NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXTENDING TACTICAL FLEET COMMUNICATIONS THROUGH VoIP

by

David T. Scott

September 2014

Thesis Advisor: John Gibson
Second Reader: Duane Davis

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** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
EXTENDING TACTICAL FLEET COMMUNICATIONS THROUGH VoIP

5. FUNDING NUMBERS

6. AUTHOR(S) David T. Scott

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)

The Navy's Fleet is in need of tactical voice communication systems that are highly reliable, protected from cyber threats, and able to operate in a denied or degraded environment. Many of the Navy's current systems rely on outdated and inefficient technology, which reduces the overall effectiveness of our tactical communication channels and also limits the accessibility of these systems to communications challenged areas within ships.

This research examines the capabilities, limitations, and overall performance of an integrated Voice over Internet Protocol (VoIP) system using four popular link layer protocols (i.e., Ethernet, 802.11n, 2.4 GHz 802.11ac, and 5 GHz 802.11ac) in an attempt to determine the feasibility of incorporating VoIP technology within Consolidated Afloat Networks and Enterprise Services and digital modular radio communication systems. The specific features compared in this study are VoIP network bandwidth consumption, overall network capacity between the four link layer protocols, VoIP codecs, VoIP call limits, intrusion detection system effects, and the effects of additional non-VoIP network traffic.

The results of the study show that afloat tactical communications can be effectively enhanced by integrating VoIP intrusion detection systems monitored VoIP network applications with afloat communications systems, and by extending those systems with wireless devices utilizing the 802.11ac protocol.

14. SUBJECT TERMS Voice over Internet Protocol, tactical communication systems, tactical communications, afloat communications, intrusion detection system, shipboard networks, wireless, link layer, Ethernet, 802.11n, GHz 802.11ac, Consolidated Afloat Networks and Enterprise Services, digital modular radio

15. NUMBER OF PAGES
95

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXTENDING TACTICAL FLEET COMMUNICATIONS THROUGH VoIP

David T. Scott
Lieutenant, United States Navy
B.S., University of Florida, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: David T. Scott

Approved by: John Gibson
Thesis Advisor

Duane Davis
Second Reader

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Navy's Fleet is in need of tactical voice communication systems that are highly reliable, protected from cyber threats, and able to operate in a denied or degraded environment. Many of the Navy's current systems rely on outdated and inefficient technology, which reduces the overall effectiveness of our tactical communication channels and also limits the accessibility of these systems to communications challenged areas within ships.

This research examines the capabilities, limitations, and overall performance of an integrated Voice over Internet Protocol (VoIP) system using four popular link layer protocols (i.e., Ethernet, 802.11n, 2.4 GHz 802.11ac, and 5 GHz 802.11ac) in an attempt to determine the feasibility of incorporating VoIP technology within Consolidated Afloat Networks and Enterprise Services and digital modular radio communication systems. The specific features compared in this study are VoIP network bandwidth consumption, overall network capacity between the four link layer protocols, VoIP codecs, VoIP call limits, intrusion detection system effects, and the effects of additional non-VoIP network traffic.

The results of the study show that afloat tactical communications can be effectively enhanced by integrating VoIP intrusion detection systems monitored VoIP network applications with afloat communications systems, and by extending those systems with wireless devices utilizing the 802.11ac protocol.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3GPP	3rd Generation Partnership Project
ADNS	Automated Digital Network System
AIFS	Arbitration Inter-Frame Spacing
BFTN	Battle Force Tactical Network
BLOS	beyond line of sight
CANES	Consolidated Afloat Networks and Enterprise Services
CBWFQ	class based weighted fair queuing
CCE	common computing environment
CODA	Common Optical Distribution Architecture
CWmax	Contention Window maximum
CWmin	Contention Window minimum
DIACAP	DOD Information Assurance Certification and Accreditation Process
DMR	digital modular radio
DOD	Department of Defense
DoS	denial of service
EHF	extremely high frequency
EM	electro-magnetic
GSM	Global System for Mobile Communications
HAIPE	High Assurance Internet Protocol Encryptor
HF	high frequency
HTTP	Hyper Text Transmission Protocol
IDS	intrusion detection system
iLBC30	Internet Low Bitrate Codec 30
IP	Internet Protocol
IPICS	IP Interoperability and Collaboration System
IPS	intrusion prevention system
IPSec	Internet Protocol Security
ISNS	Integrated Shipboard Network System
ITU	information transfer unit

