2015-03

Supporting the maritime information dominance: optimizing tactical network for biometric data sharing in maritime interdiction operations

Sinsel, Adam R.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SUPPORTING THE MARITIME INFORMATION DOMINANCE: OPTIMIZING TACTICAL NETWORK FOR BIOMETRIC DATA SHARING IN MARITIME INTERDICTION OPERATIONS

by

Adam R. Sinsel

March 2015

Thesis Advisor:	Alex Bordetsky
Second Reader:	Albert Barreto

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
SUPPORTING THE MARITIME INFORMATION DOMINANCE: OPTIMIZING TACTICAL NETWORK FOR BIOMETRIC DATA SHARING IN MARITIME INTERDICTION OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Adam R. Sinsel

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)

This research intends to improve information dominance in the maritime domain by optimizing tactical mobile ad hoc network (MANET) systems for wireless sharing of biometric data in maritime interdiction operations (MIO). Current methods for sharing biometric data in MIO are unnecessarily slow and do not leverage wireless networks at the tactical edge to maximize information dominance. Field experiments allow students to test wireless MANETs at the tactical edge. Analysis is focused on determining optimal MANET design and implementation. It considers various implementations with varied antenna selection, radio power, and frequency specifications, and two specific methods of integrating Department of Defense biometric collection devices to the wireless MANET, which utilizes a single (WR) MPU4 802.11 Wi-Fi access point to connect secure electronic enrollment kit II (SEEK II) biometric devices to the MANET, and tethers each SEEK device to a dedicated WR using a personal Ethernet connection. Biometric data is shared across the tactical network and transmitted to remote servers. Observations and analysis regarding network performance demonstrate that wireless MANETs can be optimized for biometric reach back and integrated with biometric devices to improve biometric data sharing in MIO.

14. SUBJECT TERMS
MIO, VBSS, MANET, wireless mesh

15. NUMBER OF PAGES
85

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

SUPPORTING THE MARITIME INFORMATION DOMINANCE: OPTIMIZING TACTICAL NETWORK FOR BIOMETRIC DATA SHARING IN MARITIME INTERDICTION OPERATIONS

Adam R. Sinsel
Lieutenant, United States Navy
B.S., University of Idaho, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2015

Author: Adam R. Sinsel

Approved by: Alex Bordetsky
Thesis Advisor

Albert Barreto
Second Reader

Cynthia Irvine
Chair, NPS Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research intends to improve information dominance in the maritime domain by optimizing tactical mobile ad hoc network (MANET) systems for wireless sharing of biometric data in maritime interdiction operations (MIO). Current methods for sharing biometric data in MIO are unnecessarily slow and do not leverage wireless networks at the tactical edge to maximize information dominance. Field experiments allow students to test wireless MANETs at the tactical edge. Analysis is focused on determining optimal MANET design and implementation. It considers various implementations with varied antenna selection, radio power, and frequency specifications, and two specific methods of integrating Department of Defense biometric collection devices to the wireless MANET, which utilizes a single (WR) MPU4 802.11 Wi-Fi access point to connect secure electronic enrollment kit II (SEEK II) biometric devices to the MANET, and tethers each SEEK device to a dedicated WR using a personal Ethernet connection. Biometric data is shared across the tactical network and transmitted to remote servers. Observations and analysis regarding network performance demonstrate that wireless MANETs can be optimized for biometric reach back and integrated with biometric devices to improve biometric data sharing in MIO.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. PROBLEM STATEMENT 4
- B. PURPOSE 4
- C. RESEARCH QUESTIONS 5
- D. POTENTIAL BENEFITS 5
- E. ORGANIZATION OF THESIS 5
- F. SCOPE AND LIMITATIONS 6
- G. INFORMATION DOMINANCE CONSIDERATIONS 8
  - 1. Quality Criteria and Information Dominance 8
  - 2. MIO Information Dominance through Wireless Biometric Data Sharing 11
- H. TECHNICAL FOUNDATIONS 13
  - 1. 802.11X Wireless (Wi-Fi) 13
  - 2. Wireless Mesh 14
  - 3. Mobile Ad Hoc Networks 16
  - 4. Wave Relay 18
- I. CENETIX BIOMETRICS DATA SHARING FRAMEWORK 19
  - 1. SEEK II 20
  - 2. Tactical Network and WRN 22
    - *a. Shipboard SATCOM 22*
    - *b. Commercial off-the-Shelf Global Satellite 23*
    - *c. 3G/4G 24*
    - *d. ISP 25*
  - 3. DOD Automated Biometric Identification System 25
  - 4. Biometrically Enabled Watch List 27
  - 5. ABIS versus BEWL 27
- J. SECURITY 28
  - 1. FIPS 140-2 Security Requirements for Cryptographic Modules .. 29
  - 2. Wave Relay FIPS 140-2 Compliance 30
    - *a. Wave Relay MANET FIPS 140-2 Compliance 30*
    - *b. Cipher WR 802.11 WAP FIPS 140-2 Compliance 31*
  - 3. VPN 32

II. CENETIX EXPERIMENTS IN A MIO SETTING 33
- A. NPS MIO WMD ISR EXPERIMENT, AUGUST 2014: OPTIMIZING THE WAVE RELAY MANET 34
  - 1. Antenna Selection 35
  - 2. Radio Selection 37
  - 3. Channel Bandwidth 38
- B. NPS BIOMETRIC EXPERIMENT, OCTOBER 2014: CONDUCTING IDENTIFICATION OPERATIONS USING REACH BACK 39
  - 1. Concept of Operations 40

2. Scenario and Network Design 41
3. Experiment Execution 44
4. Experiment Observation and Conclusions 46

III. ADDITIONAL ANALYSIS 49
A. WIRELESS BIOMETRICS AND INFORMATION DOMINANCE 49
B. WAVE RELAY OPTIMIZATION 49
1. Replacing Omnidirectional Antenna with Sector Antenna 50
2. Range between MANET NODES 51
C. SEEK II INTEGRATION MODELS 52
1. Performance 52
2. Security 53

IV. CONCLUSIONS AND RECOMMENDATIONS 55
A. CONCLUSIONS 55
B. FUTURE WORKS 57
1. Optimization of the Tactical MANET 57
2. Layer 2 MANET Security 57

LIST OF REFERENCES 59

INITIAL DISTRIBUTION LIST 63

LIST OF FIGURES

Figure 1. Quality Information Criteria, from [23] 9
Figure 2. Discovery to Decision Continuum, from [10] 10
Figure 3. Typical WMN, from [14] 16
Figure 4. Simple Mesh Autonomous Behavior 17
Figure 5. Quad Radio and MPU4 Specification Comparison, from [18]–[20] 18
Figure 6. SEEK II by Crossmatch Technologies, from [24] 21
Figure 7. BGAN versus VSAT, from [27] 24
Figure 8. Summary of FIPS 104-2 Security Requirements by Level, from [36] 30
Figure 9. GTS Admiral W. M. Callaghan 42
Figure 10. Experiment Network Diagram 43

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Impact to Quality Criteria 12
Table 2. Wave Relay Frequency and Range Specifications, from [19] 38
Table 3. Antenna Selection Impact on Network Performance 45
Table 4. Network Performance during Biometric Operations 46

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF EQUATIONS

Equation 1. Ideal Link Equation..50
Equation 2. Describing 6 dB Rule of Thumb..51

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	after action report
ABIS	automated biometric identification system
ADNS	automated digital network system
AES	advanced encryption standard
AOR	area of operations
ARCIC	Army Capabilities Integration Center
ATO	authority to operate
BEC	biometrics enabling capabilities
BEWL	biometrically enabled watch list
BGAN	broadband global area network
BIMA	Biometric Information Management Activity
BSS	basic service set
C2	command and control
CBRN	chemical, biological, and radiological nuclear
CBSP	commercial broadband satellite program
CD/RW	compact disc-rewritable
CENETIX	Center for Network Innovation and Experimentation
CONOP	concept of operations
COOP	continuity of operation plan
COTS	commercial-off-the-shelf
CSMA-CA	carrier sense multiple access, collision avoidance
DFBA	Defense Forensics and Biometrics Agency
DOD	Department of Defense
DRAM	dynamic random access memory
DSCS	defense satellite communications
EBTS	electronic biometric transmission specification
EFTS	electronic fingerprint transmission specification
EMI/EMC	electromagnetic interference/electromagnetic compatibility
ESS	extended service set
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FIPS	federal information processing standard

GPS	Global Positioning System
GUI	graphical user interface
HDD	hard disk drive
HTTP	hyper text transfer protocol
HTTPS	secure HTTP
IAFIS	Integrated Automated Fingerprint Identification System
IBSS	independent basic service set
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet engineering task force
ISP	Internet service provider
JIFX	Joint Interagency Field Experimentation
LAN	local area network
LOS	line of sight
MANET	mobile ad hoc network
MIO	maritime interdiction operations
MPU4	manned portable unit generation 4
NoT	network on target
NPS	Naval Postgraduate School
NRT	near-real-time
OMS/MP	operational mode summary/mission profile
P2P	point-to-point
PEO	program executive office
PMP	point-to-multipoint
POI	persons of national interest
PSK	pre-shared key
RF	radio frequency
RFC	request for comment
RSE	rapid site exploitation

SA	situational awareness
SAOFDM	self-aligning orthogonal frequency division multiplexing
SATCOM	satellite communications
SEEK II	secure electronic enrollment kit II
SFPD	San Francisco police department
SHA-2	secure hash algorithm 2
SHF	super high frequency
SNR	signal to noise ratio
SOCOM	Special Operations Command
SSE	sensitive site exploitation
TCM-BF	TRADOC capability manager biometrics and forensics team
TNT	tactical network topology
TNT WMD ISR	tactical network test bed, weapons of mass destruction: intelligence surveillance and reconnaissance
TRADOC	Training and Doctrine Command
TTP	tactics, techniques, and procedures
UGV	unmanned ground vehicle
UHF	ultra high frequency
USB	universal serial bus
USCG	United States Coast Guard
USN	United States Navy
VBSS	visit board search and seizure
VPN	virtual private network
VSAT	very-small-aperture terminals
WAP	wireless access point
WLAN	wireless local area network
WMD	weapons of mass destruction
WMN	wireless mesh networks
WPA2-PSK	Wi-Fi protected access 2-pre-shared key
WR	Wave Relay
WRN	wireless reach back network
YBI	Yerba Buena Island

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I could not have completed this work without the love and support of my family. Diana Sinsel, my loving wife, encouraged me daily and handled all manner of family affairs during my thesis travel and during my long hours in the lab. My children, Jacob and Kaylee, inspire me each day to be a better person, reach my goals, and to lead by example. I was blessed to have Dr. Alex Bordetsky advise me in completing this thesis. His expertise and support have been invaluable to me. I cannot thank him enough for guiding me through this milestone in my life. Albert “Buddy” Barreto was a life saver. As my second reader, he was tough and fair. His technical expertise was vital to my success, and our conversations on a wide range of topics kept me entertained. Eugene Bourakov worked wonders in helping me prepare and execute experiments, and I won’t forget it. Steve Mullins is the glue that holds the CENETIX group together. I greatly appreciate all that he does. Finally, Rob Schulz, Matt Maupin, Dan Lee, Malcom Mejia and other CENETIX student researchers were an amazing team. I owe them all an enormous debt of gratitude.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In recent years, the United States' maritime strategy has become increasingly focused on securing this nation's ports and protecting international maritime commons against potential sea-born terrorist attacks. Specifically, the threats include chemical, biological, and radiological nuclear (CBRN) weapons and traditional terrorist activity. Department of Defense (DOD) and U.S. Government Accountability Office research [1] shows that information sharing in maritime interdiction operations (MIO) and visit board search and seizure (VBSS) operations in littoral waters as key in successfully implementing this strategy. Likewise, Navy strategy for information dominance points out the importance of accurate and timely information sharing in the maritime domain. Relevant DOD and joint publications echo the importance of the same.

Boarding teams at the forefront of maritime security operations require a rapid and reliable exchange of information to execute MIO and VBSS missions, which is especially true of biometric data regarding potential adversaries or persons of interest to national security. Information sharing in MIO typically begins with data captured on-site (a boarded vessel) during rapid site exploitation (RSE), when operators are expected to gather biometric and other forensic data and disseminate it to remote decision makers. In some cases, operators are expected to stay on site until biometric systems or analysts have provided responses, such as match-no-match results. These responses drive the actions of operators.

Identification and verification operations, requiring biometrics collection and dissemination, are of particular operational value in the maritime domain in which adversaries can be difficult to identify because of false identification documents or a complete lack of documentation. Biometric data sharing directly counters this fundamental challenge. However, sufficiently addressing this challenge requires the DOD to leverage available biometric and tactical networking technologies fully. It demands efficient and dependable data sharing from operators to distributed nodes, on which authoritative data resides and analysts interact with the decision cycle. MIO operators are expected to make prudent decisions, based on accurate and timely information about their adversaries. To occur, the highest quality biometric data must be provided to decision makers and operators throughout the decision cycle; a natural byproduct of achieving and maintaining information dominance in the maritime domain. To that end, MIO and VBSS operators at the tactical edge must be equipped with suitable tactical networks, capable biometric devices, and access to authoritative biometric databases.

Nationally managed authoritative biometric databases, such as the DOD automated biometric identification system (ABIS), currently exist to support biometric analysis and decision making for operators. However, operators deployed to austere environments routinely lack network connectivity for reach back to ABIS.

Current procedures for biometric data sharing in austere environments require operators use on one of two untimely and inefficient methods for biometric data sharing. In the first—and most common—case, operators rely on scaled-down databases residing locally on the biometric device. For example, Crossmatch's Secure Electronic Enrollment Kit II (SEEK II) maintains a local copy of a mission or region specific biometrically enabled watch list (BEWL), which is regularly updated by the Biometric Information Management Activity (BIMA) in Clarksburg, West Virginia. Operators are expected to download the newest appropriate BEWL from BIMA on a regular basis. This scenario presents obvious shortfalls in the timeliness and accuracy of biometric data available at the tactical edge. For instance, biometric enrollments taken in Afghanistan today may be of operational significance to a VBSS team in the Arabian Gulf tomorrow. If that VBSS team is comparing biometric data against an outdated BEWL tomorrow, it would negatively impact mission success significantly. In terms of information dominance, operators using this option rely absolutely on manually retrieving the current BEWL.

The second option requires operators to manually transfer newly captured biometric data from mobile biometric devices to a suitable network using external devices (universal serial bus [USB] flash drive or compact disc-rewritable [CD/RW]). Typically, the network to which biometric data is being transferred is geographically separated from the operator. For example, an afloat boarding team member must leave the *boarded vessel* and return to the mother ship's network to transmit newly collected biometric data, and await results. In this situation as well, the process introduces obvious inefficiencies and unnecessary opportunities for human error that reduces data quality and weakens efforts to achieve information dominance.

Since 2004, the Center for Network Innovation and Experimentation (CENETIX) researchers at Naval Postgraduate School (NPS) have experimented with iterative improvements to data-sharing capabilities for various types of RSE data, including biometrics. To this end, CENETIX researchers bring to bear the NPS-SOCOM, or Special Operations Command, tactical network topology (TNT) and MIO test-bed, which provides a range of tactical networking systems, weapons of mass destruction (WMD) sensors, and biometric devices. Thus far, CENETIX research in the area of biometric data sharing has existed largely as a subset of work centered on tactical wireless networks and near-real-time (NRT) reach back for RSE in MIO events [2].

