target boat). These sensors can detect individuals at ten to twenty feet. When the sensors are approached by swimmers, they are triggered and transmit alerts through the SA application to local MOBs, TOCs, and other observation sites connected to the network. During this experiment, live streaming from patrol boats, Google Earth PLI, and Observer's Notepad were used. A remarkable fact during this experiment was the employment of the USV *Sea Fox*, which was remotely controlled from a ground station and used to chase the target vessel while transmitting live video streaming (Figure 46) through the network. *Sea Fox* was also assigned to conduct video detection of waterborne IEDs. [54]

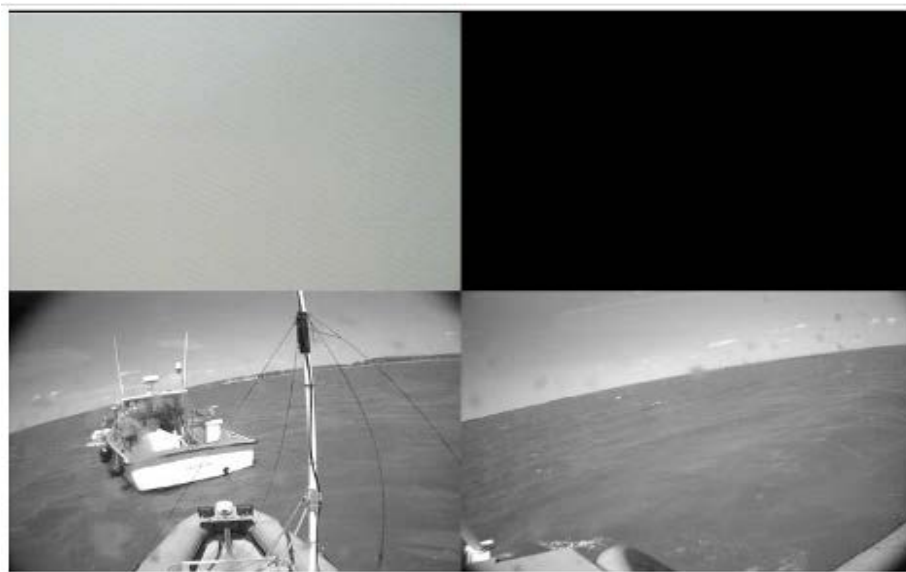


Figure 46. USV *Sea Fox* video streaming (Image from CENETIX website)

A remarkable outcome during this experiment was the achievement of ship-to-shore connectivity at a distance of 13.16 nautical miles with the use of two boats and

their peer-to-peer-mesh nodes (Figure 47), as well with the maintaining of connectivity while operating at high speeds of around 30 knots.

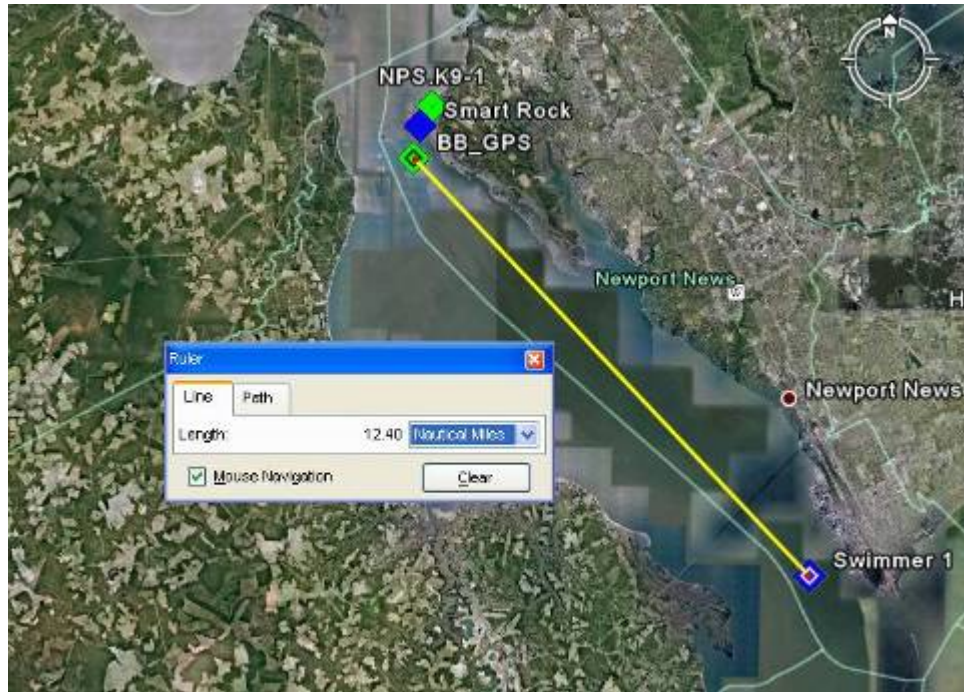


Figure 47. Riverine network connectivity at 12.4 nm (Image from CENETIX website)

3. TNT/MIO 09-04 (September 09-10, 2009)

The Fort Eustis portion of TNT/MIO 09-04 experiment took place on September 09-10, 2009. During this experiment, cooperation between MOBs and USVs for surveillance and detection was examined, as well with stand-off detection of illicit material at high speed and dissemination of SA through the network on a worldwide scale. During the Fort Eustis portion, there was collaboration with the Swedish naval warfare center in Karlskrona, Sweden. This cooperation included the control of the USV feed between the two locations. The control signals were passed over the network. During this experiment two Sea Fox USVs were employed and motion detection and video sensors were placed ashore for the detection of swimmers in a particular area. With the activation of sensors, alerts were transmitted through the network to the MOB and TOC [63].

A key research point during this experiment was the sensing ability of a sensor in proportion to speed and distance from the resource. Initially, with the employment of one vessel as sensor carrier and another as source carrier, a sensing distance of 104 ft. at a speed of 4.9 knots was achieved. During the experiment's evolution, a sensing distance of 75 ft at a speed of 58 knots was reached. At this distance and speed, there was a 100% success rate of illicit material detection by the sensor. The initial measurement array through PLI tool and the ARAM spectra diagram are depicted in Figure 48, with ME1 being the patrol boat and ME2 the target vessel [63].

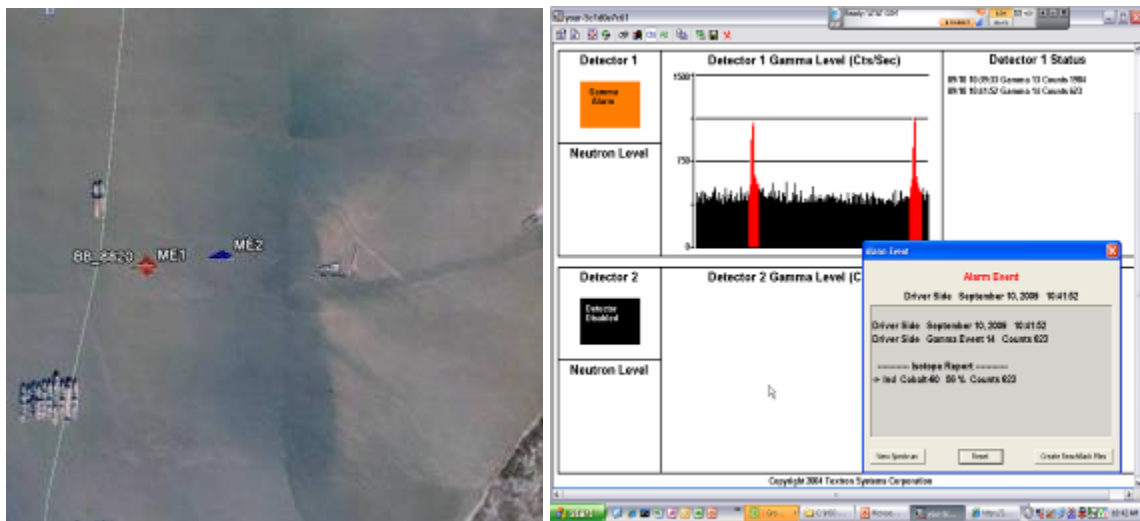


Figure 48. Sensing distance measurement between ME1 and ME2 and ARAM spectra diagram (Image from CENETIX website)

The video transmission from nodes placed ashore whose sensors were triggered by swimmers is depicted in Figure 49. With the employment of these sensor nodes, live video streaming of swimmers while meeting with the target vessel of interest was achieved.