LAN	local area network
LMR	land mobile radio
LOS	line of site
LTE	long-term evolution
Mbps	megabits per second
PBX	Private Branch Exchange
PC	personal computer
pps	packets per second
PSTN	Public Switched Telephone Network
QoS	quality of service
RAM	random access memory
RAPIDS	Real-time Automated Personnel Identification System
RF	radio frequency
RTP	Real-time Transport Protocol
RTCP	RTP Control Protocol
SATCOM	satellite-based communication
SDC	serial data controller
SIP	Session Initiation Protocol
SIPRNet	Secret Internet Protocol Router Network
SPIT	Spam-over-Internet-Telephony
SRTP	Secure Real-time Transport Protocol
SVoIP	Secure Voice Over IP
TCP	Transmission Control Protocol
TLS	transport layer security
TXOP	transmit opportunity
UA	user agent
UAC	user-agent client
UAS	user-agent server
UDP	User Datagram Protocol
UHF	ultra high frequency
vFDS	VoIP flooding detection systems
VHF	very high frequency

vIDS	VoIP intrusion detection systems
VLAN	virtual local area network
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secret Internet Protocol
WAP	wireless access point
Wi-Fi	wireless fidelity
WRED	weighted random early detection

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, John Gibson, and second reader, Duane Davis, for all of their support and guidance throughout the thesis process. I would also like to thank Anibal Intini, Brian Cooper and David Sizemore for all of their expertise and assistance throughout my research and testing.

This material is in support of a Marine Corps N1 study objective for exploring reliable communications to embarkable units within the well-decks of amphibious ships. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the Marine Corps N1 study.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM DESCRIPTION

The Navy's fleet is in need of tactical voice communication systems that are highly reliable, secured from cyber threats, and able to operate in a denied or degraded environment [1]. Many of the Navy's current systems rely on outdated and inefficient technology, which significantly reduces the overall effectiveness of our tactical communication channels. This limited technology also restricts the accessibility of these systems to communications challenged areas within the ship.

B. DISCUSSION AND MOTIVATION

Recent Naval training exercises and experiments have successfully utilized integrated voice over internet protocol (VoIP) systems to provide efficient and reliable communications in ways that have not been possible in the past [2]. These successes clearly illustrate the potential upside of increased incorporation of this technology into fleet systems.

There are numerous flaws with the current afloat, line-of-site, voice communications architecture in the Navy. The systems are unreliable, easily degraded, and depend on extremely inefficient technology. The Navy has been using these same types of communication systems for "transoceanic and transcontinental communication traffic" since 1924 [3]. Modern navies work in a new digital era of high-speed, readily available and extremely efficient cyber communication technologies. One of the most prominent new audio cyber technologies is VoIP. VoIP gives us the ability to send audio communications over a digital packet-switched network with little-to-no signal loss. The purpose of this thesis is to explore how VoIP can be used to meet the Navy's growing need for a cutting-edge, extremely reliable, and efficient means of communications afloat.

Additionally, current afloat communication systems do not have the ability to extend access to certain areas within ships. When other military units come aboard a Navy ship, they are limited to specific locations where they can access the current tactical

communication channels. This is especially troublesome for Marines embarked onboard amphibious craft within the well-decks of Navy ships. They currently have no way of accessing tactical communications until outside the "skin" of the ship. Implementation of VoIP communication channels on these ships will provide a number of mechanisms through which embarked units can gain access throughout the ship.