In recent experiments, CENETIX researchers have tested MANET technology in MIO settings using WR tactical radios by Persistent Systems, which offers wireless operation using dynamic routing capabilities and built in security controls. Although the wireless MANET algorithms utilized by WR are proprietary, these tactical radios also support standard wireless technologies, such as IEEE 802.11 Wi-Fi and Bluetooth [3], [4]. This flexibility provides a wide range of options for wireless node placement and configurations on the tactical network, which provide MIO and VBSS boarding teams vital communication and reach back capabilities. However, Persistent Systems does not recommend any wireless operation outside of its proprietary MANET, and the Crossmatch SEEK II biometric collection device is not currently authorized to connect to DOD systems via 802.11 Wi-Fi. To this point, CENETIX researchers have not yet flexed the Wi-Fi capabilities of WR and SEEK II to conduct biometric data sharing in field experiments. Doing so provides the opportunity for an evidence-based comparative analysis between strictly MANET wireless operation and an integrated model that includes 802.11 Wi-Fi operation.

To meet this challenge, this research advances previous CENETIX work by leveraging national level field experimentation, conducted in cooperation with SOCOM and the United States Coast Guard (USCG) Research and Development Center, as a testing platform for biometric data sharing over the tactical wireless MANET [5].

CENETIX field experiments provide a realistic MIO environment for testing various models of wireless biometric data sharing and viewing, firsthand, its impact on information dominance in the maritime domain.

A. PROBLEM STATEMENT

Operators conducting MIO currently use the Crossmatch SEEK II, and similar mobile devices, to collect biometrics during the RSE phase of MIO. Under the current model for employing these devices, operators are often forced to transfer biometric data manually from the biometric device via a USB flash memory or CD/RW to connected networks for dissemination to authoritative databases for comparison and analysis, or to depend on a locally stored and scaled down non-authoritative database for biometric comparison. This model for biometric data sharing unnecessarily reduces the timeliness and accuracy of mission data, which decreases situational awareness (SA), and challenges information dominance in the maritime domain.

B. PURPOSE

This research explores the benefits of wireless biometric data sharing in a MIO setting using tools within the CENETIX TNT MIO test-bed—including WR tactical networks and the SEEK II biometric collection device—to determine the most optimal integration of WR MANET, 802.11 Wi-Fi, and DOD biometric technologies to provide secure, reliable, NRT biometric data sharing at the tactical edge and support the Navy's strategy for information dominance in the maritime domain. Based on WR manufacturer recommendations, and previous CENETIX research, two viable models for wireless biometric transfer over WR will be tested and compared during CENETIX field experiments. The outcomes of these experiments inform a comparative analysis of network performance and security in the two proposed wireless implementations

C. RESEARCH QUESTIONS

This research is aimed at answering the following questions:

- How can wireless biometric data sharing support information dominance in the maritime domain?
- What is the wireless model for biometrics data sharing?
- How can WR technologies, including 802.11 Wi-Fi, be implemented to optimize the performance of the CENETIX tactical network for biometric data sharing?
- What changes can be made to the CENETIX tactical network to make it more optimal for biometric data sharing?
- How can the Crossmatch SEEK II be integrated into tactical WR MANET to provide NRT reach-back to remote C2 sites for RSE and biometric data sharing in MIO?
- What specific cyber security concerns exist with each of these solutions, and how can they mitigated?

D. POTENTIAL BENEFITS

This research is intended to provide a detailed analysis of various wireless technology and tactical network implementations that can reduce delays in RSE and biometric data sharing. Conclusions and recommendations should assist in optimizing tactical wireless networks used in MIO to support mission success and information dominance by reducing risk to the operator, compressing the decision cycle, and improving the timeliness and accuracy of mission data.

E. ORGANIZATION OF THESIS

1. Chapter I: Introduction

This chapter introduces the role of biometric data sharing in the RSE phase of MIO and VBSS operations and provides context for the research that seeks to improve biometric data sharing through the implementation of tactical wireless technologies.

2. Chapter II: Research Foundations

This chapter examines foundational research to support research objectives. It examines joint and service specific documents to demonstrate the relationship between wireless biometric data sharing information dominance in the maritime domain. It also provides technical foundations for the specific wireless technologies used by CENETIX to perform the wireless biometric data sharing.

3. Chapter III: Experiments in a MIO Setting

This chapter describes the field experiments conducted to optimize the CENETIX tactical network for the purpose of WR and SEEK II integration in wireless biometric data sharing. Iterative analysis and conclusions for each experiment influenced ongoing research, and are included for each experiment in this chapter.

4. Chapter IV: Additional Analysis

This chapter provides additional comparative analysis on matters that are not specifically addressed in Chapter III. Analysis from Chapters III and IV are crucial in developing ultimate conclusions from this research.

5. Chapter V: Conclusions and Recommendations

This chapter presents conclusions and recommendations that address the research questions and are based on analysis throughout the thesis.

F. SCOPE AND LIMITATIONS

This thesis focuses on the application of tactical wireless technologies in MIO strictly for the purpose of biometric data sharing during RSE. The general concepts of MANET, and the broader topic of wireless mesh networking technology, underpin this work. However, based on product availability, and the results of previous testing, experiments are conducted using WR radios from Persistent Systems. Various aspects of the WR, such as the dynamic routing algorithm, are considered proprietary. At times, generalizations about network behavior are required that will be supported by experiment data.

The Crossmatch SEEK II is a DOD-approved handheld biometrics collection device with a variety of connection interfaces available for networking and data transfer. CENETIX has SEEK II devices on hand for testing and experimentation. Therefore, only the SEEK II is used for biometric collection and during field experiments. research foundations

This research was conducted using the CENETIX TNT test bed and existing DOD technologies used in the collection and sharing of biometric data. The CENETIX tactical network is a broad term encompassing many technologies and specific technological implementations that support ongoing experimentation and research to improve SA and data sharing in MIO and CBRN detection and reporting operations. The “plug and play” TNT test bed, as well as a range of mesh networking and MANET devices, can be rapidly deployed and customized for a range of operational requirements. CENETIX maintains a robust inventory of tactical networking devices and components from various venders [6].

For the purpose of this research, the tactical network (deployed on the boarded vessel) is constructed with two variants of the proprietary WR radio by Persistent Systems, both of which typically operate as Layer 2 MANETs. In addition to the deployment of WR MANET to the *boarded vessel*, specialized devices are required for biometric data collection, sharing, and analysis, which includes user-operated end devices, as well as access to specialized databases. The biometric collection device used for this research is the SEEK II by Crossmatch, with Ethernet connectivity and standard 802.11 wireless capability. For testing purposes, the U.S. Army’s Training and Doctrine Command (TRADOC) capability manager biometrics and forensics team provided CENETIX researchers access to the SOFEX portal for identity operations. CENETIX uses the SOFEX portal for testing biometric data against an authoritative database [7].

This chapter serves two purposes. It describes the relationship between wireless biometric data sharing and information dominance in the maritime domain, and also fully describes each of the components and technologies required to perform wireless biometric data sharing using the two proposed models.

G. INFORMATION DOMINANCE CONSIDERATIONS

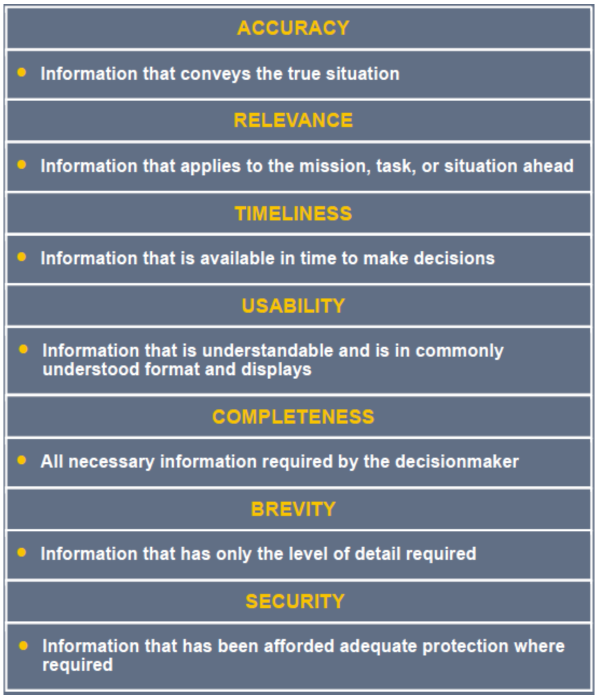
One objective of this research is to determine how wireless biometric data sharing can help achieve information dominance in the maritime domain. To answer that question properly, insights from multiple DOD joint and service-specific strategy and policy documents combine to provide a comprehensive understanding of the notion of information dominance and its relationship to success in MIO.

1. Quality Criteria and Information Dominance

Information dominance is a broad term that can be applied across the entirety of full spectrum warfare. Achieving information dominance is essential to C2. Joint Publication 6-0 joint information system stresses, "In one way or another, C2 is essentially about information: getting it, judging its value, processing it into useful form, acting on it, and sharing it with others" [8]. It is clear then that information is powerful, and that defining information dominance is instructive in determining how existing and future information systems can leverage this power to strengthen operational capability. The U.S. Navy's strategy for achieving information dominance defines information dominance as "the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects" [9].

The Navy's strategy further identifies three fundamental capabilities of information dominance: assured C2, battlespace awareness, and integrated fires. The strategy intends to combine these three capabilities to equip operational commanders with mobility in the information domain and create decision cycles that are faster than the adversary's [9]. Assured C2 entails the ability to exchange orders and responses with subordinates, understand the disposition of friendly forces, target and conduct strikes, and assess results. Battlespace awareness refers to persistent surveillance of maritime and information domains, knowledge of this nation's adversaries' capabilities and intent, and an understanding of how, when, and where U.S. adversaries operate. Integrated fires refers to the Navy's use of cyberspace to exploit and attack this country's adversaries' vulnerabilities to achieve non-kinetic effects [9].

Navy strategy for information dominance begins with the premise that information is a key enabler of mission success. Essentially, the military that can best sense, process, and deliver information will have the advantage in battle space awareness, C2, and decision making, which agrees with joint DOD guidance on information sharing and joint information systems. The DOD information sharing strategy identifies information as a force multiplier, capable of increasing operational effectiveness by increasing SA and improving C2 [10]. To that end, Joint Publication 6-0 asserts the importance of quality information in effective C2 and identifies seven key criteria of quality information as seen in Figure 1 [8].



ACCURACY

- Information that conveys the true situation

RELEVANCE

- Information that applies to the mission, task, or situation ahead

TIMELINESS

- Information that is available in time to make decisions

USABILITY

- Information that is understandable and is in commonly understood format and displays

COMPLETENESS

- All necessary information required by the decisionmaker

BREVITY

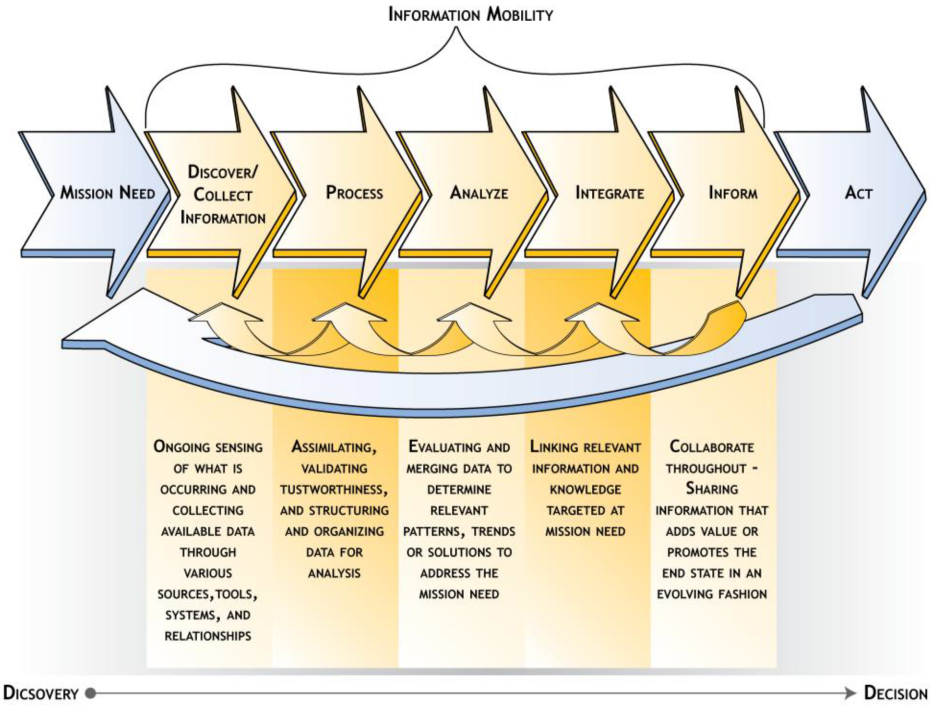
- Information that has only the level of detail required

SECURITY

- Information that has been afforded adequate protection where required

Figure 1. Quality Information Criteria, from [23]

The DOD information sharing policy describes two key concepts that directly enhance information dominance, information mobility and the universal information sharing value chain. Information mobility is defined as “the dynamic availability of information, which is promoted by the business rules, information systems, architectures, standards, and guidance/policy to address the needs of both planned and unanticipated information sharing partners and events. Information mobility provides the foundation for shared and user-defined situational awareness" [10]. The universal information sharing value chain serves as a framework that ensures information mobility and supports decision makers by implementing the discovery to decision continuum for data sharing. This model, displayed in Figure 2, is intended to "to discover and collect information and continuously add value at each stage to best inform a decision maker" [10].



Information Mobility
Mission Need
Discover/ Collect Information
Process
Analyze
Integrate
Inform
Act
Ongoing sensing of what is occurring and collecting available data through various sources,tools, systems, and relationships
Assimilating, validating tustworthiness, and structuring and organizing data for analysis
Evaluating and merging data to determine relevant patterns, trends or solutions to address the mission need
Linking relevant information and knowledge targeted at mission need
Collaborate throughout - Sharing information that adds value or promotes the end state in an evolving fashion
Dicsovery
Decision

Figure 2. Discovery to Decision Continuum, from [10]

Clearly, the DOD and the Navy agree that information is a key enabler of mission success and a force multiplier. Moreover, for information to provide the greatest impact to mission success, it must be derived from sources and systems that ensure information accuracy, timeliness, relevance, usability, completeness, brevity, and security. For decision makers to leverage this quality information fully, systems and procedures must support effective sharing and continuous improvement of information that is accomplished through information mobility and the perpetual use of the universal information sharing value chain. Using this framework, the result is an information advantage that allows decision makers who use information for one of two purposes, the creation of shared SA for decision makers, and the direction and coordination in the execution of those decisions [8].

By assisting in these decision-making functions, ever improving information, possessing key quality criteria, demonstrates operational value and creates information dominance.

2. MIO Information Dominance through Wireless Biometric Data Sharing

First, it must be stated that the wireless models of operation considered in this thesis are intended as additional capabilities for operators. Boarding team members in MIO settings, and other personnel engaged in identification and verification operations, will continue to maintain a local BEWL for specific missions and area of operations (AORs). This continuation provides redundancy in the case of connectivity loss, as well as flexibility in cases in which urgent requirements prefer the immediacy of a local BEWL over the accuracy and authority of DOD ABIS. However, operational advantages are clearly possible by connecting operators to authoritative databases. The thrust of this research assumes that connectivity to be the ultimate goal.