Figure 49. Swimmer detection by ashore node (Image from CENETIX website)

4. Lessons learned

During the TNT/MIO experiment portions of the riverine and New York/New Jersey port area, the feasibility of live video transmission from UAVs of boarding teams during embarkation was explored. Especially when the boarding team was aboard the suspicious vessel, connectivity was preserved, even though in some case there was no LOS communication between the boarding team and other network nodes. This fact had to do with the transmitted signal reflection on the “seized” ship containers which were intermediated through the LOS between the boarding team and other nodes. This connectivity contributed to the transmission of live video streaming and sensor detection, proving that communication between network nodes can be achieved even out of LOS, depending on the intervening material surface. Moreover, the contribution of high-gain antennas to connectivity and data-rate increases was more than obvious. As in the San Francisco Bay experiments, in riverine trials the presence of relay nodes expanded network coverage significantly, with the multi-hop capabilities ensuring data dissemination (video, sensor data, etc.) through the network. Furthermore, it was made clear that standoff detection of radioactive material with simultaneous data transmission from the sensor node at high speeds is more than feasible. The employment of sensors

that detected the presence and movement of swimmers from shore while transmitting live video to MOB and other centers shows how this kind of network can contribute to security operations.

D. NMIOTC, SOUDA BAY - GREECE

TNT/MIO experiments in 2009, occurred at the NMIOTC in Souda Bay, Greece. Since then, NMIOTC is an integral part of the annual TNT/MIO experiments. These experiments include participation of NPS and several other NATO and international organizations responsible for national or allied security. During NMIOTC experiments, there was exploitation of networked tactical swimmers, standoff detection of radioactive material by a UAV, large-vessel searches, and SA reach-back to expert centers on the network.

1. TNT/MIO 09-04 (September 28–30, 2009)

The first time NMIOTC participated in TNM/MIO experiments was during TNT/MIO 09-04, September 28–30, 2009. During this experiment, there was utilization of ship-to-ship and ship-to-shore broadband mesh networking. Over that mesh network the following actions were taken: (1) SA information was transmitted to the NMIOTC main building and to a moored training ship (see Figure 50), (2) GSM/GPRS was networked with swimmers, (3) security patrol and target vessels acted as network nodes, and (4) radiation sensors data was transmitted from two patrol vessels acting as a checkpoint (i.e., a chokepoint or portal that suspect vessels had to pass between). The Wave Relay systems were used for ship-to-shore connectivity (operating at 5.8 GHz and 2.4 GHz), as well as for networking along the deck of the training ship and providing ship-to-ship wireless-mesh networking. Cameras, vessel GPS-based tags, and ARAM sensor were also employed [63].

One of the research objectives was to conduct a large-vessel search by a boarding team, and to use networked swimmers to search for and detect IEDs on the hull. The boarding team sought illicit material aboard ship and identified each cache with portable ARAM sensors. The boarding team was equipped with Firestorm GPS-denial navigation systems while operating inside the training vessel (i.e., in internal compartments under

the superstructure) where there was no GPS coverage. With the use of Firestorm, the location of the boarding team and the data retrieved by the sensors were viewable through the SA tools by the expert centers at NMIOTC, NPS, and LLNL. The large vessel for experiment was the former HS *ARIS* (A-74, see Figure 50) berthed in Souda Bay for NMIOTC training purposes. It is 130 meters long [63].



Figure 50. Large vessel: HS *ARIS* at NMIOTC

To check for the possibility of ship-mounted IEDs, searches were performed by swimmers connected to the network. A simulated IED was placed on the hull of the *ARIS*. Apart from IED detection, the swimmers were tasked to inform the TOC and MOB if they detected the presence of a “suspicious” small vessel in the area, and then covertly place a tracking tag on it that could be tracked over the network. Additionally, the swimmers placed sensors ashore according to the expected itinerary of suspicious vessels; this was similar the riverine experiment. The swimmers carried tracking devices (GPS with GSM/GPRS connection) to allow the centers to be aware of each swimmer’s position, IED-detection devices simulated by a Bluetooth-based proximity detector, and waterproof voice-communications equipment. During the IED detection phase, the swimmers, after finding the IED with the Bluetooth proximity detector, relayed photographs from their support boats to the TOC for further evaluation [63]. A snapshot of swimmer positions on PLI and a picture taken below the surface are depicted in Figure 51.



Figure 51. Swimmer positions on PLI and a picture taken on the vessel hull (From [63])

As in the riverine experiment, a small-craft standoff detection and interdiction was achieved during the TNT/MIO 09–4 NMIOTC experiment. Two patrol boats equipped with a RN sensor were able to transmit detection and SA data in real time through the network using the Observer’s Notepad tool. During the standoff detection tests, it was revealed that a narrow portal—approximately 20 feet wide—was required to detect sources when suspect boats passed through the portal at high speed (i.e., 25 knots and more). Also, to facilitate data sharing with the TOC during this phase, one patrol boat acted as a relay communication node between the other portal boat and the TOC.

2. TNT/MIO 10-02 (June 12–14, 2010)

In 2010, NMIOTC participated in the TNT/MIO 10–2 experiment between June 12th and 14th. The first part of TNT/MIO 10-02 was conducted in Germany from June 7th to the 10th. The scope of TNT/MIO 10-02 was to more precisely examine: (1) ad-hoc mobile-networking architectures that employ handheld and unmanned, systems-based detectors, (2) the information-management architecture for SA sharing (e.g., sharing alerts on threats posed by a small vessel), (3) monitoring of vessels that carry illicit material in open waters by tracking movement through SA tools, and (4) standoff detection of illicit material at high speeds with sensor carrying USVs and UAVs. As in

the case of the TNT/MIO 09-04 experiment, networking with swimmers, sensor operators, and patrol boats providing reach-back to expert centers for identification of illicit material was achieved. The equipment used was the Wave Relay system solution operating at 5.8 and 2.4 Ghz for ship-to-shore and Wave Relay system solution of the ship-to-ship, on the move, broadband wireless-mesh network. For the monitoring of targets, GSM and satellite-based location posters (i.e., active tags) were utilized [55].

As mentioned above, the experiment employed network-enabled swimmers to detect a small craft carrying illicit material. The swimmers were integrated into the ad-hoc, mobile, ship-to-ship and ship-to-shore mesh network. That connection allowed them to receive video feeds on the suspicious object. An NMIOTC patrol vessel acted as a MOB that was tasked to find the suspicious boat and identify potential threats to the base. The networked swimmers transmitted information about the illicit object orally and by video, which was relayed afterwards to detection experts at the reach-back location. The swimmer positions during this particular procedure were depicted on the PLI tool. The video feed from the swimmers to the NMIOTC Headquarters simulated the experiment reach-back center. Figure 52 shows the positions of the patrol boats and the swimmers as depicted on the PLI tool. After the object was evaluated by the expert center, the swimmers tagged the target vessels with a network node that ensured target position monitoring [55].