C. PURPOSE OF STUDY

This research provides an assessment of current and future afloat tactical communications systems, their interoperability, and the various transmission media used, as well as an assessment of current VoIP technologies and systems used in military and corporate environments, and the benefits and concerns of each. In particular, this work focuses on identifying ways to improve tactical communications by augmenting current systems with protected VoIP systems, integrating VoIP technology within shipboard networks, and wirelessly extending VoIP data to areas not covered by current communications systems.

The study assesses the integration of VoIP systems with tactical communication systems and networks afloat. It analyzes how VoIP systems may affect the quality of service of an afloat network. It also identifies the possible cyber security risks and mitigations of introducing a VoIP system to an afloat network.

The research examines the capabilities, limitations, and overall performance of an integrated VoIP system in an attempt to determine the feasibility of incorporating VoIP technology within Consolidated Afloat Networks and Enterprise Services (CANES) and digital modular radio (DMR) communication systems. This was done by comparing multiple features of the following four popular link layer protocols: Ethernet, 802.11n, 2.4 GHz 802.11ac and 5 GHz 802.11ac. The specific features compared in this study were VoIP network bandwidth consumption, overall network capacity between the four link layer protocols, VoIP codecs, VoIP call limits, intrusion detection system effects, and the effects of additional non-VoIP network traffic.

Overall, the purpose is to provide a recommendation for specific ways that VoIP systems can be used to improve and extend tactical communications afloat, the hardware

and software that could be used, the systems that can be integrated, and efficient transmission media for expansion to communications-challenged areas.

D. BENEFITS OF STUDY

The integration of VoIP systems with specific afloat communication systems has the potential to create numerous benefits to the fleet. These systems can reduce the electromagnetic (EM) footprint of afloat platforms, by exchanging numerous analog voice circuits for a lesser number of digital voice channels. They will also decrease the hardware footprint onboard ships and can decrease the equipment and maintenance costs associated with that hardware. Digital VoIP technology allows for the integration of multiple shipboard communications systems as well. VoIP systems can give ships the ability to extend communications to areas onboard that may not have previously been possible, such as the well deck and temporary locations for embarkable units. This can be facilitated by leveraging existing wired and wireless networks. These systems increase the reliability and availability of our tactical voice communication channels as well. These channels can then be maneuverable within the electromagnetic spectrum, leading to greater jam resistance. Increased communications security will also be available through various cyber security technologies. Integrating VoIP systems afloat will significantly improve the Navy's tactical communications posture overall.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. AFLOAT TACTICAL COMMUNICATION SYSTEMS

Tactical communication systems afloat are the backbone of the Navy's warfighting architecture. For tactical voice communications outside the skin of the ship, the primary medium used by our military has been, and is currently, analog radio frequency (RF). The only tactical voice transmitted within the skin of the ship is on a wired legacy system with its own specific access points. There are three primary frequency ranges that have typically been used for voice communications in the RF spectrum:

- High frequency (HF): From 3 to 30 MHz, used for voice and data in beyond line of site (BLOS) communications, with ranges over thousands of miles.
- Very high frequency (VHF): from 30 to 300 MHz, used in line of site (LOS) communications, for passing voice and data from ship-to-ship, ship-to-shore and ship-to-air.
- Ultra high frequency (UHF): from 300 MHz to 3 GHz, used as the primary means for providing tactical, operational and administrative voice and data information.

The primary block of the RF spectrum used for tactical communications afloat is from 255 to 400 MHz. UHF. The extremely high frequency (EHF) range, 30 to 300 GHz, is now starting to be used more frequently for satellite-based communication (SATCOM). The super high frequency range, 3 to 30 GHz has been used in the past, but this range has become quite saturated and is now primarily used for digital communication systems. In today's Navy, non-SATCOM circuits still provide the preferred means for tactical voice communications.