By providing access to higher quality data on authoritative sources, such as ABIS, wireless operation for the operator directly contributes to identity dominance, which the Defense Forensics and Biometrics Agency (DFBA) defines as:

> The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity and/or to counter our biometric technologies and processes. This is accomplished through the use of enabling technologies and processes to establish the identity of an individual and to establish a knowledge base for that identity. This includes denying an adversary the ability to identify our protected assets. [11]

Identify dominance, in action, continuously builds authoritative identity repositories, such as the DOD ABIS, and supplies operators and decision makers on the tactical edge with quality biometric information. Additionally, identity dominance supports assured C2 and promotes battlespace awareness; two of the three fundamental capabilities of information dominance. In this way, identity dominance informs decision makers and is a vital subset of information dominance.

Additionally, key components and characteristics of the wireless model for biometric data sharing directly address information quality criteria as defined by the DOD. As shown in Table 1, reach back to the DOD ABIS directly impacts each of the seven quality criteria.

Table 1. Impact to Quality Criteria

Quality Criterion	**Benefit from Wireless Reach Back Biometric Operations**
Accuracy	DOD ABIS is authoritative and constantly updated from valid DOD and interagency sources [11].
Relevance	DOD ABIS is dedicated to DOD valued biometric data [11].
Timeliness	ABIS Priority levels are set by operational mode and mission profile [33].
Usability	DOD EBTS enrollment format was designed to ensure usable data in each enrollment [22].
Completeness	DOD EBTS enrollment format ensures completeness [22].
Brevity	DOD EBTS enrollment format forces brevity [22].
Security	WR utilized integrated hardware cryptographic accelerator, FIPS 140-2 (Up to level 2), Suite B algorithms, tamper resistant hardware, AES-CTR-256 with SHA-512 HMAC, and Over the air re-keying [18], [19].

The proposed wireless model supports Navy strategy for information dominance in two ways. First, it expands the DOD's ability to determine the disposition of forces that directly addresses the Navy's strategy objective to ensure assured C2 as an integral piece of information dominance. Identification and verification operations carried out by MIO operators provide vital information about this nation's adversaries. Connecting MIO decision makers and operators to a live authoritative database (ABIS) increases the quality of information available to them on the tactical edge. Moreover, as operators query ABIS, their inputs grow the ABIS database by providing previously undocumented enrollments, which increases the quality of biometric information resident on the authoritative source. This mutual data sharing has a synergetic effect on the system and improves C2 capabilities for future operations. Secondly, this model, applied in a MIO setting, supports the Navy's strategic goal to achieve battlespace awareness, by improving data sharing in the persistent monitoring of the maritime domain, and by way of identity dominance, extracting key knowledge about U.S. adversaries' intent and operations.

Wireless biometric data sharing offers opportunities for leveraging quality information to enable mission success. By connecting operators, the authoritative DOD ABIS using wireless reach back, DOD biometric repositories, and MIO personnel will benefit from improved data quality. Additionally, this wireless model supports the discovery to decision chain, which allows for continual improvement of information quality throughout the decision cycle. The model promotes assured C2 and improves battlespace awareness. Thus, the appropriate implementation of wireless biometric data sharing can improve mission success and help achieve information dominance in the maritime domain.

H. TECHNICAL FOUNDATIONS

The primary benefit to operators of the tactical wireless network is the flexibility and mobility provided by wireless functionality. Since 2004, CENETIX has experimented with various technologies, including ultra-wide band wireless, mesh networking, MANET, and others, to provide wireless communication to operators. The dynamic requirements-based nature of tactical wireless networks ensures the continued evolution of the tactical wireless models employed by CENETIX researchers. This section provides an in depth description of the particular technologies used for this research.

1. 802.11X Wireless (Wi-Fi)

Wireless local area network (WLAN) or Wi-Fi technology is incredibly common in industry and consumer electronics. The 802.11X, as outlined by the Institute of Electrical & Electronics Engineers (IEEE), originated in 1997 as a method to replace the costly physical infrastructure requirements of wired local area networks (LAN). The wireless model made applying changes to LANs, such as additions and deletions, much more simple and affordable. In Wi-Fi, instead of data being transmitted over the physical wire, it is transmitted over radio frequency (RF) radio waves, on channels within the 2.4 GHz or 5 GHz bands. The 2.4 GHz setting falls into the ultra high frequency (UHF) band and typically offers a greater range than the 5.0 GHz setting, which operates in the super high frequency (SHF) band and offers greater bandwidth [12].

Wi-Fi generally works in a point-to-multipoint (PMP) fashion, which extends the network to meet users' needs. In this way, Wi-Fi offers great flexibility to connect many different types of devices, such as laptops and biometric scanners to a network or the Internet. The Wi-Fi standard also allows for point-to-point (P2P) connectivity to enable two Wi-Fi devices to communicate directly with one another. Wi-Fi operates in one of two modes. Sometimes, Wi-Fi operates in ad hoc mode as part of the independent basic service set (IBSS), which typically happens when services are unavailable or unnecessary, and underlying wireless infrastructure does not exist. More commonly, Wi-Fi operates in infrastructure mode, where at least two wireless nodes connect to at least one wireless access point (WAP), which is referred to as the basic service set (BSS). Two or more BSS networks together form an extended service set (ESS) [12].

Wi-Fi is scalable and adaptable, which makes it suitable for integration with other technologies, such as WiMAX, wireless mesh, MANET, and others. Due to its relatively easy application in a variety of settings, Wi-Fi can be suitable for military purposes in some scenarios. For the purpose of this research, the term Wi-Fi refers to standard 802.11X networks operating in infrastructure mode (BSS or ESS). The term wireless mesh refers to wireless networks operating in ad hoc mode (IBSS). The distinction is more thoroughly described in the following section.

2. Wireless Mesh

Wireless mesh networks (WMN) are a derivative of the lesser utilized ad hoc mode of the 802.11X wireless (or IBSS). WMNs eschew traditional Wi-Fi infrastructure, such as APs and routers, to create a flat and dynamic network of wireless nodes. WMNs provide an excellent alternative technology for last mile communications because each node is not only a host, but also a router [13]. The nodes themselves are responsible for forwarding data packets and making routing decisions. Ultimately, the WMN connects to an Internet gateway in using a multi-hop scheme. WMNs are attractive alternatives because the technology is scalable, reliable, and relatively inexpensive to implement. As requirements increase, WMNs can be iteratively grown with additional nodes and gateways to meet the needs of users.

While WMNs have their origins in ad hoc wireless networking, a bit of a distinction does exist between WMNs and ad hoc networks. As stated in [13], "The main difference between a WMN and an ad hoc network is perhaps the traffic pattern: in WMNs, practically all the traffic is either to or from a gateway; while in ad hoc networks, the traffic flows between arbitrary pairs of nodes."

Naturally, the minimalist approach to WMN implementation lends itself to military applications; especially in a maritime setting that lacks the infrastructure required for 802.11X Wi-Fi. For instance, operators can leverage WMN technology for reach-back during vessel boarding operations by simply deploying with lightweight and mobile WMN radios and devices. A backhaul path is necessary for desired reach back. In the WMN framework, it is simply a gateway and easily added to any WMN. Many options already provide this capability and are discussed in depth later. An instructive illustration of a basic mesh networks comes from Bosung et al. in [14].

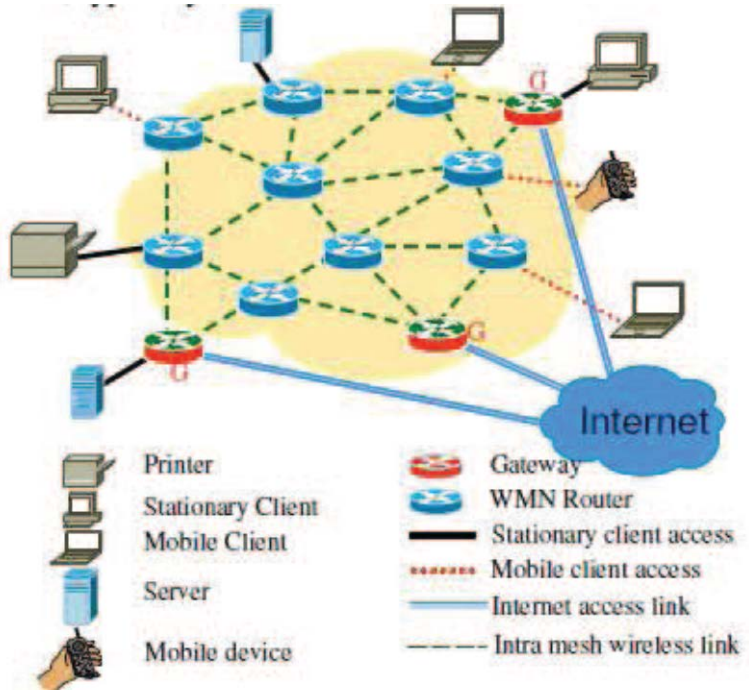


Figure 3. Typical WMN, from [14]

3. Mobile Ad Hoc Networks

MANET and WMN technology both stem from the original 802.11 standard, and not surprisingly, share many of the same qualities. However, the mobile nature of nodes on MANET systems creates a marked difference between common stationary WMNs and MANETs. MANETs are autonomous rapidly forming, self-healing, and self-organizing networks capable of dynamic routing and true peer-to-peer communication. According to the Internet engineering task force (IETF) request for comment (RFC) 2501, MANETs “have dynamic, sometimes rapidly-changing, random, multi-hop topologies which are likely composed of relatively bandwidth-constrained wireless links” [15].

Key distinctions about MANET are relevant in analyzing suitability for specific applications. As a subset of the broader concept of ad hoc networking, MANET is unique in that it is specifically deployed to allow constant communication between nodes on-the-move. As asserted by Orwat et al., MANETs must be capable of two vital functions to accomplish this type of communication, decision making and optimization. MANETs are formed by individual mobile nodes capable of making decisions about themselves, neighbor nodes, and the overall health and status of the network. Autonomous decision making compensates for the lack of traditional infrastructure. The decentralized decision making on a MANET absolutely depends on optimization. Nodes must be capable of making decisions based on optimality that protects and maintains the overall health of the network. Decision making and optimization is the key to the autonomous nature of MANETs. Nodes must be able to perform these vital operations to create a network capable of self-organizing and self-healing [16]. Figure 4 is a simple depiction of the ad hoc topology that characterized MANETs provided by Dean [17].

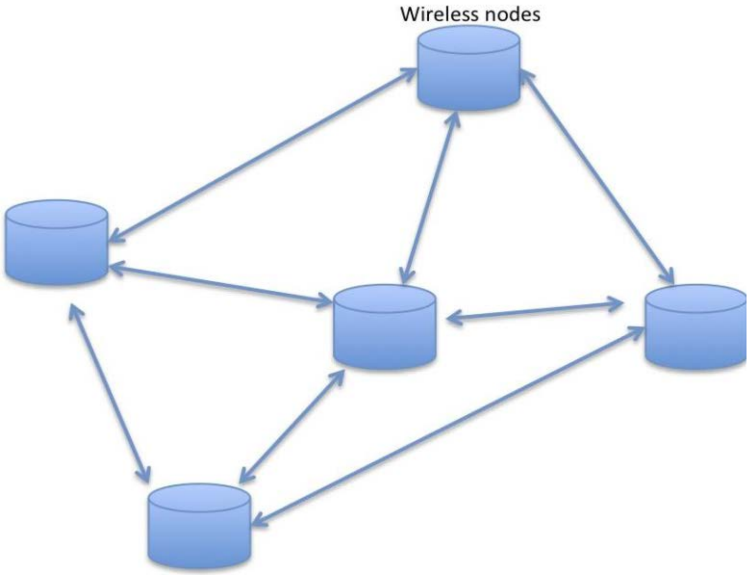


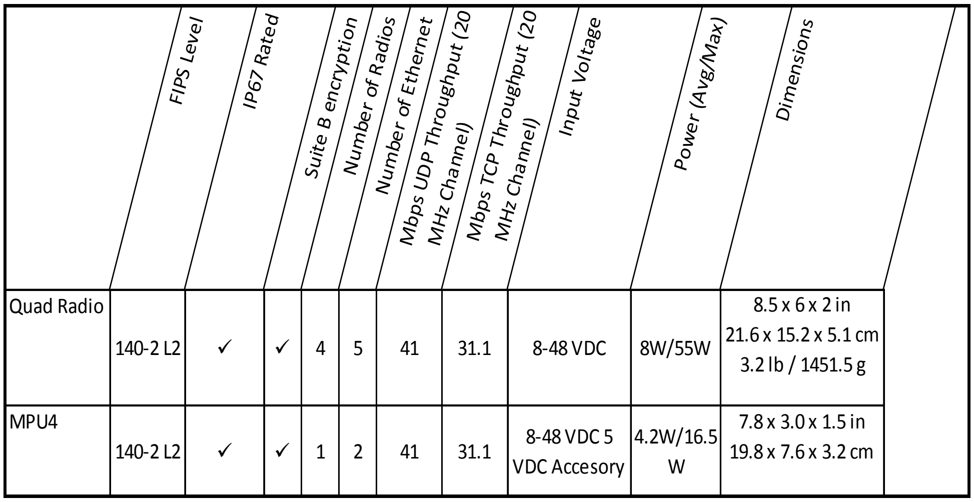
Figure 4. Simple Mesh Autonomous Behavior

MANET offers many benefits in an operational setting. Its decentralized nature, as well as its self-forming and dynamic routing capacities, reduces initial overhead and resource requirements. Fewer personnel are required to leverage MANET in forming rapidly deployable systems to support SA and data sharing between remote stations.

4. Wave Relay

WR™ radios are tactical radios designed and manufactured by Persistent Systems. WR radios are wireless OSI layer 2 devices designed to operate using proprietary onboard software, which is responsible for node decision making and network optimization. According to the manufacturer, the WR system was designed to “maintain connectivity among a large number of highly mobile nodes” [18].

CENETIX researchers currently have access to two WR radio models that are especially applicable to maritime operations, the WR quad radio router and the manned portable unit generation 4 (MPU4). Field experiments conducted during this research utilized both radios to form the MANETs for testing, which will be discussed later in the text. Figure 5 provides a comparison on the quad radio and MPU4 using data compiled from technical description documents [18]–[20].



	FIPS Level	IP67 Rated	Suite B encryption	Number of Radios	Number of Ethernet	Mbps UDP Throughput (20 MHz Channel)	Mbps TCP Throughput (20 MHz Channel)	Input Voltage	Power (Avg/Max)	Dimensions	
Quad Radio	140-2 L2	✓	✓	4	5	41	31.1	8-48 VDC	8W/55W	8.5 x 6 x 2 in 21.6 x 15.2 x 5.1 cm 3.2 lb / 1451.5 g	
MPU4	140-2 L2	✓	✓	1	2	41	31.1	8-48 VDC 5 VDC Accesory	4.2W/16.5 W	7.8 x 3.0 x 1.5 in 19.8 x 7.6 x 3.2 cm	

Figure 5. Quad Radio and MPU4 Specification Comparison, from [18]–[20]

In maritime experiment sites, the larger size and greater power of the quad radios are suitable for fixed mounting on large and small vessels, while the smaller and less powerful MPU4s provide mobile communications and network connectivity to boarding team members stationed on each vessel.