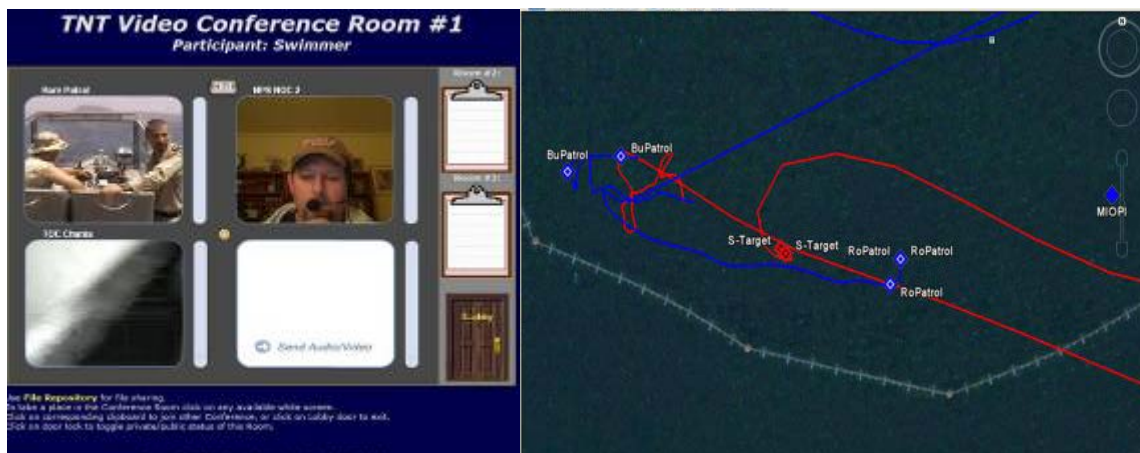


Figure 52. Swimmer video feed and positions on PLI (Image from CENETIX website)

After the swimmers' task was completed, a small craft with an RN source onboard was used to explore the efficacy of standoff detection on the move. The sensor on a patrol boat first alerted on the source at a distance of 100 ft; however, the expert centers were unable to identify the threat. The centers recommended closing to 50 ft, and then 20 ft, but neither distance produced satisfactory RN sensor data to identify the threat. Next, a standoff detection test was conducted by a RN equipped UAV *Vellerofontis* mini-helicopter (see Figure 24). The *Vellerofontis* was also equipped with a camera that allowed video streaming through the network. The UAV, controlled by its separate radio control link, achieved aerial detections of the source from above the target vessel. This sensor data was sufficient to allow source identification by the experts receiving feed from the helicopter [55]. The detection-spectra diagram and video streaming during *Vellerofontis*'s flight is depicted in Figure 53.

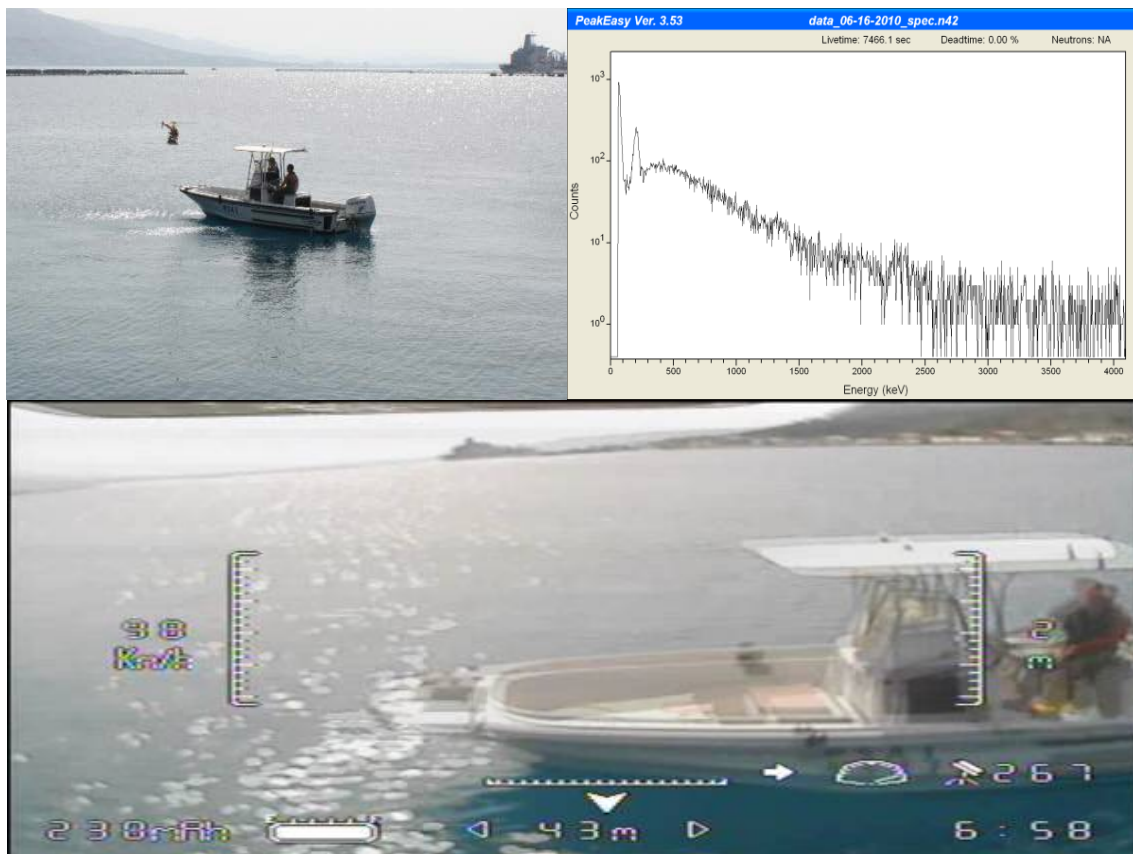


Figure 53. UAV standoff detection results (Images provided by NMIOTC)

The most significant outcome of the NMIOTC portion of the TNT/MIO 10–02 experiment was the success of standoff aerial detection and identification of illicit material by the UAV, with simultaneous SA data dissemination through the network. This success provides unambiguous facts that UAVs are capable of providing valuable support to MIO sensor networks, an alternative, valuable tool for the success of MIO missions to interdict RN materials. It must be kept in mind that this particular UAV's speed when fully loaded with sensors and communication systems was nearly 100 km/h and its range was around three nautical miles. That range limitation was due to the non-networked, LOS radio control signal from the UAV's ground station to the UAV.

3. TNT/MIO 11–02 (June 9–10, 2011)

The NMIOTC portion of TNT/MIO 11–02 experiment took place in Souda Bay, Greece between June 9th and 10th of 2011. Generally, the research areas of this experiment in its totality, including the San Francisco Bay Area network, were:

- Integration of boarding teams to ad-hoc mobile networking architectures.
- Information management architectures to share alerts on CBRNE threats found onboard crafts.
- Surveillance methods for locating, tagging, and tracking of vessels suspected of carrying CBRNE materials.
- Exploitation of USVs and UAVs for standoff detection at high speeds
- Uncovering potential vulnerabilities of these ad-hoc sensor networks [38]

The main scope of this experiment at NMIOTC was threats tracking integration, CBRNE threats detection, and interdiction of maritime threats in the vicinity of a naval base. The following capabilities were investigated: (1) networked-enabled tactical swimmers for tagging suspect vessels and threat detection aboard a small craft, (2) cooperation between swimmers and boarding teams, (3) communication with expert centers for a network-controlled chokepoint establishment and (4) standoff detection during a high-speed chase. The swimmers provided the boarding teams with descriptions of parasite boxes (i.e., suspected IEDs), target data, etc., and also provided the boarding

team with spectra files obtained by their portal sensor (see Figure 13) via USB drives, since direct dissemination through the network, as initially planned, was not feasible. These spectra were disseminated through the network to expert centers by manually posting on Observer's Notepad. Furthermore, during this experiment a USV with a source onboard was used to simulate a target vessel posing a threat to a naval base. The mini-helicopter *Vellerofontis* was used to conduct standoff detection at high speed and disseminate radiation detections and live video streams of the threat through the network [38].