1. Radio Communication Systems

The Navy has used a number of radio communications systems throughout the years, some of the most recent being the AN/WSC-3, the digital modular radio (DMR), and the Battle Force Tactical Network (BFTN). These systems are discussed below.

a. AN/WSC-3

The AN/WSC-3, often referred to as the "Whiskey-3," transceiver has been one of the Navy's primary means of LOS communications since about 1983 [4] and is still being used on many naval vessels. The AN/WSC-3 operates in the UHF spectrum range, from 225 to 399.975 MHz, using amplitude and frequency modulation techniques [5]. It is capable of both LOS and satellite communications, and its high transmit power allows for reliable communications over long distances. However, the AN/WSC-3 is an old radio and has extremely high downtime and maintenance costs. This radio is currently being replaced by the Navy's digital modular radio.

b. Digital Modular Radio

The DMR is the newest radio used for tactical voice communications in the Navy. The DMR is a software-defined radio. These extremely versatile digital radios can be configured with a number of different software packages in order to communicate on multiple types of waveforms. While the term "waveform" has various interpretations, suffice it to say that compatibility between radio systems, and often the applications supported by these systems, requires that each device generate and process the appropriate waveforms. These waveforms tell the DMR how to interpret the RF signal, and give it the ability to communicate with numerous types of other radios. The DMR operates anywhere from 2 MHz to 2 GHz providing capability in the HF, VHF, and UHF spectrums. One DMR is capable of operating on four channels simultaneously (see Figure 1). A full DMR suite can handle up to 128 simultaneous channels through its human machine interface [6]. The system is being further developed with upgrades planned to provide HF broadband capabilities to support a net-centric environment while replacing other outdated systems [5].

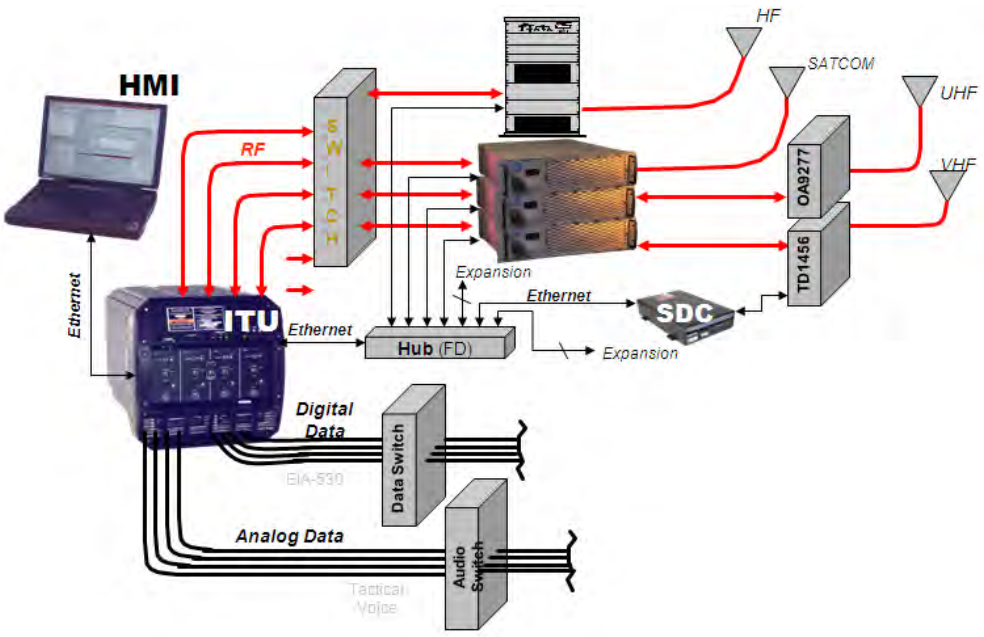

Figure 1. Basic DMR Architecture, from [5]

c. Battle Force Tactical Network

BFTN is another tactical communication system used for wireless transmission of voice and data between surface, air, submarine, and shore based units. Typically, BFTN is used to transmit digital data rather than tactical audio communications, though audio communication capability is present. This system uses the HF and UHF frequency ranges to transmit low data-rate digital information, such as email and chat. It supports encrypted communications within the Department of Defense (DOD) and between DOD and its coalition partners as well. Ongoing upgrades to this system provide for HF and UHF LOS data links of up to 0.128 Mbps and 1.9 Mbps, respectively [5].