According to Persistent Systems, both radios:

> can be configured to function as an 802.11 access point. Standard clients such as laptops with built in 802.11 cards may access this system…For maximum performance, always disable the 802.11 AP unless it is required. To use a radio as a 802.11 Access Point, the radio must be set to a valid 802.11 frequency and the channel width must be set to 20 MHZ. [20]

Despite WR's 802.11 WAP capability, Persistent Systems does not recommend using Wi-Fi. The company recommends operating the WR radios in the proprietary MANET manner whenever possible. According to Persistent Systems Founder and CEO Herb Rubens,

> Connecting via Ethernet is absolutely the most efficient and secure means. WiFi wastes the spectrum on transmissions to your device which could have otherwise been used to support the network as a whole. The WiFi is also less secure. Our Fips 140-2 level 2 is for the MANET side, not the wifi side. We don't have control over how security is implemented in the WiFi client of the SEEK device so we can't certify that. [21]

Accordingly, CENETIX researchers have operated the WR radio according to the manufacturer's recommendations, and have always leveraged the WR MANET for data sharing over the CENETIX tactical network. Security is specifically addressed later in this chapter.

I. CENETIX BIOMETRICS DATA SHARING FRAMEWORK

CENETIX researchers collaborate with USCG, United States Navy (USN), San Francisco law enforcement, SOCOM, and a host of DOD and international partners on a variety of maritime field experiments. The CENETIX team partners with TRADOC capability manager biometrics and forensics team (TCM-BF) and USSOCOM to conduct biometrics training. TCM-BF provides field tested and authorized biometric sensors to CENETIX researchers. USSOCOM supports CENETIX research with training and by providing access to authoritative biometric databases for testing.

Operators need three basic system requirements to obtain NRT analysis of biometric data collected in remote locations: (1) a device capable of collecting high-quality and properly formatted biometric data, (2) a connected network capable of two-way real-time communication with an authoritative biometric database, and (3) an authoritative biometric database.

The network requirement can be broken into two sub-requirements. Operators require a tactical network on the *boarded vessel* to provide communication and data sharing onboard amongst the team. For the purposes of the thesis, it is referred to as the tactical wireless network, or specifically as the WR MANET. To provide "last mile" communications, some form of wireless reach back network (WRN) is required. Both these network requirements are discussed in this chapter.

For research and experimentation purposes, SEEK II serves as the biometric collection device; WR MANET serves as the tactical network; WRN is achieved using USCG satellite communications (SATCOM) during field experiments, and the identity operations SOFEX training portal serves as an authoritative database.

Several alternative technologies exist to provide WRN and are examined in this chapter. Additionally, because SEEK II maintains the BEWL as an alternative to ABIS, a description of BEWL operation and procedures is included in this chapter.

1. SEEK II

The SEEK II is a mobile multi-modal biometrics collection device produced by Crossmatch Industries. While this thesis does not endorse specific vendors, the SEEK II is available to CENETIX researchers and authorized for biometric data transfer by the DOD. Army personnel at TCM-BF provide SEEK II devices and training to CENETIX researchers. The device captures and formats standards-based fingerprints, and iris and facial images, which conform to the DOD's electronic biometric transmission specification (EBTS). This specification describes customizations of FBI electronic fingerprint transmission specification (EFTS) transactions, which are required to interface with the DOD ABIS. The SEEK II allows operators to create fingerprint, iris, and facial-based biometric records and enroll those records in the ABIS system or to the locally stored BEWL [22].

The biometric scanner unit consists of two-finger optical fingerprint plates and dual iris scan and facial image sensor camera. It has two USB 2.0 host connections and one Ethernet port. SEEK devices currently operate on Microsoft Windows XP SP3 and the 32 bit version of Windows 7. Onboard memory is capped at two gigabytes of dynamic random access memory (DRAM), and the removable hard disk drive (HDD) has a capacity of 64 gigabytes. Although SEEK II is not currently authorized to operate wirelessly under its authority to operate (ATO) [23], SEEK II supports 802.11 b or g wireless, and supports 802.11 Bluetooth as well. Additionally, the device has embedded Global Positioning System (GPS) technology and supports 3G connectivity, which expands its operational versatility.

The device is significantly ruggedized to support tactical use. The dual batteries are hot swappable. The touchscreen display and keyboard are damage resistant and designed for visibility during bright daylight and dark conditions. The onboard microphone performs noise canceling for voice capture. It is capable of storing an on-board BEWL of up to 120,000 enrollments, which can be queried by the user to provide match-no match responses for new enrollments [24].

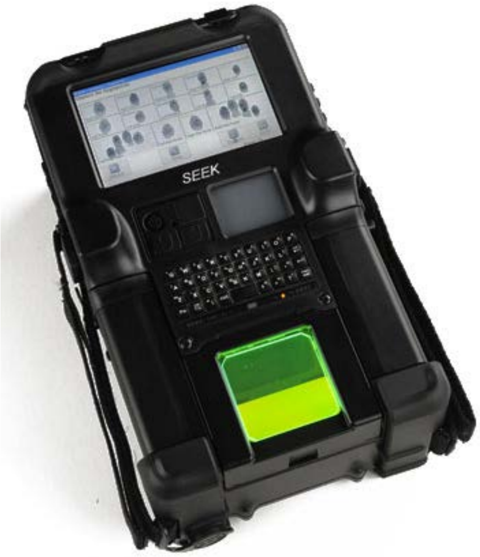


Figure 6. SEEK II by Crossmatch Technologies, from [24]

2. Tactical Network and WRN

As discussed earlier, the WR Quad and MPU4 radios operate as Layer 2 MANET, and form the core of the CENETIX tactical wireless network during field experiments. WR utilizes its proprietary routing algorithms to provide wireless connectivity between other WR nodes on the tactical network. WR nodes provide tactical network connectivity to the SEEK II via a direct Ethernet connection or by providing an 802.11 WAP [18], [19]. All communication and data sharing occurring on the *boarded vessel* happens over the WR MANET.

The WRN is responsible for reach back, or connectivity beyond the *boarded vessel* that is sometimes referred to as "last mile" communications. WRN can be provided many ways. Some examples are:

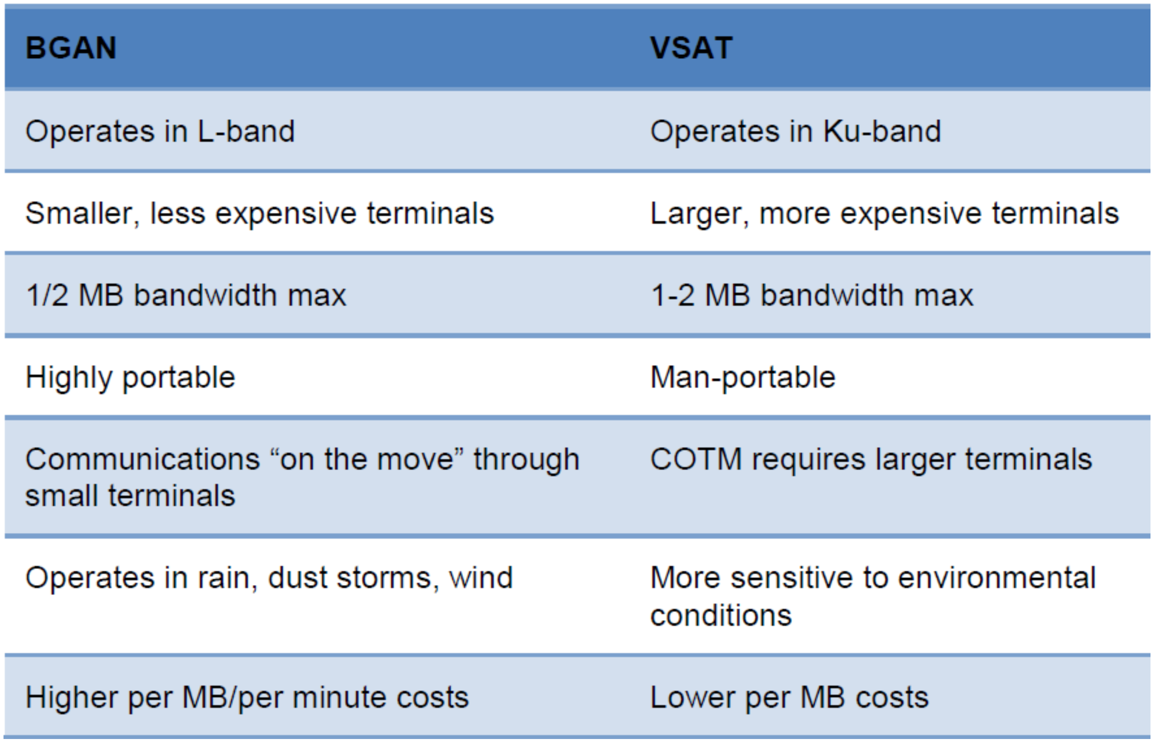
a. Shipboard SATCOM

In a typical VBSS scenario, the boarding team is launched from a larger naval vessel that encompasses organic SATCOM resources. For example, the vast majority of U.S. Navy vessels are equipped with an automated digital network system (ADNS), and a shipboard router that can route data over the several different SATCOM paths. ADNS Increment III, and newer, allows units to transport data over commercial broadband satellite program (CBSP) SATCOM 1 or defense satellite communications (DSCS) SATCOM. Data is transferred from the ADNS router, through the space segment, to Navy teleport sites [25]. These sites function as Internet service providers (ISP) and can provide access to the Internet. Connecting the tactical MANET to ADNS for WRN provides access to the identity operations SOFEX portal or to the DOD ABIS portal. In MIO related VBSS missions, shipboard SATCOM is the most common form of reach back, and most desirable due to its speed and reliability. As with any DOD information system, information assurance can be a concern. Connecting to a DOD ADNS router requires appropriate authority to connect and operate.

b. *Commercial off-the-Shelf Global Satellite*

Commercial-off-the-shelf (COTS) Global Satellite products are available to provide remote operators to SATCOM without access to traditional SATCOM. Two products, in particular, have been used in previous CENETIX testing and are suitable for MIO and VBSS applications. A broadband global area network (BGAN) terminal is a satellite earth terminal manufactured and operated by Inmarsat. Additionally, very-small-aperture terminals (VSAT) are available from multiple vendors and service providers [26]. Generally speaking, BGAN is lightweight and more mobile than VSAT but offers lower bandwidth.

BGAN and VSAT both provide sufficient bandwidth to support biometric data sharing in MIO. Ultimately, the choice is between the greater mobility of BGAN and the superior bandwidth offered by VSAT. As stated by Antillon in [27], both products depend on line of sight (LOS), which should be considered when operators determine their location on the *boarded vessel*. Antillon provides a good comparison between VSAT and BGAN specifications in his work on hastily formed networks in [27].



BGAN	VSAT
Operates in L-band	Operates in Ku-band
Smaller, less expensive terminals	Larger, more expensive terminals
1/2 MB bandwidth max	1-2 MB bandwidth max
Highly portable	Man-portable
Communications “on the move” through small terminals	COTM requires larger terminals
Operates in rain, dust storms, wind	More sensitive to environmental conditions
Higher per MB/per minute costs	Lower per MB costs

Figure 7. BGAN versus VSAT, from [27]

c. 3G/4G

In recent CENETIX experiments, 3G and 4G cellular networks have proven successful in providing reach back to the CENETIX Command and Control Center in Monterey, CA. Bordetsky explains in [28] that in field experiments from 2008 and onward, CENETIX has successfully used 3G and 4G cellular service from various providers to provide redundancy to commercial and DOD SATCOM for MIO field experiments in San Francisco Bay and at international sites. Various forms of data collected during CENETIX RSE demonstrations has been shared successfully using 3G and 4G. These devices can provide a Wi-Fi hotspot or WAP to nodes on the tactical network. Obviously, MIO operators in remote locations typically cannot access commercial cellular services, but 3G and 4G technology can be feasible as a reach back tool in urban environments, such as major ports and harbors [29].

Using open or shared Internet from cellular service introduces security concerns. Virtual private networks (VPN) can be used to harden the reach back circuit and significantly counter cyber security risks to biometric data sharing. VPN integration to the WRN is addressed later in this chapter.

d. ISP

In some cases, direct access to an ISP is possible. During CENETIX field experiments in the San Francisco Bay, the USCG station on Yerba Buena Island provided access to the open Internet through a commercial ISP. Although not likely in most MIO or VBSS situations, like 3G and 4G, a commercial ISP may be an option in more urban environments. This option may also require the use of VPN to harden the WRN sufficiently.

3. DOD Automated Biometric Identification System

ABIS is a "generic term for any automated biometric identification system." [30] The DOD ABIS serves specific defense oriented biometric needs. Its original design was based on the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System. DOD ABIS encompasses and electronic database and all related applications and tools to provide storage, retrieval, and queries of fingerprints and other biometric data that has been collected on persons of interest to national security [30]. The current iteration of this system is labeled Next Generation NG-ABIS, but is still generally referred to as simply DOD ABIS. According to the U.S. Army's biometrics enabling capabilities (BEC) branch of program executive office (PEO) for enterprise information systems, in [31], DOD ABIS is:

> The central, authoritative, multi-modal biometric data repository. It is the enterprise-level authoritative data source for DOD biometrics. NG-ABIS expands capabilities with multi-modal (fingerprint, palm, iris, face) storage and matching, watch list capability, and improved integration with interagency repositories. It is based on adaptations of COTS products, using open architecture to minimize development and speed deployment. The system takes advantage of low-risk, cost-effective blade hardware to optimize system availability and scalability, and ensure continuity of operations. NG-ABIS interfaces with numerous DOD and interagency biometrics systems, including the FBI Integrated Automated Fingerprint Identification System (IAFIS), and the Department of Homeland Security IDENT System, storing and matching biometric data on persons of interest to DOD.

According to [32], Version 1.2 of ABIS utilizes improved algorithms to reduce inconclusive returns and provide faster matching than previous iterations. It handles between 30,000 and 45,000 transactions per day and provides continuous BEWL availability to DOD customers. ABIS storage capacity is currently 18 million records, and is scalable to 48 million records. It has a robust and comprehensive continuity of operation plan (COOP) that includes a fully capable master recovery system.

Biometric files interfacing with DOD ABIS must be compliant with DOD electronic biometric transmission specification (EBTS) version 3.0. Earlier versions of this standard focused primarily on fingerprints, but the expanding role of biometrics in a broader range of DOD operations required greater biometric capabilities. EBTS v2 and EBTS v3 greatly increased the scope of the EBTS standard to include search ability for iris scan and facial recognition images, as well as DNA samples [28].

Operators can connect to ABIS through an existing web portal. The SEEK II is authorized to access ABIS via hypertext transfer protocol (HTTP) or secure HTTP (HTTPS) [33]. Currently, operating operator queries to the DOD ABIS are prioritized into four categories determined by the operational mode summary and mission profile.[1] Priority one is highest and carries a maximum response time of 15 minutes. Category two receives responses within 30 minutes; category 3 within 60 minutes; and category 4 within four hours [33].

[1] According the Army Capabilities Integration Center (ARCIC), An operational mode summary/mission profile (OMS/MP) is a time-phased representation of planned operations at the tasks, conditions, and standards level across the range of military operations. The regulation governing development of OMS/MPs is TRADOC Regulation 71-20, *Concept Development, Capabilities Determination, and Capabilities Integration*." In the context of biometric operations, the OMS/MP of an organization conducting biometric operations determines their priority to the DoD ABIS. Generally, priority 1 is reserved for special operations missions. Depending on the mission, MIO could fall into any of the four priorities. Advertised times for each priority level is maximum. Available at https://acc.dau.mil/adl/en-US/690239/file/75488/USA%20-%20Guidebook%20-%20OMS%20_%20MP%20Development,%2030%20Sep%202013.pdf.