The NMIOTC portion of TNT/MIO 11-02 was divided into four phases. In the first phase, there was simulation of early detection and interdiction of suspect vessel in the Baltic Sea close to Karlskrona harbor. This information was used at NMIOTC in follow-up classification when the source was detected in Souda Bay. During the second phase of the experiment, a large-vessel (HS *ARIS*) was searched by networked swimmers carrying portable sensors and relaying SA data through the network. In the third phase, small craft tracking, detection, and search were executed. A USV was used to simulate a small manned boat. The fourth phase was the same as the third, but instead of the USV, a small manned vessel was employed [38].

After the first-phase (i.e., the simulated of early detection of a suspicious vessel and source), transition to live experimentation was conducted. During the second phase, the networked swimmers were deployed around the large vessel to execute their assignment, transmitting video feed to the video-conference tool via cameras mounted on their helmets. A snapshot of the video-conferencing and swimmer deployment is depicted in Figures (12) and (14). The swimmers provided video and oral evaluation of their search and exchanged information with experts. On the other hand, the boarding team on the vessel received spectra detections from the swimmers through the mesh network and uploaded them to Observer's Notepad to be seen and evaluated by the experts [38]. Detections by swimmers were conducted with the use of the portable detector depicted in Figure 13. The position of the swimmers was mapped with the PLI tool, is depicted in Figure 54.



Figure 54. Swimmers Location on PLI during large-vessel search (Image from CENETIX website)

Apart from swimmer deployments, a boarding team embarked on the vessel to investigate for the presence of radioactive material inside the ship. For the transmission of voice, video, and sensor data from internal compartments below deck to the TOC at NMIO TC headquarters, TrellisWare radios were used. The network-performance statistics for throughput and latency, according to the location of the boarding team during this phase, are depicted in Figure 55. [20]

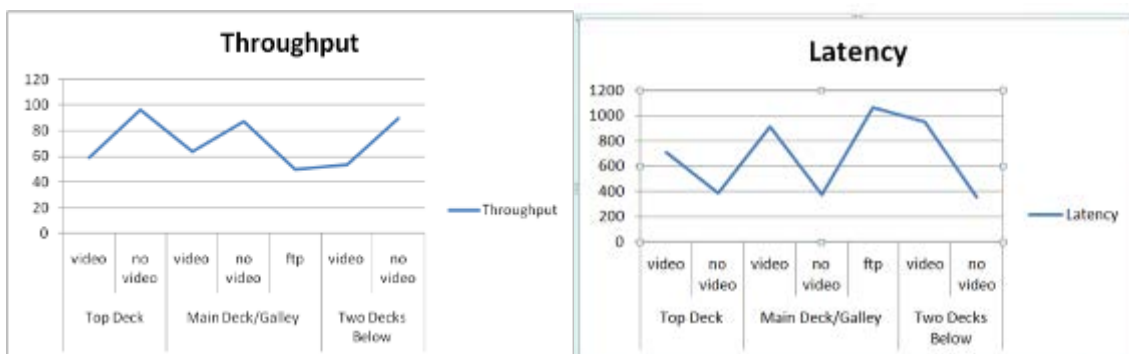


Figure 55. Network performance statistics during large-vessel search (From [20])

After the large-vessel search phase, small-craft detection and interdiction was executed. The distance between the target and patrol boat for standoff detection was reduced successively during this phase from 100 ft to 20 ft. Even though there were

detection alerts, the sensor's data output was insufficient for the experts to identify the source material. The location of vessels was visible on the PLI tool. Each boat was connected to the mesh network with Wave Relay equipment; however, TrellisWare CheetahNet radios were also employed as an alternative network for voice communications among all boats and the MOC, and for video-streaming transmission from the boat in the observer's role to the TOC.

After unsuccessful attempts to identify the radiological source, the experiment proceeded to the next phase, which included USV and UAV employment. The USV, with the radioactive source onboard, was ejected by the target craft. The UAV conducted standoff detection of the source, chasing the USV at high speed, providing live video-streaming, tracking, and sensor data to the experts through the mesh network [38]. A snapshot of the USV pursuit by the UAV and of the sensor data is depicted in Figure 56.

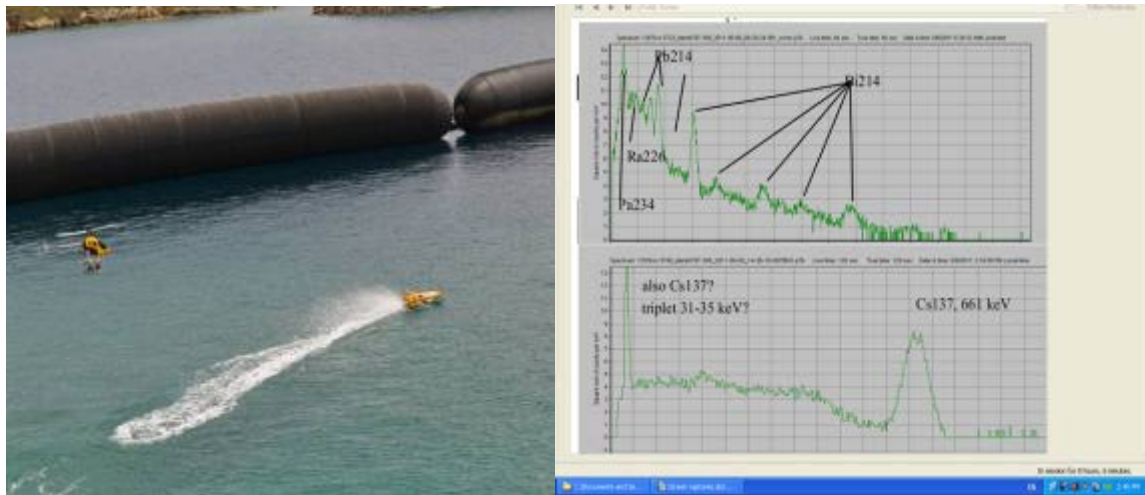


Figure 56. UAV-USV pursuit and sensor data (Images provided by NMIOTC)

During this experiment portion the following tasks were achieved [38]:

- Satellite reach-back to expert centers (e.g., NATO JCBRN COE)
- Exploitation of ad-hoc broadband wireless-mesh network with patrol vessels and sensors as nodes

- Use of an additional mesh radio network for the boarding team (Trellis Ware)
- Use of ad-hoc mobile, broadband, wireless-mesh network for the swimmers (Wave Relay)
- Tracking with GSM and Globalstar Satellite network use.

This experiment proved the significant contribution of ad-hoc sensor networks consisting of several types of nodes (vessels, UAV, swimmers, etc.) to MIO and how these networks can facilitate the detection, and rapid identification and evaluation of a threat by experts anywhere in the world through SATCOM communications network link reach-back. Diagrams of the experiment networks are depicted in Figures (57), (58), (59), retrieved from TNT/MIO 11-2 report.

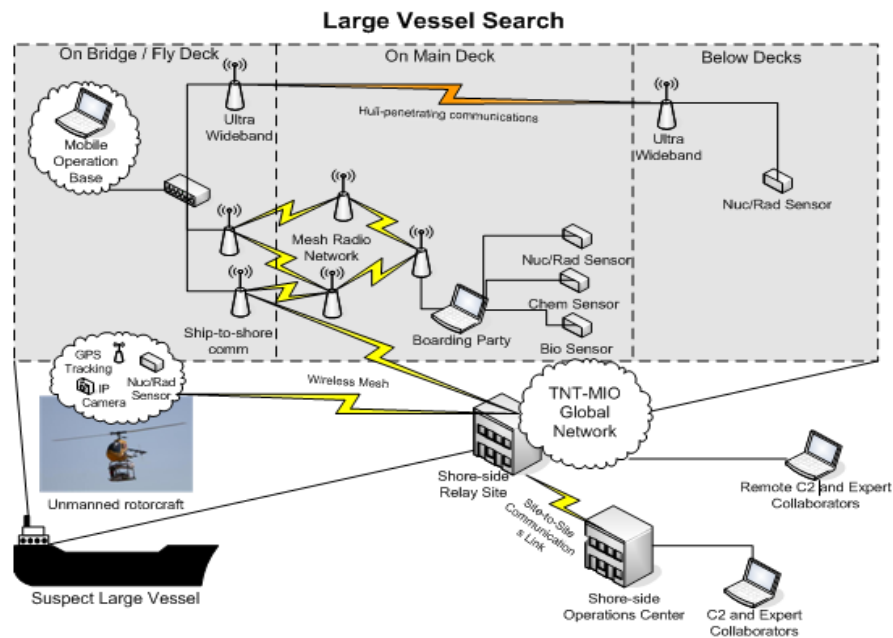


Figure 57. Large-vessel search ad-hoc sensor network (From [38])