2. Network Communication Systems

Three of the most prolific network communications systems used by the Navy today are the Automated Digital Network System (ADNS), Integrated Shipboard Network System (ISNS), and Consolidated Afloat Networks and Enterprise Services (CANES).

a. Automated Digital Network System

ADNS [5] is the primary afloat traffic management system for Internet Protocol (IP) connections to and from shipboard networks. The newest version is ADNS Increment III, which is used on large, force-level platforms such as carriers and amphibious ships. It supports data rates between 25 and 50 Mbps. Increment III supports IP version 4 and 6 hosted VoIP, video, and data traffic.

One of the main functions of ADNS is to provide quality of service (QoS) dynamic bandwidth management. This provides the ability to allocate bandwidth in real time to the highest priority systems and networks. Traffic priority is categorized based on guidance from Fleet Cyber Command. Traffic markings necessary for prioritization are implemented by the Blue Coat Packet Shaper [7], an application traffic management device with the ability to monitor, control, and improve traffic flow. Traffic priority markings provided by the packet shaper, give administrators a greater situational awareness of the status of traffic and QoS changes on the network.

b. Integrated Shipboard Network System

ISNS is the Navy's current shipboard network architecture. It provides a typical access or integrated local area network (LAN) infrastructure to connect client workstations, printers, servers, and other network equipment. It is the backbone for all of the ship's command, control, communications, computers and intelligence networked applications. ISNS' core set of applications and services are provided by a suite of government-off-the-shelf and commercial-off-the-shelf products known as the Common PC Operating System Environment. Unfortunately, much of the hardware and software components that make up ISNS is no longer supported. ISNS is now being replaced by a new and improved network infrastructure known as CANES.

c. Consolidated Afloat Networks and Enterprise Services

CANES is the newest network system to be fielded in the fleet to replace all of the Navy's older and outdated computing systems. CANES includes many improvements over previous systems in areas such as "tailored profiles and information management,

collaboration, information discovery, information exchange, and information storage" [5]. It is based around a common computing environment (CCE) for enhanced performance, improved maintenance, and a better overall end-user experience. CANES provides QoS through a series of service level agreement thresholds, enforced by a service level management system. This allows for a more detailed level of prioritization than in previous systems. Unlike other computing environments, CANES is built to directly support VoIP traffic on specific enclaves. This will allow for VoIP communications, internally, as well as with other ships and shore sites connected to Defense Information Systems Agency enterprise networks.

The following is an abbreviated list of some of the major components in the CANES architecture [5]:

- CANES network devices
- Cisco C3750G switches
- Cisco C3750V2 switches
- Cisco C3750X switches
- Cisco C2921 routers
- CANES end-devices and software
- HPZ200 small form factor workstations
- Panasonic Toughbook CF-52 Laptops
- HP t5745 Thin Clients
- XEROX printers
- Cisco EnviroXtreme 7962 handsets
- Windows 7 Professional 64 bit OS
- Red Hat Bare Metal OS v 5.3
- SecureOffice Trusted Thin Client Software
- CANES Data Center Devices and Software
- Netra SPARC T3-1 Servers
- vSphere Enterprise 4.1 ESX
- vCenter Server 4 Standard
- vCenter Site Recovery Manager

- Solaris Global Zone
- Solaris 10 U7 for SPARC
- Microsoft Windows Server Datacenter 2008
- Red Hat Enterprise Linux Standard
- IBM Blade Center HTs
- Cisco Catalyst Switch Module 3110G
- HS22V blades
- IBM DS3512 Express Dual Controller Storage System
- IBM EXP3512 Express Chassis

Aside from the hardware and software that CANES provides to the fleet, the system's major design improvement is its use of the CCE. The CCE is based on the concept of taking many services and applications that are currently hosted on separate servers, each running its own particular operating system and putting them all into a common network and set of servers. This consolidation is made possible through virtualization technologies using service-oriented architectures. CANES is currently being developed to bring together 37 separate core services and applications [8]. Through this consolidation of services and equipment, the CANES CCE allows for easier system upgrades and updates, higher quality administration, an increase in availability of services, and a reduced hardware footprint.