4. Biometrically Enabled Watch List

The term biometrically enabled watch list (BEWL) refers to any list of persons of national interest (POI) that identifies those persons with biometric characteristics [30]. In addition to providing a true biometric identity for POIs, the BEWL also describes known dispositions or assessments on POI status, which aide decision makers in determining appropriate actions for operators interacting with these individuals. A comprehensive DOD BEWL exists within the larger DOD ABIS, but it is too large to be held on existing mobile devices like the SEEK II. This storage limitation is resolved by the creation of smaller BEWLs tailored to AOR or mission specific requirements. These smaller BEWLs can be loaded onto biometric devices to provide immediate responses for operators engaged in MIO or in ground-based identification and verification operations [33]. For example, the Global War on Terror resulted in an incredible dependence on the DOD's Afghanistan BEWL, which contains only roughly 0.5% of the biometric enrollments of the larger DOD ABIS [34].

5. ABIS versus BEWL

As previously stated, the SEEK II is capable of maintaining an integrated BEWL with up to 120,000 enrollments (250,000 in newer models of the same device). Obviously, this number is far smaller than the much larger authoritative DOD ABIS database, and can result in less accurate information on the tactical edge for operators and decision makers. However, because the BEWL is stored on the SEEK II device, biometric responses are immediate.

The convenience of a locally stored BEWL on SEEK II offers obvious benefits to timeliness. However, BEWL creation, promulgation, and updating occur periodically, which creates a potential for diminished relevance and accuracy of biometric data available to operators. According to tactics, techniques, and procedures (TTP) in [33], commanders of units conducting biometric operations are encouraged to ensure BEWL updates are checked daily, but the minimum requirement for BEWL updates is weekly.

Considering the significant number of systems feeding the DOD ABIS and the sheer volume of available biometric data, even a 24-hour lapse in synchronization (between local BEWL and DOD ABIS) could have a negative impact on the quality of biometric data. For example, a biometric enrollment from Afghanistan could be of importance to a biometric search being conducted in another AOR within the recommended 24-hour update period. Clearly, even this daily update could miss important information in the new enrollment. If only the weekly updates are performed, the data synchronization problem is exacerbated. Moreover, these problems are evident in the best-case scenario, where operators have consistent access to biometric repositories. Deployed operators may be forced to extend beyond weekly updates in some operational environments.

Fortunately, available technology is capable of addressing this issue. The multi-modal SEEK II provides ample biometric collection capability; supporting fingerprints, facial recognition, and iris scanning, which are all supported by DOD ABIS and the DOD EBTS standard. More to the point, the SEEK II already includes multiple interfaces that support network connectivity, including, USB, Ethernet, Bluetooth, and Wi-Fi, which could be used at the tactical edge to achieve NRT biometric responses. However, these capabilities often go unused. Remote operators can lack on-site connectivity, which requires them to rely solely on the local BEWL. In the case of wireless reach back, the current ATO approves only wired Ethernet connections.

J. SECURITY

Cyber security is of particular concern during data sharing in identification and verification operations. Biometric data are generally considered unclassified but sensitive that require the protection for confidentiality and integrity of the data. However, wireless networks, such as those deployed by CENETIX, automatically accept certain risks associated with wireless operation. The two proposed wireless models operate in different ways and include their own specific security implications. The primary cyber security concern for the tactical network is the manner in which each model handles the security of data-in-transit between the SEEK II device and the WR MANET. WR encryption throughout the MANET complies with federal information processing standard (FIPS)

140-2. Wireless operation between the SEEK II and the WR WAP relies on non-proprietary encryption schemes [3], [36].

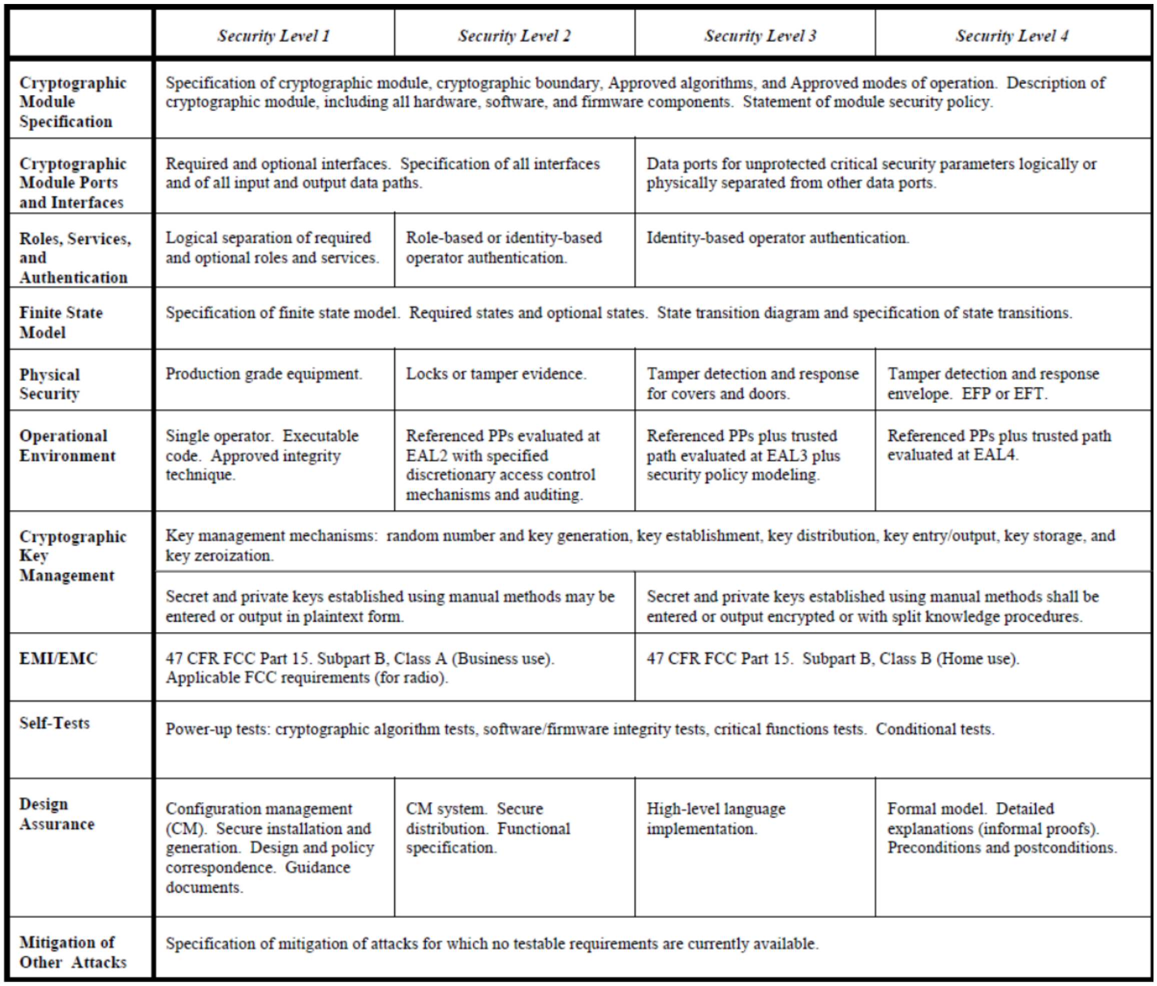
1. FIPS 140-2 Security Requirements for Cryptographic Modules

Cryptographic products that operate in a sensitive but unclassified environment must meet the specifications listed in FIPS 140-2. This federal standard is based on the broader National Institute of Standards and Technology FIPS 140 standard. FIPS 140-2 outlines requirements and standards for cryptographic modules, including hardware and software components, to maintain the confidentiality and integrity of information, which is processed by the cryptographic module.

FIPS 140-2 defines four security levels—level 1 through level 4. Level one offers the lowest level of security and level four offers the highest. The requirements for each level address areas of concern for design and implementation of cryptographic functions within the module. The areas of concern include:

> Cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. [36]

Figure 8 provides a summary of the requirements for each of the four security levels specified by FIPS 140-2.



	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Figure 8. Summary of FIPS 104-2 Security Requirements by Level, from [36]

2. Wave Relay FIPS 140-2 Compliance

Throughout this research related field experiments, WR radios have been used to transmit data wirelessly on the tactical network in two ways, the proprietary WR MANET and 802.11 Wi-Fi. Wireless MANET operation is FIPS 140-2 compliant. As stated previously, 802.11 Wi-Fi operation on WR radios is not FIPS 140-2 approved.

a. Wave Relay MANET FIPS 140-2 Compliance

WR radios—quad radios and MPUs—are validated by the governments of the United States and Canada as compliant with FIPS 140-2. The radio's encryption scheme relies on National Security Agency approved Suite B algorithms, specifically, counter mode advanced encryption standard (AES) encryption with a secure hash algorithm 2

(SHA-2) 512 bit hash-based message authentication code (CTR-AES-256 HMAC-SHA-512). The non-proprietary security policy, which is kept on file by NIST.gov, states that in addition to CTR mode, WR can also use CBC and GCM modes. While Persistent Systems defaults to a 256-bit key, WR radios can also use 128 and 192 bit keys for encryption and decryption of network traffic [36].

In addition to the security provided by FIPS Level 1 requirements, FIPS Level 2 provides additional physical security by requiring tamper-proof evidence on the cryptographic module itself or its container to protect the module's plaintext cryptographic keys, as well as the critical security parameters. WR's ruggedized form factor meets this requirement. Level 2 also requires role-based authentication for operators on the cryptographic module [35]. According to [36], WR meets this specification by implementing web browser access to module management functions over HTTP/TLS. The interface supports three roles: crypto officer, network management, and user. Roles are authorized to execute appropriate functions IAW with FIPS 140-2. In this way, FIPS 140-2 accreditation allows WR MANETs to implement the cyber security concepts of "least privilege" and "separation of duties."

However, the FIPS 140-2 accreditation for WR only applies to the cryptographic boundary for each radio. In [36], Persistent Systems defines those boundaries:

> For the MPU3S, MPU3D, MPU4, and QRS, the physical cryptographic boundary is defined as the module case, which includes the Wave Relay main board, including the hardware cryptographic accelerator chip, drivers, CPU, and on‑board flash memory. The boundary does not include any port caps.

According to the manufacturer, the 802.11 WAP is available during the FIPS mode of operation, but the WAP and the device accessing the WAP is not FIPS 140-2 compliant [36]. In other words, only MANET operation of the WR tactical network is FIPS 140-2 compliant.

b. Cipher WR 802.11 WAP FIPS 140-2 Compliance

WR quad radios and MPU4 utilize only Wi-Fi protected access 2-pre-shared key (WPA2-PSK) for securing their WAP. The radios use AES-128 with cipher block chaining, message authentication code (CBC-MAC)[36]. As stated earlier, encryption functions related to the 802.11 WAP fall outside of the cryptographic boundary of WR radios and are not FIPS 140-2 approved.

The Crossmatch SEEK II biometric device operates on Windows XP SP 3, which supports WPA-2-PSK, as does the SEEK II onboard wireless adapter [24]. The SEEK II can communicate wirelessly, at some level of security, with quad radio or MPU4 over the WAP. However, WR's FIPS 140-2 accreditation does not apply to this mode of operation [36].

3. VPN

As stated previously, commercial services can sometimes be leveraged to provide reach back from the tactical network to ABIS. Using open or public Internet can be convenient and efficient, but it places data in transit at risk, and makes it vulnerable to a host of cyber threats. A relatively simple countermeasure, which provides significant reduction in cyber threats, is a VPN.

Determining a specific definition for VPN can be difficult due to the range of diversity in capabilities by VPN manufacturers. Despite the many differences in commercial VPNs, some commonalities and core capabilities exist to help define VPN technology. Put simply, a VPN is an established connection over an existing public or shared network infrastructure that implements encryption and authentication technologies to secure payload data in transit between two nodes or endpoints not directly connected [37]. An effective VPN should execute cryptographic functions, such as encrypting, hashing, shared keys, and digital certificates, to protect against cyber threats, such as eavesdropping, packet tampering, man-in-the-middle attacks, and replay attacks [38]. Properly implemented, a VPN provides substantial protection to the confidentiality and integrity of data being shared between two points.

II. CENETIX EXPERIMENTS IN A MIO SETTING

To maximize operational benefits from wireless biometric data sharing and reach back over the CENETIX tactical network, efforts were made to measure baseline performance of the network, identify network inefficiencies, and develop recommendations for network optimization. For the purposes of this thesis, optimization efforts addressed two areas of the CENETIX network, the WR MANET itself and the integration of wireless operation of the SEEK II on the MANET.

As previously stated in Chapter II, WR tactical radios form the MANET portion of the tactical network. Baseline performance data is difficult to ascertain due to the dynamic (on a per-packet, sub second basis) and self-forming nature of MANETs. The proprietary nature of the WR routing algorithm is another challenge in accurately predicting tactical network behavior. Despite these challenges, many characteristics of the network and its components offer measurable data and clearly stated specifications, which can be used to form evidence-based recommendations for optimizing the tactical network.

This chapter provides the details of two experiments. The first experiment addressed the optimization of the CENETIX wireless MANET for MIO scenarios in the San Francisco Bay. The second experiment used outcomes from the first experiment to improve MANET performance in preparation for wireless integration of the SEEK II biometric device. During the second experiment, the improved CENETIX wireless MANET was used to conduct biometric data sharing using two models of wireless operation. Data was collected on the performance of both models to inform a comparative analysis and determine the most optimal model of the SEEK II wireless operation.

A. NPS MIO WMD ISR EXPERIMENT, AUGUST 2014: OPTIMIZING THE WAVE RELAY MANET

In August 2014, CENETIX researchers joined with USCG boarding teams, as well as USCG Research & Development Center in Alameda, California to conduct the Semi-Annual Tactical Network Test Bed, Weapons of Mass Destruction: Intelligence Surveillance And Reconnaissance (TNT WMD ISR) event. Researchers intended to demonstrate and measure capabilities of the CENETIX tactical network, as well as a range of sensors and emerging peripheral technologies, within a MIO setting.

Key portions of the MIO experiment occurred onboard the vessel GTS Adm. Callaghan (AK-1001), which served as the experiment's *boarded vessel*. Testing focused on boarding team communication over the tactical network, as well as reach back to remote C2 stations. For the purposes of this experiment, a communications station located on Yerba Buena Island (YBI) operated as a remote C2 station. Small USCG Auxiliary and San Francisco police department (SFPD) vessels served as relay nodes between the *boarded vessel* and C2 station on YBI. Boarding team members were equipped with WR and TrellisWare mobile tactical radios during common boarding operations, such as sensitive site exploitation (SSE) and RSE. All stations (vessels and YBI) were equipped with a WR quad radio operating on the 5.8 GHz band.

Boarding team communication within internal compartments on the *boarded vessel* occurred over TrellisWare radios. Previous testing, as well as indications in the set-up phase of this scenario, indicated the lower frequency TrellisWare radios performed better inside of the "skin of the ship." WR radios on the exterior of the ship were utilized for exterior boarding team communication and reach back or "last mile" communication to the remote station at YBI. Ongoing CENETIX research efforts regarding the wireless transfer of biometric data to remote C2 cells rely on efficient and reliable "last mile" communications. Therefore, optimization of the "topside" WR MANET is a key concern. Baselining this network, and efforts to approach optimal performance of the wireless MANET, were intended to assist in best implementing the CENETIX tactical network in future field experiments for wirelessly sharing biometric data.