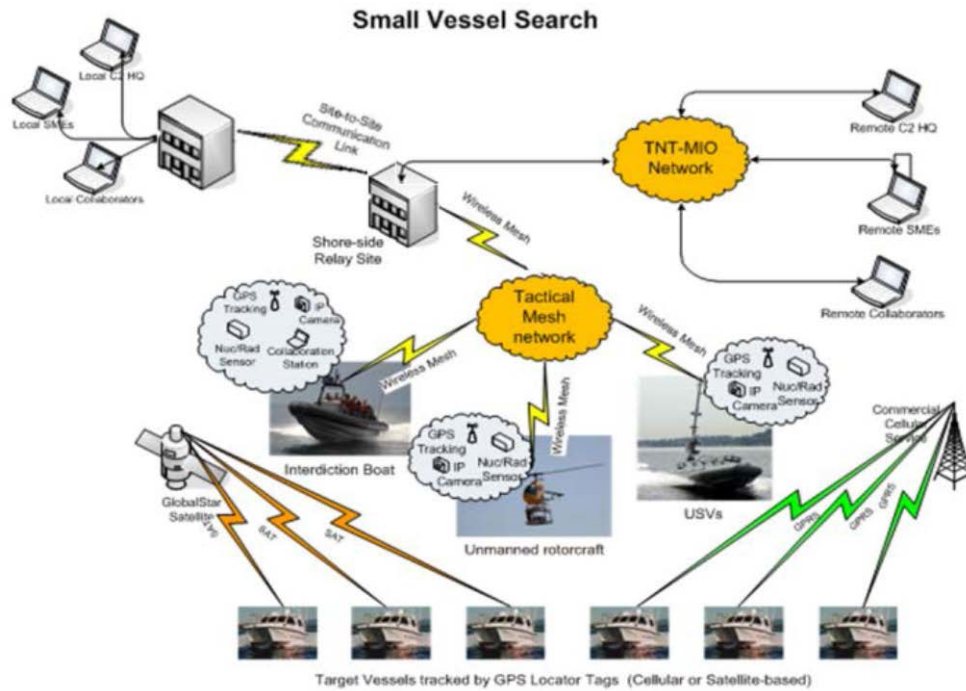


Figure 58. Small-vessel search ad-hoc sensor network (From [38])

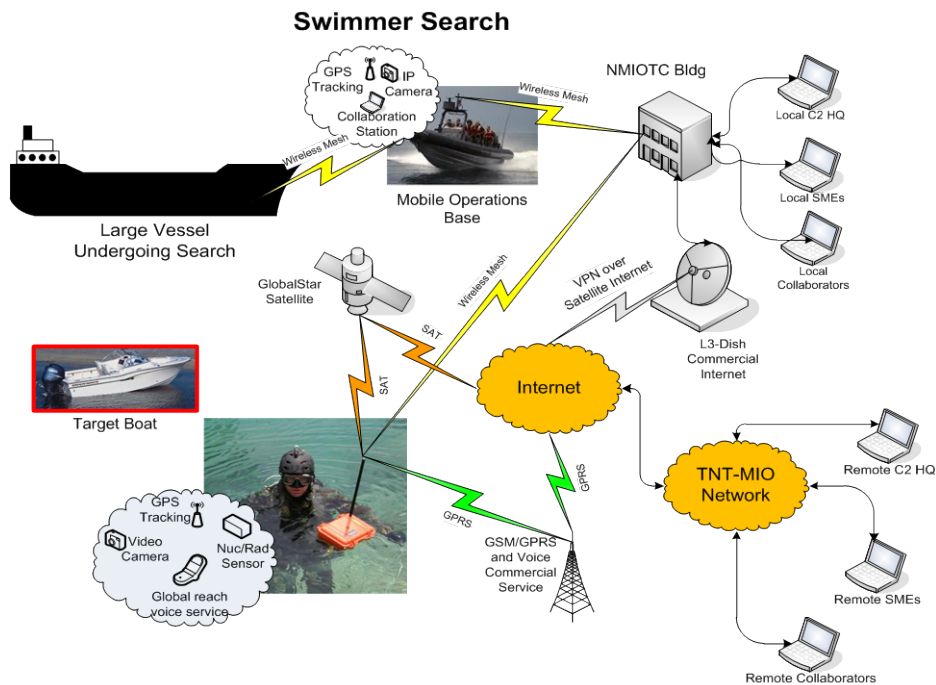


Figure 59. Swimmer ad-hoc mobile, broadband, wireless-mesh network (From [38])

4. TNT/MIO 12–02 (June 12–14, 2012)

The most recent experiment in NMIOTC was one of the two outside the USA portions (the first took place in Sweden and Poland) of TNT/MIO 12–02, which was conducted between June 12th and 14th, 2012. During the NMIOTC experiment, there was a large-vessel search by networked swimmers and boarding teams using portable sensors and mesh peer-to-peer networking. Apart from the large-vessel scenario, there were small-craft search phases, where a target vessel was simulated by a USV and their objectives were small-vessel detection and evaluation by swimmers, setup of primary and secondary chokepoints, and high-speed standoff detection and pursuit with UAV employment as executed in TNT/MIO 11–02. Finally, an experiment was conducted where the USV and UAV roles were reversed. The UAV mini-helicopter was used as the source carrier and detection was conducted by the surface vessel.

The main scope of TNT/MIO 12–02 at NMIOTC was similar to TNT/MIO 11–02 (see page 89). During this experiment, spectra data uploads were achieved through Observer’s Notepad, SA data dissemination of patrol and target vessel locations, and information exchange among participants (including the NPS NOC) via chatting and voice files upload through Observer’s Notepad and also via voice, video and video-conference as in previous NMIOTC experiments. The evaluation of threats was conducted by the experts at NMIOTC and other locations, e.g., NATO JCBRN COE in the Czech Republic. Standoff detection of illicit material and data dissemination was achieved by a patrol vessel and a UAV. The mini-helicopter carrying the radioactive material conducted flights above the patrol boat, which was equipped with the sensor. Detections were achieved by the patrol boats when the mini-helicopter flew at a distance and height from the boats of ten meters and three meters, respectively. The quality of the detection allowed the experts who received the data to identify the material. Simultaneously, there was a live streaming-video transmission through the network by the camera on the UAV. The networking systems used were TrellisWare and Wave Relay systems, as in previous experiments.

5. Lessons learned

Using actual NATO boarding crews from NMIOTC is one of the most significant parts of TNT/MIO experiments being held by USA and international organizations. The experiments conducted at NMIOTC proved once more the necessity and the contribution of ad-hoc sensor networks to MIO and regional security operations. The sensor network was designed and configured to provide high quality services such as video-conferencing, PLI tools, and detection of illicit material. The employment of networked swimmers constitutes a milestone for this kind of network, since swimmers can be used to approach suspicious objects at the surface or on a vessel's hull and, with expert collaboration support, identify them through the exchange of video, sensor, and voice communications data. Apart from the employment of swimmers, the use of the mini-helicopter showed how UAVs can be utilized in MIO for flexible (i.e., they can more readily and rapidly position themselves) detection of CBRNE materials. The ability of UAVs to detect sources at high speeds and at some distance from the source carrier adds a valuable tool for the conduct of MIO. Furthermore, the plausible scenario during TNT/MIO 12-2 showed that the detection and identification of CBRNE material approaching by air (with a UAV in this case) is feasible by surface means. This detection can be considered an early warning when a radioactive attack by air is imminent and can result in threat interdiction and destruction in a timely manner. The centers connected to the network were aware of tagged vessels movements, through the PLI tool, at all times, allowing interdiction when necessary. The communications equipment significantly facilitated attaining the experiments' objectives: the Trellis Ware system contributed to the communication between the boarding team and headquarters while the Wave Relay systems facilitated node connection and data dissemination through the network.