B. VOIP

In order to understand how VoIP can be integrated with afloat tactical communications systems (i.e., CANESs and DMRs), it is beneficial to know more about certain aspects of the technology. This research will further analyze three such aspects: the development of VoIP technology, the specific protocols in which VoIP operates upon, and VoIP security.

1. VoIP Development

Voice over Internet Protocol is one of the most commonly used communication technologies today and has become popular worldwide [9], [10].[1] It has numerous uses both in the consumer market and private homes. VoIP technology has also taken hold in the corporate sector. Many militaries are now using VoIP for a multitude of applications, as well.

a. The VoIP of the Past

The VoIP concept began in the 1990s when PC enthusiasts realized they could send voice data over the Internet instead of using the typical Public Switched Telephone Network (PSTN). This required both users to have a microphone and speakers connected to a computer with Internet connectivity while running compatible VoIP communication software. VocalTec, Inc., released the first Internet phone program in 1995 [11]. Around 1998, VoIP technology expanded to include calls from PCs to phones as well. By the year 2000, about three percent of all voice traffic was sent via VoIP [11]. *BBC News* Correspondent Mark Ward in 2004 cited Internet pioneers such as Vint Cerf in predicting that "the net will stop being a part of the telephone network, and instead the telephone network will become a part of the net" [12]. With current trends, this prediction appears to be coming to fruition.

b. The VoIP of Today

Three of the largest communities leveraging VoIP are the consumer market, the corporate sector, and military organizations. No matter where it's used, in order to be a reliable technology, VoIP must be available on demand. According to Mehmet Toy of the *Information and Communication Technology* book series, "Services such as broadcast video, voice over IP, and video on demand require five-nines availability, which means a high-level [of] survivability against failures" [13]. VoIP services with such a degree of reliability are now typically offered in cable and Internet bundles from major service

[1] Section 1 is derived from a prior Naval Postgraduate School (NPS) research paper of the author, titled, "The Development of VoIP" [10].

providers, for instance, AT&T U-verse, Comcast Xfinity, and Verizon FiOS. Third party companies like Ooma, Vonage, and MagicJack, offer VoIP services via a home Internet connection and some additional equipment for a nominal fee. Other companies, such as Google and Skype, offer free VoIP services through web-based and computer-based software that allows users to access VoIP services using any Internet connection. The smartphone industry has quickly taken to this concept as well, with numerous third party applications (e.g., Viber, talkatone, text+) being developed to allow for VoIP communications via a phone's data plan or nearby wireless fidelity (Wi-Fi) network. With the emergence of an all-packet-switched cellphone infrastructure, such as long-term evolution (LTE), packet-oriented voice capabilities are necessary to allow the cellular industry to move away from the circuit-switched voice systems of third generation and earlier systems [14].

Outside of the consumer market, VoIP is becoming the preferred communications method for businesses and military organizations as well [15], [16]. VoIP has provided an inexpensive solution for communications within and between businesses using their current IP network infrastructure, thus eliminating the need for a telephone service provider and separate telephone infrastructure. Certain companies also offer services to link communications between VoIP networks and the PSTN. Current provider exemplars include Jive, Nextiva, MPROCOM, VoIP DITO, and Onsip. Much like the corporate world, the military is leveraging VoIP communication solutions as well. Shore commands like Tactical Training Group Pacific use VoIP for exercise, coordination, and business communications. VoIP has large military implications in areas such as communications within and between commands and ships, hastily-formed communications in support of training evolutions, and secure communications. Unfortunately, the Navy's afloat community has been slow to adopt VoIP, which has only recently begun to make its way to the fleet through the CANES system [5].

c. The VoIP of the Future

VoIP has had tremendous growth and development, and the trend is expected to continue for many years [9]. VoIP's future will likely hold developments such as new

protocols, new applications of the technology, and a possible full takeover of the telecommunications industry. New protocols have been, and will continue to be, developed based upon VoIP technology. VoIP continues to be further integrated into wired, Wi-Fi, and cellular networks and devices. One of many VoIP researchers (Axvoice) supports this assertion, and states that some other factors contributing to the expansion of VoIP include "better call quality, low cost of making phone calls, portability, and flexibility of use" [9]. Whether it is new protocols, new uses, or a new standard for telecommunications all together, VoIP technology will account for an increasing share of U.S. telecommunications infrastructure in years to come as depicted in Figures 2 and 3. Current shipboard environments stand to benefit from fully integrating such a persistent, evolving, and expanding technology as VoIP.