CENETIX researchers and members of the USCG Research and Development Center were asked to monitor, capture, and analyze network performance, which included physical site survey, throughput measurement using the Solar Winds software, and monitoring the WR network management interface. Observations and data collection from this experiment informed some basic hardware, setup, and configuration requirements for CENETIX researchers in later experiments dedicated to wirelessly sharing biometric data. Feedback and analysis was provided by all team members in the form of after action reports (AAR). Feedback was compiled and analyzed at the CENETIX laboratory in Monterey to conduct a comprehensive analysis on MANET performance. Researchers consistently observed inefficiencies as a result of antenna selection and radio configuration and characteristics.

1. Antenna Selection

WR quad radios, located on each vessel, utilized a 360° Sector Array (operating as omnidirectional) antenna, with an 8 dBi gain (standard Persistent Systems WR model). Locations of quad radio relay nodes on small vessels were effectively static throughout the experiment. Intermittent connectivity and inadequate data rates indicated that link quality was poor throughout the MIO boarding scenario, which reduced the operators' and researchers' ability to transmit data over the network. Specifically, link outages and suboptimal data rates (below 1 Mbps) prevented operators from efficiently transmitting data over the network [39].

Based on the static nature of the relay vessels, USCG Research & Development Center feedback recommended implementing a higher gain directional antenna on the *boarded vessel* and training it on the relatively static nearest afloat relay node. This relatively simple, but significant, modification would better suit CENETIX research for the specific MIO application. By increasing directivity, it is possible to concentrate the signal on the approximate location of relay node. Moreover, increasing the gain (measured in dBi or decibel isotropic), the reception cone is narrowed and the effective range of the antenna is increased and signal quality is improved.

In addressing the range issue between afloat nodes, the “6 dB rule” is a good rule of thumb in planning future experiments. As explained by M. F. Young in his contribution to the FCC outreach program [40], “every time you double (or halve) the distance from the transmitter to the receiver, the signal level is lowered (or increased) by 6 dB.” Additionally, narrowing the cone beam from the antenna decreases interference, which reduces noise to improve link quality. Thus, simply selecting a higher gain directional antenna can significantly increase the effective range from the *boarded vessel* and result in substantial improvements to the signal to noise ratio (SNR). Chapter IV includes further analysis of these concepts.

CENETIX researchers agreed with this assessment. As a result, students planned to test static directional antennas in future experiments, and intended to optimize antenna selection for MIO scenarios similar to those conducted in the San Francisco Bay. Moreover, this observation correlates with Bordetsky’s and Bourakav’s research regarding network on target (NoT), which proved the effectiveness of antenna directivity in self-aligning orthogonal frequency division multiplexing (SAOFDM) in providing a ship-to-shore tactical link capable of providing up to 5 Mbps throughput in similar MIO conditions [29].

To note some distinctions, that tactical link utilized radios operating at 900 MHz, and the directionality of the antennae was an automatic function of the selected algorithm. However, the research does indicate that tactical network performance can be improved using directional antennae. Furthermore, it shows that speeds of up to 5 Mbps are possible in a virtually identical maritime setting. Data rates during the August CENETIX experiment did not exceed 2.58 Mbps. SNR on the tactical link remained at approximately 39 dB. Increased noise and interference, as a result of the suboptimal antenna selection, likely prevented the tactical network from achieving higher data rates [39].

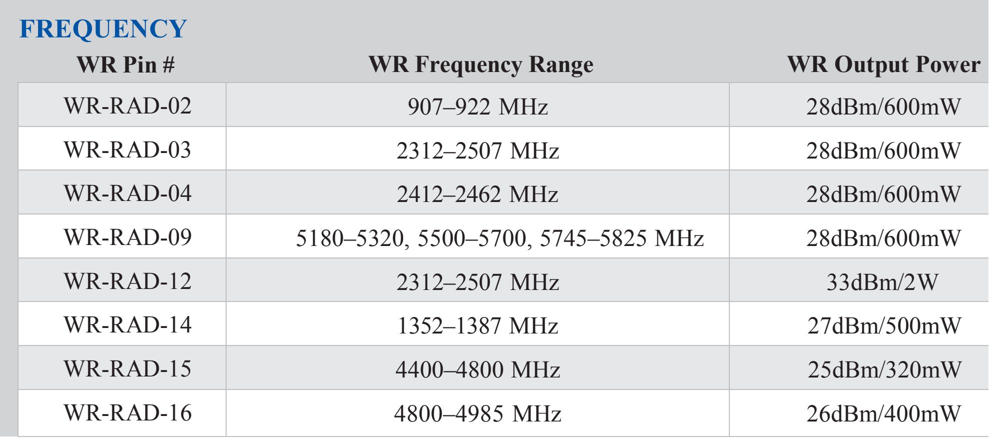
2. Radio Selection

WR MPU4 radios come from the manufacturer with specific frequency and power capabilities. WR-RAD-03 radios selected for this experiment operated in the 2312-2507 MHz frequency range at 600 mW output power. This selection was suboptimal for the following two reasons.

First, as evidenced by Adnen in [41], lower frequency radios suffer less loss due to attenuation, and typically perform better than higher frequency radios in shipboard settings. The lower frequency signal more successfully penetrates ship bulkheads and provides greater resilience to varying maritime environmental conditions. CENETIX researchers discovered in this same experiment that the TrellisWare tactical radios outperformed the WR radios, especially inside the skin of the ship. The TrellisWare radios were operating in the 1410–1460 MHz frequency range, and proved to be more capable of transmitting through bulkheads onboard the *boarded vessel*. The benefits of lower frequency were also evident on the exterior portions of the ship where superstructure and other components of the vessel existed as barriers to line of site. Persistent Systems currently produces suitable WR tactical radios capable of operating at a lower frequency, which should be more resilient to the problems of signal absorption, dispersion, and interference common in a shipboard environment.

Secondly, as evidenced by Zhang in [42], the maximum output power for the WR-RAD-03 for is 600 mW. Generally, it is understood that increased power can increase range. In the context of the WR MANET, it should be noted that optimal power settings on a per-packet basis is desirable. Presumably, it is a function of the proprietary WR onboard software. For the purposes of this experiment, it is accepted that increasing the maximum available output power only increases the network's ability to maximize throughput. WR offers radios capable of 2 W maximum output power. However, at present, the 2 W variant of the MPU4 operates at the same frequency range of the WR-RAD-03 (2312–2507 MHz). Persistent Systems provides Table 2, which illustrates radio output power specifications [19]. While the MPU4 offered superior performance outside the skin of the ship, an optimal radio selection should consider frequency and power in the context of the specific application. Optimal radio choice should provide a range of frequency and power settings to meet specific operational requirements and environmental realities. In this case, it would be desirable to select a radio that performs well inside the skin of the ship and externally.

Table 2. Wave Relay Frequency and Range Specifications, from [19]



FREQUENCY

WR Pin #	WR Frequency Range	WR Output Power
WR-RAD-02	907–922 MHz	28dBm/600mW
WR-RAD-03	2312–2507 MHz	28dBm/600mW
WR-RAD-04	2412–2462 MHz	28dBm/600mW
WR-RAD-09	5180–5320, 5500–5700, 5745–5825 MHz	28dBm/600mW
WR-RAD-12	2312–2507 MHz	33dBm/2W
WR-RAD-14	1352–1387 MHz	27dBm/500mW
WR-RAD-15	4400–4800 MHz	25dBm/320mW
WR-RAD-16	4800–4985 MHz	26dBm/400mW

Additionally, the quad radio is capable of operating in 5.8 GHz or 2.4 GHz bands. Although the 5.8 GHz band was suitable for this field experiment, the option provides optimization choices under different circumstances.

3. Channel Bandwidth

WR quad radios can be configured for channel widths of 5 MHz, 10 MHz, 20 MHz, or 40 MHz [18], [19]. MPU4 radios do not support 40 MHz channel width. As a result, the 20 MHz channel width selection was in place throughout the August MIO experiment. Using the 20 MHz channel width setting, researchers expected to maximize data rates over the tactical network. However, the 20 MHz setting introduces a greater opportunity for noise on the channel, which can result in a decreased SNR and negatively impact receiver sensitivity. Increased noise on the channel may also increase the error rate on the network, which reduces the overall success of packet transmission and degrades link quality. Network latency and reduced data rates observed during the August MIO experiment may have been, in part, due to the 20 MHz bandwidth setting. If the network is otherwise optimized, lowering the channel width setting is one way to lower error rate and improve link quality. Additionally, reducing the WR channel width setting to 10 Mhz or 5 Mhz effectively reduces the noise on the channel without reducing signal strength. The tradeoff decision between the higher data rate of the 20 MHz channel width or the improved link quality of 5 or 10 MHz channel width setting must also consider environmental factors and operational objectives. In this particular case, reducing the channel width to improve link quality may have been prudent.

Optimization of "last mile" communications via the WR MANET tactical network is crucial to providing operational value to personnel engaged in MIO and executing biometric identification operations. Key considerations for optimizing the tactical network should be increased range, reduced latency, minimized error rate, and sufficient throughput or data rates. Based on evidence and observations resulting from the August TNT WMD ISR event, CENETIX researchers recommended the following changes to the WR MANET.

- Implement directional high gain antennae on the boarding vessel.
- Select radios with sufficient output power. 2 Watt WR models are recommended.
- Select radios capable of lower frequency operation
- Select channel width setting lower than 20 MHz. 10 Mhz is recommended. (a constraint of the MPU4 capabilities, which requires that the 20 MHz channel width be selected to support 802.11 WAP)

B. NPS BIOMETRIC EXPERIMENT, OCTOBER 2014: CONDUCTING IDENTIFICATION OPERATIONS USING REACH BACK

On October 3, 2014, CENETIX researchers traveled to Alameda, California to conduct research onboard the Military Sealift Command vessel GTS Admiral W. M. Callaghan and at YBI. Building on previous CENETIX TNT research, students constructed a wireless MANET to test wireless reach-back capabilities for biometric data sharing.

Past CENETIX research had demonstrated the evolving and significant capabilities of wireless MANET in a maritime setting using WR and TrellisWare radios to provide SA, C2, and information sharing. In August 2014, the CENETIX team conducted a large-scale experiment in Alameda in cooperation with the USCG, Joint

Interagency Field Experimentation (JIFX), SFPD, and various other partners. The experiment focused on CBRN SSE, detection and reporting, and had great success in proving new applications of tactical wireless networks, networks on-the-move, unmanned ground vehicle (UGV) integration, submerged human diver networks, and a host of emerging technologies. Additionally, feedback from CENETIX students, the USCG Research and Development Center, and other research partners, provided recommendations for optimizing the tactical network for future MIO scenarios [39], [43].

During the August experiment, this research was focused on identifying methods to improve performance of WR MANET. Feedback from the August experiment provided researchers with recommendations for improving the tactical network. To the extent possible, those recommendations were followed during this experiment. However, the primary aim of this experiment was to conduct biometric data sharing wirelessly—using two proposed methods—and collecting data about network performance during wireless operation.

Accordingly, the scope of the experiment on October 3, 2014 was narrowly focused on biometric data sharing over the CENETIX tactical network. The specific goal was to transmit and receive biometric data wirelessly from the SEEK II through the WR MANET to the CENETIX server and the SOFEX Internet portal using two proposed wireless models: MPU4 as an 802.11 WAP, and MPU4 tethered via Ethernet to a SEEK II. The NPS server was used for data collection and collaboration, and the SOFEX portal provided NRT analysis and response for biometric data.

1. Concept of Operations

The following list outlines the CONOP for the CENETIX biometric reach back experiment.

- Rapidly deploy the MANET in a manner consistent with USN and USCG boarding team operations.
- Setup and configure two wireless models for SEEK II connectivity.
- Enable WAP on MPU4 and connect the SEEK II wirelessly to MPU4 WAP.

- Tether the SEEK II to the MPU4 with an Ethernet cable. (For this research, a tethered device allows operator mobility as one wireless device)

- Test connectivity to the CENETIX server.

- Test connectivity to the SOFEX biometric portal located at http://sofex.identityops.com/UserLogin.aspx?ReturnUrl=%2fdefault.aspx .

- Measure network performance using Solar Winds application to determine baseline.

- Apply antenna recommendations for network optimization from August 2014 TNT MIO experiment.

- Conduct mock RSE; specifically biometric data collection. Capture role-player mock biometric data including finger prints, iris scans, and facial recognition photos. (MOC training files)

- Enroll mock biometrics to the biometric application on the SEEK II.

- Send biometric data to the CENETIX server using both wireless models.

- Upload enrollments to the SOFEX portal for "match or no-match" using both wireless models.

- Collect data concerning network performance during the testing of both wireless models.

- Log activity throughout on the CENETIX server's observer's notepad.

2. Scenario and Network Design

The GTS Admiral W. M. Callaghan (Figure 9) platform was used to simulate a *boarded vessel*. Coast Guard facilities on YBI served as the remote C2 station, which provided ultimate reach back for the tactical network. The SFPD provided the patrol vessel MARINE 7, and the Coast Guard Auxiliary provided a small support vessel. These vessels served as afloat relays.

Figure 9. GTS Admiral W. M. Callaghan

The tactical network was constructed using a wireless MANET consisting of four WR quad radios and one MPU4. Additional devices were added as nodes including laptop computers and a SEEK II biometric collection device. The *boarded vessel* was outfitted with one WR quad radio, which was installed on the ship's superstructure, two decks above the main deck. A Windows laptop, including the Solar Winds application, was connected to the Quad Radio with a wired Ethernet connection for network performance monitoring. Additionally, one MPU4 was deployed onboard, and it connected wirelessly to the Quad Radio over the 2.4 GHz UHF band. The WAP was enabled on the MPU4 for 802.11 SEEK II Wi-Fi operations. Alternatively, the MPU4 provided tethered connectivity for the mobile SEEK II operation. The two relay vessels were also equipped with quad radios, and the C2 cell on YBI had an installed WR quad radio operating on the 5.8 GHz band.

At YBI, the CENETIX network connected to a router that supplied VPN access to the CENETIX server located in Monterey, California, or by way of a static route, to the Internet for accessing the SOFEX biometrics portal. The static route was an addition to previous iterations of the CENETIX tactical network. To address security, the CENETIX team implemented a VPN as the only option for remote access to the CENETIX server. In addition to added security for the CENETIX infrastructure, this modification also provides a useful simulation in connecting operators securely to a protected network. See Figure 10.