E. SUMMARY

As described in this chapter, several experiments have been conducted on how ad-hoc sensor networks can facilitate MIOs and regional security operations. The technology evolution and the adaptation of innovative means during the above-described experiments show clearly the capabilities of ad-hoc sensor networks to support these security and

interdiction operations. The employment of UAVs and swimmers/divers as network nodes expand MIO-network abilities to detect illicit material in the maritime domain. Moreover, the use of appropriate networking equipment (as the respective used during the above mentioned experiments) results, except for the necessary data dissemination that can be voice, video, or sensor spectra, to the area coverage by the network augmentation. This coverage augmentation is achieved either with a range increases of direct communication between two nodes or through the use of communication relay nodes such as those used in San Francisco Bay and the riverine experiments. Furthermore, the SA tools used during these experiments resulted in better exploitation of the employed means, as well as with network control and monitoring. Another outcome from these experiments is the fact that a source can be detected and afterwards identified and evaluated without the physical presence of experts on the scene. Also, the use of UAVs and USVs to approach the source carrier and determine the presence or absence of CBRNE material increases the potential of smaller security forces to more efficiently and effectively perform these vital security and interdiction missions. In these experiments, almost all assets mentioned in Chapter III were used, except for buoys and radar nodes, proving that their employment is not only feasible, but necessary and advantageous for the evolution of these operations.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

A. CONCLUSIONS

The main concept that this thesis examined was the potential contributions of ad-hoc sensor networks in MIO and regional maritime security operations. By investigating network requirements from actual operations in the field, reviewing possible network equipment under development,, and results of relevant field experiments on ad-hoc sensor networks, the potential was shown for the use of ad-hoc sensor networks to improve mission performance during MIO and regional maritime security operations evolution and specifically enhance force protection and homeland defense against assymetric threats (e.g., CBRNE weapons) was shown.. This improvement is accomplished because network-enabled boarding teams can conduct their tasks on a suspect vessel by providing their TOC and reachback centers of excellence with real-time information (e.g., transmitting video, voice, and advanced sensor data) through the network. A multitude of platforms (e.g., warships, security patrol boats, Coast Guard Cutters, USVs and UAV, and buoys etc.) can succeed in detecting the presence of CBRNE materials being transported aboard surface vessels, and in some cases carried onboard aircraft (see experiment TNT/MIO 12–2). With the proper network communication systems, data can be disseminate through the network over significant distances either directly between two nodes or indirectly through the use of multiple nodes and their multi-hop capability. With the employment of all these means, the detection and interdiction of a vessel that may carry CBRNE material or WMDs can take place a safe distance from shore and friendly forces, minimizing the risks to friendly forces, civilians and property. Furthermore, the innovative employment of networked swimmers and divers enabled them to share, in real-time, vital information that traditionally had no way of moving very far to or from the divers in a short period of time. With ad-hoc sensor networking, divers, boarding teams, unattended sensors, security forces, and their MIO TOC can coordinate their information and operations rapidly—and with the real-time support of centers of excellence (e.g., LLNL and DTRA), high-level command and control elements (e.g., emergency operations centers, regional

headquarters, and special operations commands), and intelligence centers. Additionally, the ad-hoc sensor networks show great promise to expand and enhance coverage and adaptability for regional maritime security operations: they can provide for multi-sensor inputs to SA tools such as the Google Earth PLI for node-location monitoring. The coverage of the ad-hoc sensor network is determined, as discussed in Chapter II, by the effective communication range of its node, and their multi-hop capabilities.

This research showed that a reliable direct communication distance of seven nautical miles was achieved between mobile small surface vessels. That distance was expandable to fourteen nautical miles with the use of a relay node. Moreover, these experiments proved that the higher the antenna gain of the two nodes, the larger the throughput and data rate achieved. Consequently, one significant factor on which the coverage of an ad-hoc sensor network relies is the equipment used. With the appropriate equipment and availability of participating nodes, the network coverage can be increased significantly beyond fourteen nautical miles. Conceptually, with the inclusion of WiMAX capacities, network connectivity beyond LOS at a distance of approximately twenty-seven nautical miles is possible. With relays nodes, the area covered by the network can be augmented encompass many mobile sensor nodes operating an area with a radius of fifty nautical miles. Moreover, using UAV systems, discussed in Chapter III, the network can likely achieve data-link communications at distances of 100 nautical miles. However, connectivity range, and consequently coverage area, is highly affected by the amount and type of disseminated data (e.g., voice, video, etc.) and still has to be examined thoroughly, especially in the case of MIO networks where the assets/nodes are moving on the sea surface and in the air.

Another significant outcome regarding the use of ad-hoc networking in MIO, as it was presented in the discussed in Chapter IV's review of experimentation, is the achievement of information exchange between assets/nodes operating on-scene and remote experts located elsewhere in the world and far away from the MIO. The assets/nodes are the boarding teams, the networked swimmers, UAVs etc., that can carry sensors and disseminate the collected data through the network and consequently to the remote experts who evaluate the situation in near real-time.

Concerning the QoS that ad-hoc sensor networks provide to MIO and regional security operations, it is shown in the outcomes of the TNT/MIO experiments that data in the form of video, voice, text chat or sensor spectra can be disseminated through the network to provide other nodes (e.g., the TOC and MOB) with real-time information from the operational theater. The bandwidth capabilities in the experiments allowed duplex communication among nodes, depending on the nodes' individual equipment. The latency and the packet loss observed during experiments were not eliminated; however, most of the time, they did not prevent continuous network connectivity and reliable receipt of vital information at key nodes (e.g., TOC and reachback centers). Depending on the equipment used and the nature (e.g., number of bytes) of the data to be disseminated, ad-hoc sensor networks appear capable of effectively supporting MIO communications requirements, and offer flexibility to support moving assets/nodes, scalability, and fault tolerance. Moreover, with the appropriate array of nodes, connectivity can be maintained even in the case of node failures, resulting in network survivability during execution. Furthermore, another factor that increases the survivability of the network, and consequently the flow of information, is its own versatility: the availability of ways that participating nodes can transmit data. For example, during TNT/MIO experiments, the boarding team and swimmers could transmit and receive information to and from experts either with video or voice or through text chat via the Observer's Notepad application. When the automatic transmission of sensor spectra was not possible, the boarding team or swimmers succeeded in transmission to expert centers by uploading the data files in Observer's Notepad. The survivability of the MIO ad-hoc sensor network is also enhanced with VPN utilization, as has been tested in TNT/MIO experiments, preventing non-authorized network use and monitoring, and potential cyber attacks that could lead to DoS.

Even though ad-hoc sensor networks can support MIO and regional security operations, there are still limitations to their use. The most significant is the energy constraints of some assets/nodes. For example, the boarding team or networked swimmers have limited power available during their missions. The equipment they carry is usually battery powered, so there is the potential, of running out of energy and not

being able to share their information through the network. The same constraint may apply to UAVs such as the mini-helicopter employed in TNT/MIO experiments with NMIOTC. Energy consumption rates also depend on the applications used and the amount of data to transmit. Another limitation on ad-hoc sensor networks is the connectivity range. Although a direct connectivity range of seven nautical miles was achieved during TNT/MIO experiments and is considered more than sufficient for MIO, there remains a need for a greater connectivity range that allows a less dense array of nodes to cover data flow for a large area. Extended connectivity ranges also enhance network survivability in case of node failure. Of course, tradeoff analysis will need to be conducted to balance cost of increased connectivity coverage against more lesser-capable relay nodes. Also, the limited standoff distance from which a sensor can detect CBRNE material can be considered a potential constraint, even though it does not have to do with the network's overall performance, rather just the sensitivity of the detector itself. The throughput of the ad-hoc sensor network can also be a potential limitation. Though the throughput achieved was highly satisfying, allowing video, voice, and sensor data to be transmitted in high fidelity field experiments, the amount and variety of data can be excessively high and may not be supported by the bandwidth of the network, since throughput is reduced during multi-hop transmission. More experimentation must be conducted to understand and overcome these limits.