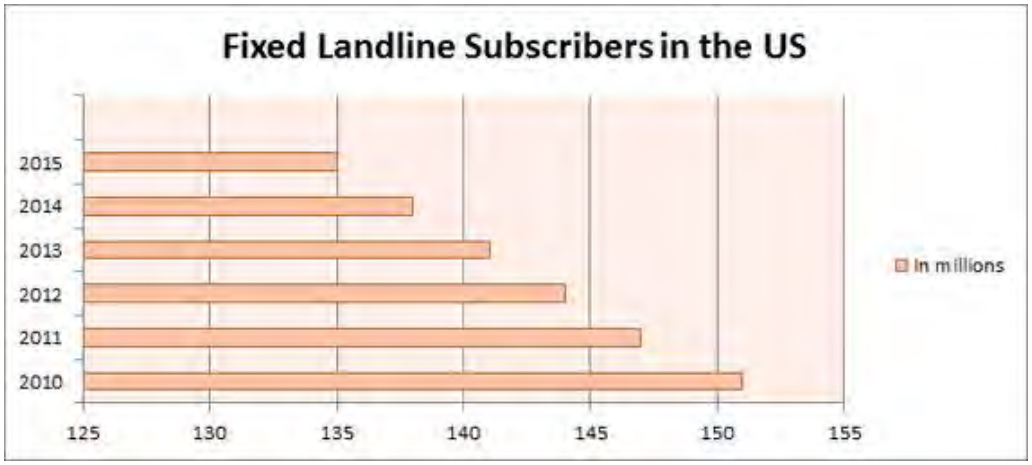

Figure 2. Fixed Landline Subscribers in the U.S., from [9]

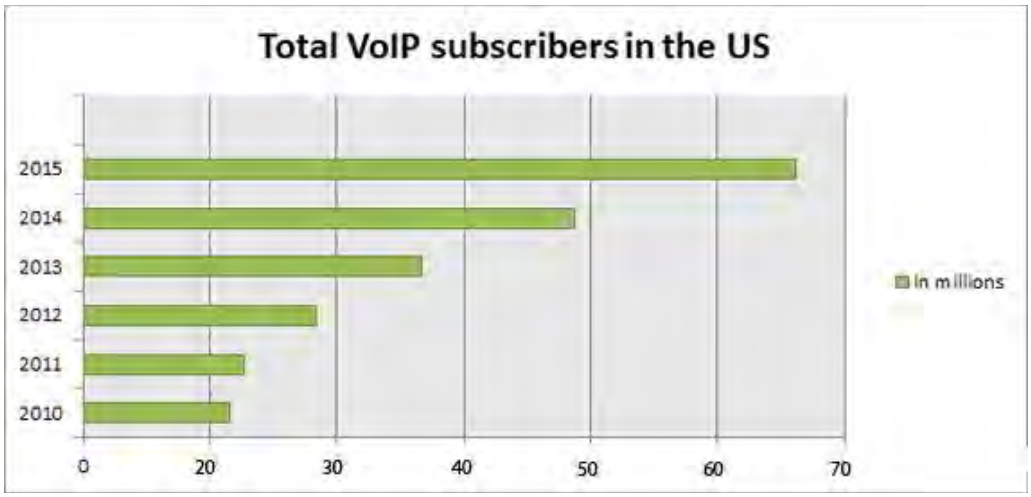

Figure 3. Total VoIP Subscribers in the U.S., from [9]

2. VoIP 101

VoIP consists of a suite of different protocols that work together to deliver multimedia data between users. The two major signaling protocols used in different VoIP architectures are H.323 and Session Initiation Protocol (SIP) [17]. Many other protocols are used that either assist the signaling protocols, transfer multimedia data, or perform various other VoIP support functions. Since the technology is IP-based, it relies on a number of other non-VoIP-specific protocols. Aside from just the design of the protocol, there is an entire vocabulary unique to VoIP as well.