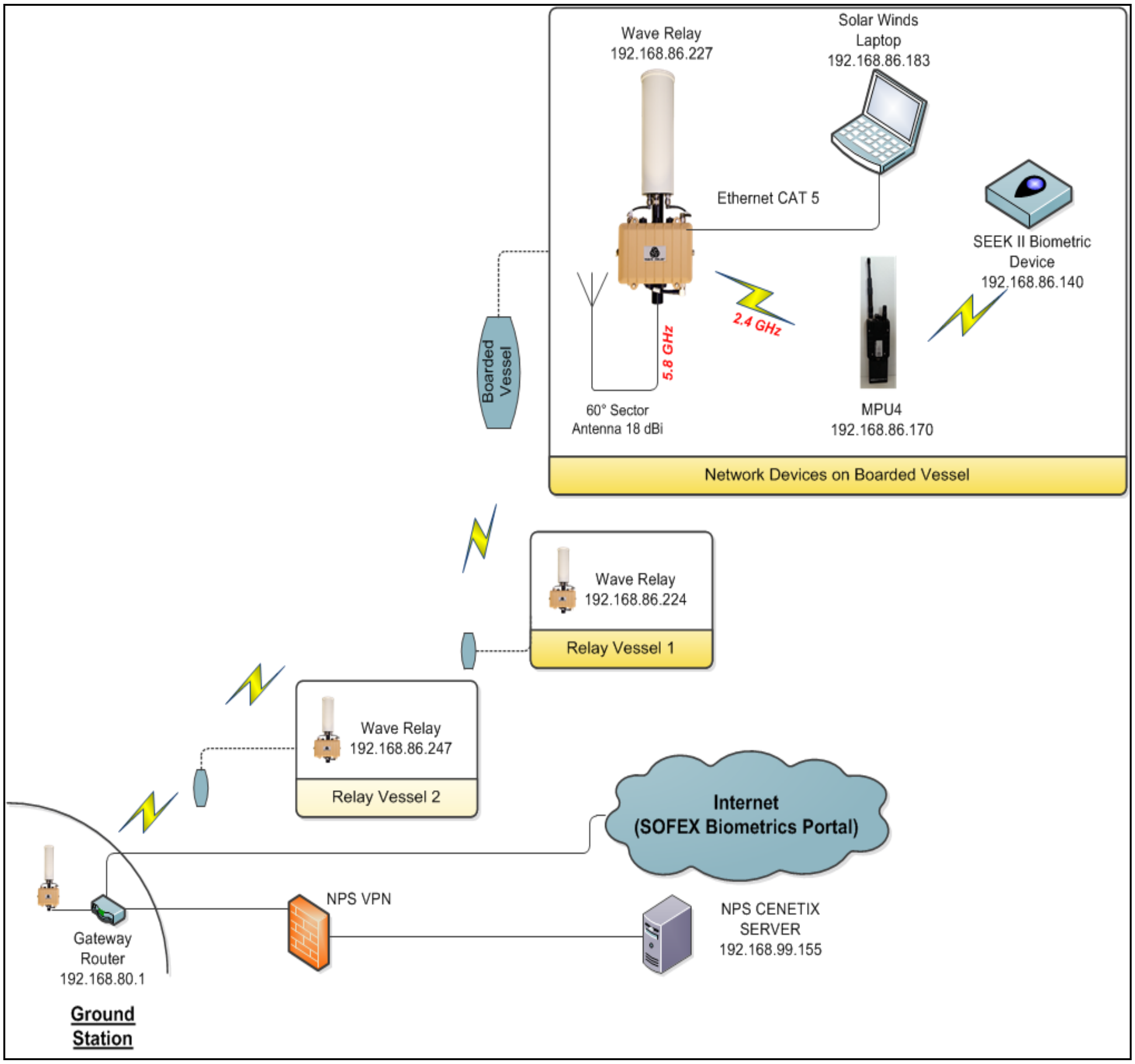


Figure 10. Experiment Network Diagram

3. Experiment Execution

The first task was network installation and configuration. All nodes were configured and tested successfully at the CENETIX lab in Monterey, California, but required on-site verification of network operation. The MANET operated properly immediately upon installation. To verify this operation, and determine baseline measurements, students conducted ping tests and sent data across the MANET. Measurements were conducted using Solar Winds and the Windows command prompt. Students on the *boarded vessel* used the SEEK II to collect biometrics including fingerprints, iris scans, and facial recognition photos.

Following system setup and baseline measurements, initial attempts to transfer biometric data wirelessly over the MANET and to the SOFEX Portal failed. Troubleshooting efforts suggested the SEEK II was the faulty component. Ultimately, the problem stemmed from default firewall settings within Microsoft Internet Explorer on the SEEK II. Students installed Mozilla Firefox web browser onsite, resolving connectivity failure between the SEEK II and the SOFEX Portal.

With the issue resolved, researchers on the *boarded vessel* contacted YBI-based CENETIX personnel to coordinate the biometric sharing phase of the experiment. During coordination, it became evident that network performance had degraded, despite the fact that the vessels remained in place and no changes had been made to the infrastructure. Earlier CENETIX experiments had experienced similar issues caused by inadequate range between quad radios (5.8 GHz band) on *boarded vessel* and relay nodes. Feedback from the August MIO experiment in Alameda, California suggested replacing all, or part of, the quad radio's standard omnidirectional antenna (3 X 120° sector 8 dBi) with a higher gain directional antenna [43].

One of three standard 120° sector antennas on the *boarded vessel*'s WR quad radio was replaced with a 60° 18 dBi directional antenna. The antenna selection was intended to increase gain and improve signal to noise ratio to improve the quality of the data link between the *boarded vessel* and the nearest afloat relay node. This change to the network resulted in a considerable increase in network performance, as indicated by

ICMP ping results between the Solar Winds laptop onboard Adm. Callaghan and the CENETIX server. These measurements are shown in Table 3.

Table 3. Antenna Selection Impact on Network Performance

	Baseline	**During Network Degradation**	**Post-install of 60° 18 dBi Sector Antenna**
Avg. Ping Sweep Range	20–35 ms	85–100 ms	5–15 ms
Throughput	2.53 Mbps	Not Measured	3.43 Mbps

After increasing the speed and reliability of the data link, CENETIX researchers once again began the biometric data sharing portion of the experiment. Researchers attempted to transmit biometrics to the SOFEX portal using the two wireless models described in this document’s concept of operations.

First, researchers enabled the 802.11 WAP on the MPU4 and selected the radio’s default 802.11 access point configurations. This selection forced the MPU4 to automatically select the operating frequency, and operate using the 20 MHz bandwidth (channel width). Using this model, researchers were able to access the CENETIX server and the SOFEX portal quickly. Researchers transmitted EFT and XML files, which contained full biometric enrollments for two role players, to both destinations. Placement of the files on the CENETIX server’s collaboration portal was instantaneous. The SOFEX portal received the biometric enrollments and returned a match/no-match response in under one minute. This response came in two forms, a viewable “green return” on the SOFEX web-based graphical user interface (GUI) and via a standard SMTP email to the account’s registered user. Using the Solar Winds laptop, researchers monitored network performance during enrollment and response. As shown in Table 4, ping sweep data and throughput measurements were comparable to baseline measurements. Measurements were taken with the SEEK II located at 25 ft. and 50 ft. from the WAP.

Next, researchers disabled the 802.11 WAP on the MPU4 and tethered the SEEK II directly to the MPU4 using a standard Ethernet cable produced by Persistent Systems. Similarly, researchers gained immediate access to the CENETIX server and the SOFEX portal. They executed the enrollment process again and monitored network performance. Match response time was virtually identical, and network performance metrics were similar to those collected during 802.11 Wi-Fi operation and baseline measurements.

Table 4. Network Performance during Biometric Operations

	802.11 Wi-Fi (25 ft)	**MPU4 Tether (25 ft)**	**802.11 Wi-Fi (50 ft)**	**MPU4 Tether (50 ft)**
Avg. Ping Sweep Range	10–20 ms	10–20 ms	10–20 ms	10–20 ms
Throughput	3.24 Mbps	3.37 Mbps	3.21 Mbps	3.37 Mbps

4. Experiment Observation and Conclusions

The eight significant takeaways from this experiment are listed as follows.

- Adding a WR 802.11 WAP to the standard WR MANET provided wireless connectivity to the SEEK II with sufficient data rates for transmitting biometric enrollments (XML or EFT files) to the authoritative SOFEX biometrics database and receiving NRT match/no-math response.

- SEEK II tethered easily to the WR MPU4 using a standard Ethernet cable, which provided a wireless reach back to the SOFEX biometrics database, with sufficient data rates for transmitting biometric enrollments (XML or EFT files) to the authoritative SOFEX biometrics database and receiving NRT match/no-math response.

- Both models provide mobility to MIO operators and support wireless reach back model for biometric data sharing.

- In this case, differences in network performance between the two proposed models were negligible. However, this experiment only implemented one node (the SEEK II) competing for 802.11 Wi-Fi resources provided by the MPU4 WAP. Researchers expect that multiple Wi-Fi devices connected to one MPU4 WAP would result in reduced data rates for those nodes as a result of shared access on a half-duplex Wi-Fi link.

- Testing showed that tethered operations were marginally faster. For example, after the addition of the of 60° 18 dBi Sector Antenna, baseline throughput of the WR MANET was 3.43 Mbps. When the SEEK II was added to the MANET as a tethered device, throughput was measured at 3.37 Mbps (with the SEEK II and MPU4 in various locations)—approximately a 1.8% reduction in data rate, when compared to baseline. When the SEEK II was added as an 802.11 Wi-Fi node using the MPU4 WAP, throughput was measured at 3.21 Mbps (with SEEK II located 50 ft. from WAP)—approximately a 6.4% reduction in data rate. As stated in the third conclusion, additional Wi-Fi nodes would increase demand on a single WAP, and could significantly increase this performance delta.

- The MPU4 802.11 WAP will only operate simultaneously with the WR 2.4 GHz band when configured to operate with the 20 MHz channel width. According to Herbert Rubens of Persistent Systems,

  > If the MPU4 is running on a 20 MHz ISM Band channel and a Wi-Fi access point is enabled, it can both run the access point and the MANET at the same time. It uses the AP as a wireless wire, meaning the behavior for the wireless client should be the same as a laptop connected to the MPU4 with an Ethernet cable. The 802.11 client should be able to talk to other devices and radios in the network and do everything you would expect it to do [21].

- The static route on the VPN router is a useful option for simultaneously providing reach back to protected networks and assets residing on the Internet.

- As mentioned previously, following the August CENETIX TNT MIO WMD ISR scenario, the USCG Research and Development Center and CENETIX made four recommendations to optimize the CENETIX tactical network. Only the antenna selection recommendation was implemented in this experiment. As previously mentioned, the addition of a 60° 18 dBi directional antenna resulted in measurable improvements in link quality and network performance. The remaining three recommendations were not possible in this experiment. Operating the 802.11 WAP on the WR MPU 4 required researchers to utilize the 20 MHz channel width setting, rather than the lower settings recommended. WR MPU4 radios used in this experiment were not capable of operating at the lower frequency or higher power settings recommended.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ADDITIONAL ANALYSIS

Analysis and field experiment outcomes from Chapter III provide the basis for some basic conclusions that address the research questions in this thesis. However, additional analysis considering the totality of this research is necessary to provide ultimate conclusions and recommendations.

A. WIRELESS BIOMETRICS AND INFORMATION DOMINANCE

Analysis of the relationship between wireless biometric data sharing and information dominance in the maritime domain is straightforward. As stated in [1], information sharing in the maritime domain is key in executing the nation's maritime strategy. Concepts and principles described in [8]–[10] demonstrate the DOD's and the Navy reliance on timely and accurate information to enable decision makers and operators on the tactical edge. The definition of identity dominance in [9] lends itself to the accomplishment of information dominance by directly addressing the notions of assured C2 and battlespace awareness, two of the three fundamental capabilities of information dominance, as defined by [9].

Selecting the most optimal mode of wireless biometric data sharing in MIO not only improves performance of the wireless tactical MANET, but also improves the efficiency of identification and verification operations, which in turn, improves identification dominance that can synergistically enhance information dominance. Thus, opportunities are created to leverage the cyber and information domains to support the mission success in MIO, and effectively, implement maritime strategy.

B. WAVE RELAY OPTIMIZATION

Optimizing the MANET tactical network is primarily related to three constraints: tactical network component specifications (radios and antennas), range between nodes, and environmental conditions related to MIO settings. While operators cannot control environmental factors, such as weather and atmospherics, range can be addressed through antenna selection and device configuration on the MANET. Additionally, available tactical radios, such as WR, are available with a variety of specifications and configuration options that can be tailored to operational requirements. For instance, missions requiring significant boarding team communication below decks might require radios with different power and frequency characteristics than would be ideal for routine operations occurring on the exterior of the boarded vessel. Tailored radio selection accounts for such differences.

1. Replacing Omnidirectional Antenna with Sector Antenna

As stated in Chapter III, replacing the standard WR 8 dBi omnidirectional antenna with an 18 dBi 60° vertical sector antenna resulted in improved network performance. Improvements were a result of improved SNR as a result of increased directivity and gain characteristics of the new antenna. As explained by Atayero and Luka in [44], using the ideal link equation given in Equation 1, where P_r is the received power and all other parameters are identified.

$$P_r = \frac{P_t G_t G_r c^2}{(4\pi)^2 f_1^2 R_1^2} \text{ (watts) where}$$

P_r = Receiver Power in watts

P_t = Transmitter Power in watts

G_t = Transmitter Antenna Gain

G_r = Receiver Antenna Gain

λ_1 = Wavelenth in meters

f_1 = frequency in Hertz

R_1 = distance from Tx to Rx in meters

Equation 1. Ideal Link Equation

Using the ideal link equation, because G_t was increased by 10 dB or a factor of 10, the power received was then increased by a factor of 10. Therefore, the SNR was also increased by a factor of 10 or 10Db.[2] In this case, only the transmit antenna was replaced. However, if the same antenna was used at the transmitting and receiving node, G_t in both antennas would have increased by a factor of 10, and the power received would increase by a factor of 100, which would result in a 20 dB increase in SNR. Clearly, increased antenna directivity, and thus increased gain, provides opportunities to improve link quality significantly across the WR MANET.

2. Range between MANET NODES

Distance between nodes also impacts link quality, which can be addressed by physically decreasing the distance between vessels or by simply adding appropriately placed nodes on the network As stated in Chapter III, the 6 dB rule of thumb is useful is approximating the effectiveness of these actions, assuming that additional nodes are placed at a points between and equidistant to nodes. Consider the ideal link equation again. If all parameters remain constant, except for $R_{1,}$ then the equation easily reduces, as shown in Equation 2.

$$P_r = \frac{K_1}{R_1^2}$$

Equation 2. Describing 6 dB Rule of Thumb

Equation 2 shows that if the range is doubled then power received is reduced by a factor of 4, or 6 dB. Likewise, if the range is halved, power received is increased by the same. The application of antenna theory in preparation for future CENETIX field experiments could prove useful in network design elements, such as node and vessel placement in maritime settings.

[2] As stated in Chapter III, the distance between vessels remained approximately 0.5 nautical miles (926 meters) throughout the experiment.

C. SEEK II INTEGRATION MODELS

1. Performance

Experiment results from October 2014 indicated faster ping sweep times and greater throughput for the Ethernet tethered model of operation, as was true at distances of 25 ft. and 50 ft. for Wi-Fi[3] operations. Several explanations for these results follow.

The SEEK II wireless NIC and the MPU4 WAP mode support 802.11n, or Wireless N standards. Maximum data rate over Wireless N is dependent upon many variables. In the best case scenario, with multiple antennas and operating on the 40 MHz channel width setting, Wireless N is capable of speeds up to 600 Mbps. As stated earlier, the WR MANET utilized the MPU4 to provide a WAP. This utilization was a constraint because the WR MPU4 has only one antenna and is designed only to operate as a WAP while using the 20 MHz channel width setting. These factors limited the maximum data rate of the 802.11 Wi-Fi link between the SEEK II and the WAP to approximately 150 Mbps.

On the other hand, modern gigabit Ethernet connections can obtain data rates of up to 1 Gbps, or 1000 Mbps, which is much faster than Wireless N [45]. WR radios and SEEK II both support gigabit Ethernet connections. These higher data rates occur because wired Ethernet simply does not suffer from many of the variables that contribute to free space path loss.