B. OTHER APPLICATIONS – POTENTIAL FUTURE RESEARCH

Apart from MIO and regional security operations, ad-hoc sensor networks are able to support naval area surveillance operations. For this application, radar, video, and EO/IR systems are required. During the TNT/MIO experiments discussed in this thesis, none of these systems—except for cameras—were employed. The use of smart buoys and UAVs, except for *Vellerofontis*, were not examined, though the presence of a vessel may be considered a surrogate for a buoy. Assets with the appropriate sensors and communications means can be placed in such an array to ensure the surveillance and monitoring of a wide area from the sea surface. For example, a potential area that these assets/nodes could be deployment in is waters off of the Horn of Africa where the detection and interdiction of pirate vessels that threaten safe and free commercial

navigation is a high profile mission. Another area where a network consisting of UAVs, buoys, vessels with radar, cameras, WMD sensors, and EO/IR devices, in combination with satellite surveillance, could be deployed is the Mediterranean Sea to help prevent illegal immigration from Africa and Asia to Europe.

Except for surveillance purposes, ad-hoc sensor networks like those for MIOs can enhance the force protection, not only of a naval base, but of a commercial port, by detecting suspicious cargo on vessels or floating objects that may pose an imminent threat.

Connectivity-range augmentation, direct and indirect, is one of the factors defining the coverage area of the network; the other is the coverage of each individual sensor. Together with bandwidth increase, this issue will be the object of much research. With technological evolution, these problems are likely to be resolved soon, but the tradeoff analyses will remain: as technology evolves, so does the cost of these systems. The employment of radar and surveillance systems in ad-hoc sensor networks has to be examined thoroughly to provide, in addition to the video and data dissemination discussed in this thesis, real-time radar picture through the network to other nodes such as TOCs, intelligence centers, and ships operating far away. Creating that kind of wide-area, integrated, mostly unattended sensor-provided SA picture to support decision makers' information needs should be a networking goal to provide better fidelity surveillance than can only be achieved by costly satellite surveillance or the commitment of a large number of manned military or security force assets. This is a rich area for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- [1] “Maritime Interdiction Operations.” Retrieved May, 15, 2012, from *Wikipedia*: http://en.wikipedia.org/wiki/Maritime_interdiction
- [2] A. Carr, “Maritime Interdiction Operations in support of the Counterterrorism war,” paper, Naval War College, Newport, RI, 2002.
- [3] NATO, *Allied Maritime Interdiction Operation*, Allied Tactical Publication (ATP) – 71, 2005.
- [4] I. Koukos, “Ad-hoc Sensor Networks as part of a Regional Security Grid,” *NMIOTC MIO Journal*, issue 3, pp. 40–42, May 2011.
- [5] H.J. Hof, D. Wagner, and R. Wattenhoffer, “Chapter 1: Applications of Sensor Networks,” in *Algorithms For Sensor And Ad-hoc Networks – Advanced Lectures*. Berlin, Germany: Springer, 2007.
- [6] L. Thu Bui, S. Alam, R. Rajagopalan, C. K. Mohan, K. G. Mehrotra, and P. K. Varshney, “Chapter 8: Multi-Objective Evolutionary Algorithms for Sensor Network Design,” in *Multi-Objective Optimization in Computational Intelligence: Theory and Practice*. Hersey, New York: Information Science Reference, 2008.
- [7] D. Kotsifas, “Network-based mitigation of illegal immigration in Aegean Sea (Greece),” M.S. thesis, Dept. Inform. Sci., Naval Postgraduate School, Monterey, California, 2010.
- [8] A. Kounoudes and C. Protopapas, “Artemis – A novel multipurpose Smart Buoy,” *NMIOTC MIO Journal*, issue 4, pp. 77–78, November 2011.
- [9] D. Schauland, “What is an Ad-hoc network?” [Online]. Available at: <http://www.wisageek.com/what-is-an-ad-hoc-network.htm>
- [10] “Wireless Ad-hoc Network.” Retrieved May, 15, 2012, from *Wikipedia*: http://en.wikipedia.org/wiki/Wireless_ad-hoc_network
- [11] S. Crisostomo, J. Barros, and C. Bettstetter, “Flooding the Network: Multipoint Relays versus Network Coding,” in *Proc of the 4th IEEE International Conference*, pp. 119-124, Shanghai, P.R. China, May 26–28, 2008.
- [12] M. Rouse, “Flooding definition,” June 2007. Available at: <http://searchnetworking.techtarget.com/definition/flooding>
- [13] “IEEE 802.11.” Retrieved June, 14, 2012, from *Wikipedia*: http://en.wikipedia.org/wiki/IEEE_802.11

- [14] "IEEE 802.16." Retrieved Jun, 14, 2012, from *Wikipedia*:
http://en.wikipedia.org/wiki/IEEE_802.16.
- [15] K. Scarfone, C. Tibbs, and M. Sexton, *Guide to Securing WiMAX Wireless Communications – Recommendations of the National Institute of Standards and Technology*. Gaithersburg: NIST – Computer Security Division, September 2010.
- [16] "Mobile Ad-hoc Networks (MANETs)," from Advanced Network Technologies Division of National Institute of Standards and Technology website:
http://w3.antd.nist.gov/wahn_mahn.shtml.
- [17] O. Cengiz, "Adaptive Tactical Mesh Networking: Control Base MANET model," M.S. thesis, Dept. Inform. Sci., Naval Postgraduate School, Monterey, California, 2010.
- [18] "Wireless Mesh Networks." Retrieved May, 18, 2012, from *Wikipedia*:
http://en.wikipedia.org/wiki/Wireless_mesh_networks.
- [19] M. Sichitiu, "Wireless Mesh Networks: Opportunities and Challenges," in *Proc of the Wireless World Congress*, Palo Alto, California, May 2005.
- [20] A. Bordetsky, "Detector Networking Studies NPS-LLNL Field Experimentation Based Student Studies," Naval Postgraduate School – USA Defense Threat Reduction Agency, Monterey, California, After Action Report, 2011.
- [21] S. Misra, I. Woungang, and S.C. Misra, *Guide to Wireless Sensor Networks*, London. U.K.: Springer, 2009.
- [22] "Wireless Ad-hoc Sensor Networks." from Advanced Network Technologies Division of National Institute of Standards and Technology website:
http://w3.antd.nist.gov/wahn_ssn.shtml.
- [23] F. Chen, "Single sink node placement strategy in Wireless Sensor Networks" presented at *Electric Information and Control Engineering 2011 International Conference*, pp. 1700-1703, Wuhan, P.R. China, April 15–17, 2011.
- [24] L. Saraswat and S. Kumar, "Cluster level optimization of residual energy consumption in WSN for lifetime enhancement," *International Journal on Computer Science and Engineering*, vol. 4, no2, pp. 162–165, February 2012.
- [25] S. Meguerdichian, F. Koushanfar, G. Qu and M. Potkonjak, "Exposure in Wireless Ad-hoc Sensor Networks," in *Proc of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 139-150, Rome, Italy, July 16–21, 2001

- [26] K. Kar, and S. Banerjee, "Node placement for connected coverage in sensor networks," in *Proc of WiOpt: Modeling and Optimization in Mobile, Ad-hoc and Wireless Networks*, Sophia-Antipolis, France, March 3–5 2003.
- [27] D. B. Jourdan, and O. L. de Weck, "Layout optimization for a wireless sensor network using a multi-objective generic algorithms," in *Proc of the IEEE 59th Vehicular Technology Conference*, vol. 5, pp. 2466-2470, Milan, Italy, May 17–19, 2004.
- [28] K. Ferentinos, and T. Tsiligiridis, "Adaptive design optimization of WSN using generic algorithms," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 51, issue 4, pp.1031–1051, March 2007.
- [29] L. Tong, Q. Zhao, and S. Adireddy, "Sensor Networks with Mobile Agents," in *Proc of the Military Communications Conference '03*, vol. 1, pp. 688-693, Boston, Massachusetts, October 13–16, 2003.
- [30] R. Rajopalan, and P. Varshney, "Data aggregation techniques in sensor networks: A survey," Paper 22, Syracuse University - Electrical Engineering and Computer Science Dept., 2006.
- [31] R. Mulligan, and H. Ammari, "Coverage in Wireless Sensor Networks: A Survey," in *Network Protocol and Algorithms*, vol. 2, no. 2, pp. 27–53, 2010.
- [32] G. Stavroulakis, "Rapidly Deployable, Self Forming, wireless networks for Maritime Interdiction Operations," M.S. thesis, Dept. Inform. Sci., Naval Postgraduate School, Monterey, California, 2006.
- [33] C. Levis, J. Johnson and F. Teixeira., *Radiowave Propagation Physics and Applications*. Hoboken, New Jersey: Wiley, 2010.
- [34] P. Santi, and D. Blough, "The Critical Transmitting Range for Connectivity in Sparse Wireless Ad-hoc Networks," in *IEEE Transactions on Mobile Computing*, vol.2, no.1, pp. 25–39, January–March 2003.
- [35] S. L. Willis, and C. J. Kikkert, "Radio Propagation Model for Long Range Ad-hoc wireless Sensor Networks," presented at *International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 1, pp. 826-832, Maui, Hawaii, June 13–16, 2005.
- [36] J. Frihat, F. Moldoveanu, and A. Moldoveanu, "Impact of Using Upper Layers Security in Ad-hoc Wireless Networks," *U.P.B. Sci. Bull., Series C*, vol. 71, iss.2, pp. 63–74, 2009.

- [37] M. Subramanian, "Chapter 1.8: Network Management: Goals, Organization and Functions," in *Network Management – Principles and Practice*. Boston, Massachusetts: Pearson, 2006.
- [38] A. Bordetsky, "Networking and Interagency Collaboration On Maritime – Sourced Nuclear Radiological Threat Detection and Interdiction (June 7–10, 2011)," NPS/LLNL-Monterey, California, Experiment TNT MIO 11–2 Report, 2011
- [39] "The National Oceanic and Atmospheric Administration's (NOAA) Chesapeake Bay Interpretive Buoy System (CBIBS)," from Chesapeake Bay Interpretive Buoy System website, Available at: <http://buoybay.noaa.gov/about/about-the-system.html>.
- [40] "Wave Glider Sensor Hosting Autonomous Remote Craft (SHARC) Overview," presentation by Liquid Robotics at NPS, March 06, 2012.
- [41] "Wave Glider Concept," from Liquid Robotics website: <http://liquidr.com/technology/wave-glider-concept/>.
- [42] "Wave Glider specification sheet," from Liquid Robotics website: <http://liquidr.com/files/2012/06/Wave-Glider-0612.pdf>.
- [43] "BASIL USV/Buoy specification sheet," ACSA Underwater GPS, Meyreuil, France.
- [44] Program Executive Officer, Littoral and Mine Warfare (PEO LMW), *Unmanned Maritime Systems Program Office (PMS406)*, Washington, DC, 2011.
- [45] W. Gayle, "Analysis of Operational Manning Requirement and Deployment Procedures for Unmanned Surface Vehicles Aboard U.S. Navy Ships," M.S. thesis, Dept. Bus. And Public Policy, Naval Postgraduate School, Monterey, California, 2006.
- [46] "USV Sea Fox," from NPS Center for Autonomous Vehicle Research website: <http://www.nps.edu/Academics/Centers/CAVR/Vehicles/SeaFox.html>.
- [47] "U-Ranger7 Data Sheet," Calzoni Marine Handling and Lighting Solutions, Bologna, Italy, May 2009.
- [48] "Intergrator UAV Specification Sheet," Insitu Inc., Bingen, WA.
- [49] "Fury 1500 UAV Specification Sheet," AME Unmanned Air Systems, San Luis Obispo, California.
- [50] "SR 200 VTOL UAV Specifications," from Rotomotion LLC website, available at: http://www.rotomotion.com/prd_UAV_SR200.html.

- [51] “CybAero – APID 60 VTOL UAV System Specification Sheet,” from CybAero Inc. website, available at:
http://www.cybaero.se/upload_docs/271_Produktblad%20CybAero%20APID%2060.pdf.
- [52] “SAAB Skeldar V-200 UAV Specification Sheet,” SAAB technologies group.
- [53] “CENETIX mission,” from CENETIX-NPS website:
<http://cenetix.nps.edu/cenetix/cenetix.asp>.
- [54] A. Bordetsky, “Networking and Collaboration On Interdicting Multiple Small Craft Possessing Nuclear Radiation Threat,” NPS/LLNL-Monterey, California, Experiment TNT/MIO 09–02 After Action Report, 2009.
- [55] A. Bordetsky, “Networking and Interagency Collaboration On Small Craft Maritime – Sourced Nuclear Radiological Threat Detection and Interdiction (November 5, 2010),” NPS/LLNL-Monterey, California, Experiment TNT/MIO 10–02 Final Report, 2010.
- [56] A. Bordetsky, “Networking and Interagency Collaboration On Maritime – Sourced Nuclear Radiological Threat, Port of NY-NJ / Fort Eustis / Europe (September 08–12, 2008),” NPS/LLNL-Monterey, California, Experiment TNT/MIO 08–04 Quick Look Report, 2008.
- [57] “Wave RelayTM technology,” from Persistent Systems, LLC website:
<http://www.persistentsystems.com/technology.php>.
- [58] “Wave RelayTM MPU4 specification sheet,” from Persistent Systems website:
http://www.persistentsystems.com/products_7a.php.
- [59] “Wave RelayTM MPU3 specification sheet,” from Persistent Systems website:
http://www.persistentsystems.com/products_2a.php.
- [60] “Wave RelayTM Quad Radio Router specification sheet,” from Persistent Systems website: http://www.persistentsystems.com/products_4a.php.
- [61] “Wave RelayTM Sector Antenna Array specification sheet,” from Persistent Systems website: http://www.persistentsystems.com/products_3a.php.
- [62] “TW-220 CheetahNet Radio specification sheet,” from TrellisWare technologies website: <http://www.trellisware.com/products/manet-products/cheetahnet-tw-220/>.
- [63] A. Bordetsky, “Networking and Interagency Collaboration On Maritime-Sourced Nuclear Radiation Threat and Small Craft Interdiction, San Francisco, CA / Fort Eustis, VA / Germany / Sweden / Greece (September 09–10 / 24–30, 2009),” NPS/LLNL-Monterey, California, Experiment TNT/MIO 09–04 Report, 2009.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Dr. Dan Boger
Department of Information Sciences
Naval Postgraduate School
Monterey, California
4. Dr. Alex Bordetsky
Department of Information Sciences
Naval Postgraduate School
Monterey, California
5. Commander (USN) John P. Looney
Department of Information Sciences
Naval Postgraduate School
Monterey, California
6. Lieutenant (HN) Theofanis Kontogiannis
Hellenic Navy General Staff
Athens, Greece
7. Embassy of Greece
Office of Naval Attaché
Washington, DC
8. Hellenic Navy General Staff
Athens, Greece