Moreover, in the October experiment, the SEEK II benefitted from a dedicated Ethernet connection. The tethering approach, preferred by Persistent Systems, ensures it would be the case no matter how many SEEK devices are added to the network in this manner. The same cannot be said for 802.11 Wi-Fi operation of the SEEK II on the WR MANET. Multiple SEEKs operating Wi-Fi would compete for WAP resources and be allocated less time on the channel that would result in slower data rates. Additionally, the half-duplex nature of Wi-Fi operation necessitates a collision avoidance mechanism; in this case, carrier sense multiple access, collision avoidance (CSMA-CA). The additional

[3] These distances were used as controls for tethered operation as well, even though those distances are quite insignificant when the wireless portion of the link occurs only over WR.

overhead required to carry out CSMA-CA makes Wi-Fi even more inefficient than Ethernet by reducing the payload per packet to support avoidance.

2. Security

The primary question about security in this thesis addresses the connection between the SEEK II and the MANET. To be clear, the tethering model is not impacted by security concerns inherent to Wi-Fi networking, which increases the overall security of the system. However, neither of the modes of operation considered in this work benefit from the assurance of FIPS 140-2 certification where the SEEK II, or to the traffic between the SEEK and the MANET, is concerned because the cryptographic boundary of the WR does not extend beyond the radios themselves. Therefore, FIPS-140 2 certification, based on WR's built-in security model, does not extend to other devices added to the MANET, such as the SEEK II. To be sure, while FIPS certification does not apply to either model, the tethering model does benefit from the inherently more secure Ethernet link between the SEEK II.

In a MIO environment, operators carry the MPU4 strapped to their person. The operator personally holds the SEEK II device during operation. The physical 24 inch Ethernet connection between the devices provides the operator positive control over the devices and their connection. This scenario offers obvious security benefits over a model, which requires wireless operation between the operator's SEEK II and an a potentially unmanned MPU4 [33].

It is worthwhile to examine the way in which each model handles encryption and decryption. The tethering model uses only the WR encryption scheme between WR nodes and no encryption across the Ethernet link. The Wi-Fi model depends on WPA2-PSK to protect data between the WR WAP and Wi-Fi devices, such as the SEEK II. The WR MANET uses AES-256 for encrypting and decrypting network traffic, while the WR WAP approaches these functions using WPA2-PSK, which utilizes AES-128. Clearly, the larger key size of the WR MANET offers greater security. It also does not require the use of a PSK. While still a common form of encryption for home users, WPS2-PSK is not appropriate for enterprise use or in systems carrying sensitive data. As early as 2010, WPA2-PSK was proven susceptible to the Hole 196 exploit, which compromises the shared key completely over the air [46]. In a WPA2-PSK implementation, if only one user’s key is compromised all users are compromised. Therefore, given the sensitive nature of MIO operations, avoiding the use of WPA2-PSK may be desirable.

IV. CONCLUSIONS AND RECOMMENDATIONS

This thesis explored methods to improve mission success in U.S. Navy maritime interdiction operations by improving information dominance in the maritime domain by optimizing the CENETIX tactical network for wirelessly sharing biometric data within the tactical environments, and ultimately, providing reach back to authoritative biometric databases, such as the DOD ABIS. Research efforts intended to, first, optimize the broader CENETIX WR MANET. Secondly, it was meant to determine the feasibility of leveraging 802.11 Wi-Fi technology for the integration of the SEEK II to the WR MANET, and to provide a comparative analysis between a 802.11 Wi-Fi operation of the SEEK II and the WR tethering approach to conducting wireless operation. The research questions in Chapter I directed all research efforts. This chapter provides answers to those questions based on data collection and observations from CENETIX field experiments, as well as recommendations for future work in this area.

A. CONCLUSIONS

The wireless sharing of biometric data in MIO can provide operators with reach back to authoritative databases, such as the DOD ABIS, which enables NRT biometric analysis for new biometric enrollments collected during MIO. This sharing enhances the DOD's ability to achieve identity dominance, which directly contributes to mission success by supporting successful execution of the Navy's information dominance strategy.

Slight modifications to the CENETIX tactical network can improve MANET performance to enhance biometric data sharing at the tactical edge, provide an opportunity for operator reach back to authoritative DOD biometric databases to improve information sharing and mission success in MIO. These modifications include the following.

- Replacing WR omnidirectional antennas with higher gain directional antennas
- Selecting tactical radios with frequency and output power characteristics appropriate for the maritime domain and tactical environment

These modifications can result in improved SNR and greater link quality to ensure success in biometric data sharing across the tactical network and contribute to reliable and efficient reach back to decision makers and authoritative databases.

Wireless integration of the SEEK II and the WR MANET, using the 802.11 WAP, is a feasible model for wirelessly sharing biometric data at the tactical edge. However, network performance should be expected to decrease as the number of SEEK II, or similar, devices on a single WR WAP increase. The SEEK II connection to the WAP precludes the use of WR FIPS 140-2 accredited data encryption, but the WR and SEEK II both support WPA2-SPK encryption, which offers some level of security for the data in transit between the SEEK II and WR WAP.

Of the two models of wireless SEEK II operation considered in this work, the tethering model offers greater network performance, and is inherently more secure than the 802.11 Wi-Fi model. The tethering model should be the preferred method of integrating the SEEK II, or similar biometric devices, to the tactical MANET.

The 802.11 Wi-Fi integration model may be suitable in situations in which the number of available tactical radios is a constraint. Multiple SEEK II devices can connect to a single WAP that allowed them access to the MANET, and ultimately provide reach back. Conversely, the tethering model requires one tactical radio for each SEEK II or Wi-Fi device. The Wi-Fi model provides an option of limited hardware footprints to boarding teams.

Ultimately, research on the CENETIX tactical network shows that 802.11 Wi-Fi is a feasible method for connecting the SEEK II and similar devices to the tactical MANET; however, in most cases, tethering SEEK II biometric devices directly to tactical radio via Ethernet provides the most optimal performance and increases network security for conducting biometric data sharing during MIO.

B. FUTURE WORKS

Many opportunities exist for future work on this topic. Two are key, and would be well suited for near-term exploration.

1. Optimization of the Tactical MANET

This study considered MIO scenarios that were present in CENETIX field experiments. In these scenarios, relay nodes were largely static to support the specific MIO objectives outlined in field experiment planning. However, many variables exist that could prove very dynamic in alternative scenarios with different objectives. To discover more optimal tactical network design and implementation for a range of MIO scenarios, continuous throughput testing should be accomplished to include continuously altering antennas, distance between nodes, bearing to nodes, radio power, and radio frequency configuration, while researchers monitor the network's performance and capture data about throughput. During continuous testing, various types of MIO operations should be simulated that require the transmission and reception of various types and sizes of data across the MANET. Capturing data from continuous throughput monitoring allow CENETIX researchers to analyze the findings and determine a range of optimization efforts, which can be applied to specific scenarios. Moreover, it could result in finding one "best" solution that offers the greatest opportunity to achieve information dominance in MIO and support mission success, when various constraints make customization undesirable or impossible.

2. Layer 2 MANET Security

At the tactical edge, the strictly layer 2 operation of the MANET offers many benefits, but also introduces specific security concerns. Research such as [16] is available regarding MANET security. However, a knowledge gap occurs regarding how known layer 2 cyber vulnerabilities impact the maritime domain. Thorough analysis of existing research on MANET security can help form some experiments. The CENETIX tactical network provides an opportunity for penetration testing and vulnerability analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] S. L. Caldwell, “Testimony before the subcommittee on government management, finance, and accountability, committee on government reform, House of Representatives, maritime security: Information-sharing efforts are improving, statement of Stephen L. Caldwell, acting director homeland security and justice issues,” United States Government Accountability Office, Washington, DC, GAO-06-933T, Jul. 2006.

[2] M. J. Verett, “Performance and usage of biometrics in a testbed environment for tactical purposes,” M.S. thesis, Dept. of Information Sciences, Naval Postgraduate School, Monterey, CA, 2006.

[3] Wave relay white paper. (n.d.). Department of Defense, Persistent Systems. [Online]. Available: http://www.persistentsystems.com/persistent-systems government. Accessed Nov. 7, 2014.

[5] J. A. Davis, “An analysis of network and sensor performance within IEEE 802.x wireless MESH networks in the Tactical Network Topology (TNT),” M.S. thesis, Dept. of Information Sciences, Naval Postgraduate School, Monterey, CA, 2006.

[6] K. A. Stewart. (2014, May 23). NPS, international special forces groups, NATO collaborate to counter CBRN threats. [Online]. Available: http://hdl.handle.net/10945/41344

[7] SOFEX identity operations database. (n.d.). [Online]. Available: http://sofex.identityops.com/. Accessed Oct. 3, 2014.

[8] Joint Chiefs of Staff, “Joint communications system,” Washington, DC, Joint Publication 6-0, Jun. 2010.

[9] Navy strategy for achieving information dominance 2013–2017. (n.d.). United States Navy. [Online]. Available: http://www.public.navy.mil/fccc10f/Strategies/Navy_Strategy_for_Achieving _Information_Dominance.pdf. Accessed Nov. 12, 2014.

[10] DOD information sharing strategy. (2007, May). Department of Defense. [Online]. Available: http://dodcio.defense.gov/Portals/0/Documents/DIEA/InfoSharingStrategy.pdf

[11] “Biometrics Glossary, v6.0,” Biometric Identity Management Agency BIMA (now called Defense Forensics & Biometrics Agency, DFBA), Clarksburg, WV, Apr. 2012.

[12] B. O'Hara and A. Petrick, *IEEE Handbook: A Designers Companion*. New York: IEEE Press, 2005, ch. 2, pp. 5–15.

[13] J. Jun and M. L. Sichitiu, "The nominal capacity of wireless mesh networks," *Wireless Communications, IEEE* , vol. 10, no. 5, pp. 8, 14, Oct. 2003.

[14] B. Kim et al., "Tactical network design and simulator with wireless mesh network-based backbone architecture," in *Applications and Technology Conference (LISAT), 2010 Long Island Systems*, 2010, pp. 1, 5, 7.

[15] S. Corson and J. Macker, "IETF Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations," *IETF RFC 2501*, 1999.

[16] M. E. Orwat et al., "An ontological approach to secure MANET management," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference*, 2008, pp. 787, 794.

[17] T. Dean, *Network+ Guide to Networks*, 6th ed. Boston, MA: Course Technology, 2013, pp. 153–154, 297–299, 700–701.

[18] Quad radio specification sheet. (n.d.). Persistent Systems. [Online]. Available: http://www.persistentsystems.com/pdf/Quad_SpecSheet.pdf. Accessed Aug. 1, 2014.

[19] MPU4 specification sheet. (n.d.). Persistent Systems. [Online]. Available: http://www.persistentsystems.com/pdf/MPU4_SpecSheet.pdf. Accessed Aug. 3, 2014.

[20] *WR User Manual, Version 3.0*, New York: Persistent Systems, 2014, pp. 5, 10–14.

[21] H. Rubens, Founder and CEO, Persistent Systems, private communication, Oct. 2014.

[22] DOD electronic biometric transmission specification version 3.0. (2011). DIN: BIMA-STB-STD-11-001. Biometrics Identity Management Agency. [Online]. Available: http://www.biometrics.dod.mil/Files/ Documents /Standards/DOD_ EBTS_v3_0.pdf

[23] SOCOM Research, Development and Acquisition Center, "Authorization to operate SEEK II," USSOCOM J6 ATO, MacDill Air Force Base, FL, Feb. 2013.

[24] *SEEK II Specification Sheet*, Palm Beach Gardens, FL: Cross Match Technologies, 2011, pp. 1–2.

[25] D. Bartlett, “Satellite mesh architectures in the maritime domain,” M.S. thesis, Dept. Information Sciences, Naval Postgraduate School, Monterey, CA, 2014.

[26] B. Steckler, “BGAN and VSAT don’t leave home without them,” NPS HFN Research Group, unpublished.

[27] O. Antillion, “Hastily formed networks (HFN) as an enabler for the emergency response community,” M.S. thesis, Dept. Information Sciences, Naval Postgraduate School, Monterey, CA, 2012.

[28] A. Bordetsky, “Testbed for tactical networking and international collaboration in maritime interdiction operations,” presented at CENIC 2010. Conf., Monterey, CA, 2010.

[29] A. Bordetsky and E. Bourakov. (2006). Adaptive on-demand networking with self-aligning wireless nodes. [Online]. Available: http://calhoun.nps.edu/handle/10945/35925

[30] Defense Forensics and Biometrics Agency (DFBA). (2013, Apr.). DOD biometrics enterprise architecture (integrated) v2.0, common biometric vocabulary (CBV). [Online]. Available: http://www.biometrics.dod.mil/Files/Documents/References/common%20biometric%20vocabulary.pdf

[31] Biometric Enabling Capabilities (BEC). (n.d.). U.S. Army PEO enterprise information systems. [Online]. Available: http://www.eis.army.mil/ programs/bec. Accessed Nov. 14, 2014.

[32] S. Vann-Olejasz, “Army acquisition, logistics and technology,” presented at Project Management Office, DOD Biometrics, PMO DOD Biometrics Briefing, Sep. 2014.

[33] “Multi-Service tactics, techniques, and procedures for tactical employment of biometrics in support of operations,” DOD Air Land Sea Application Center (ALSA), Joint Base Langley-Eustis, VA, ATP 2-22.85, Apr. 2014.

[34] J. C. Buckle, U.S. Army ICOE (U.S.), private communication, Nov. 2014.

[35] “Security Requirements for Cryptographic Modules,” U.S. Dept. of Commerce, Washington, DC, NIST PUB 140-2, May 2002.

[36] “FIPS 140-2 non-proprietary security policy, persistent systems wave relay quad radio router and man portable unit (generation 2, generation 3 single/dual, and generation 4, level 2 validation, version 5.2,” New York: Persistent Systems, Jan. 2015.

[37] R. Deal, *The Complete Cisco VPN Configuration Guide*, Indianapolis, IN: Cisco Press, 2006, p. 12.

[38] S. Zeltser et al., *Inside Network Perimeter Security*, Indianapolis, IN: Sams Technical Publishing, 2005, pp. 161, 167–168.

[39] K. S. Sorrell, LT, USCG Research and Development Center, private communication, Oct. 2014.

[40] M. F. Young. (2004). Understanding dB. FCC outreach program. [Online]. Available: http://wireless.fcc.gov/outreach/2004broadbandforum/comments/YDI_understandingdb.pdf

[41] A. Adnen, "Propagation modeling of wireless systems in shipboard compartments," M.S. thesis, Dept. Electronic. and Computer. Engineering, Naval Postgraduate School, Monterey, CA, 2003.

[42] J. Zhang. (2007). Power control in wireless ad hoc networks. [Online]. Available: http://search.proquest.com/docview/35574598?accountid=12702

[43] A. R. Sinsel, "White paper: NPS CENETIX MIO TNT WMD ISR EXPERIMENT August 2014," unpublished.

[44] A. Atayero and M. Luka, "Satellite link design: A tutorial," *International Journal of Electrical & Computer Sciences* IJECS-IJENS, vol. 11, no. 04, pp. 1–2, Aug. 2011.

[45] M. Norris, *Gigabit Ethernet Technology and Applications*. London: Artech House, 2002, p. 58.

[46] S. Ahmad, "WPA2 Hole 196," presented at DEFCON 18 Conference Conf., Las Vegas, NV, 2010.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California