Any major communications technology typically comes with its own specific vocabulary that describes the same types of devices with a unique set of terms, and VoIP is no different. The end devices (e.g., PCs, VoIP phones, telephones) are typically referred to as endpoints or user-agents (UAs). More specifically, they are the user-agent client (UAC), used to create the call request, and the user-agent server (UAS), used to receive the call request. Each UA can function as either the client or server, depending on who initiates the call. A computer-based VoIP application that uses a device's audio components is known as a "soft phone," whereas a hardware-based VoIP phone that directly connects to a network is known as a "hard phone." There are many different types of VoIP servers, some that can be on the same device, some that have similar names to other network servers, and some that perform the same functions but have

entirely different names. These are VoIP devices such as registrar servers, proxy servers, redirect servers, gateways, gatekeepers, and multipoint control units [17].

One of the two prevailing VoIP signaling protocols is H.323. This protocol was built as a foundation for transmitting communication data over IP networks. It is excellent for transmitting (and transforming) VoIP data across many different types of networks, from the integrated services digital network to the PSTN, and even cellular networks. It performs somewhat similarly to the PSTN's signaling protocol Signaling System Number 7. H.323 does not have much security by design; however, it does rely on the H.235 set of protocols for authentication security [17].

There are a number of devices used in a typical H.323 architecture including the H.323 gateway, call manager, and gatekeeper. The H.323 gateway provides the translation and interface between H.323 and other protocols and networks such as SIP and PSTN. The call manager is the VoIP supervisor. It directs all calls for the network and controls the services and features provided to the UAs. Finally, the gatekeeper is used for signaling and directory services for calls across multiple networks. A simple Cisco H.323 system is shown in Figure 4, along with a basic call establishment diagram in Figure 5.

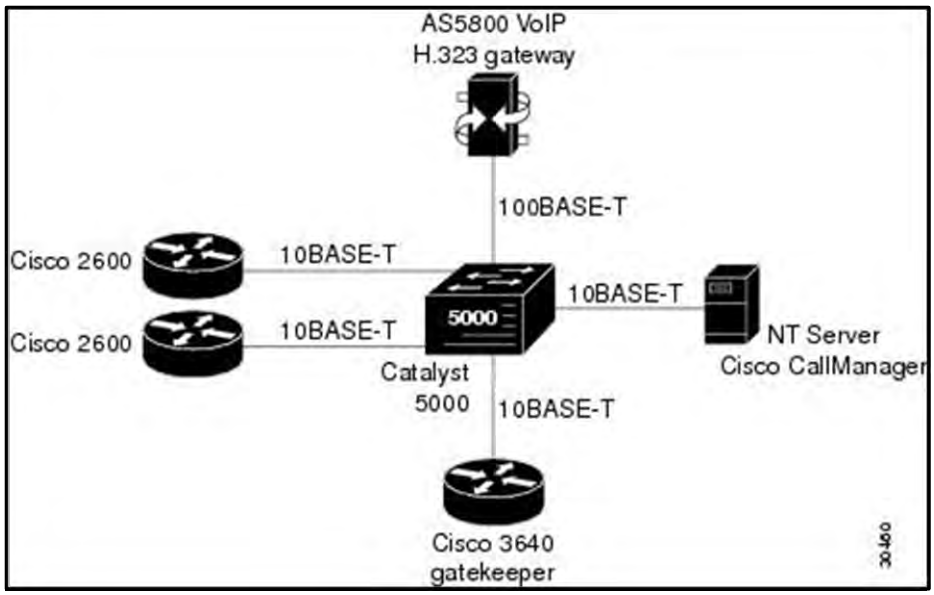

Figure 4. Basic H.323 Network Diagram, from [18]

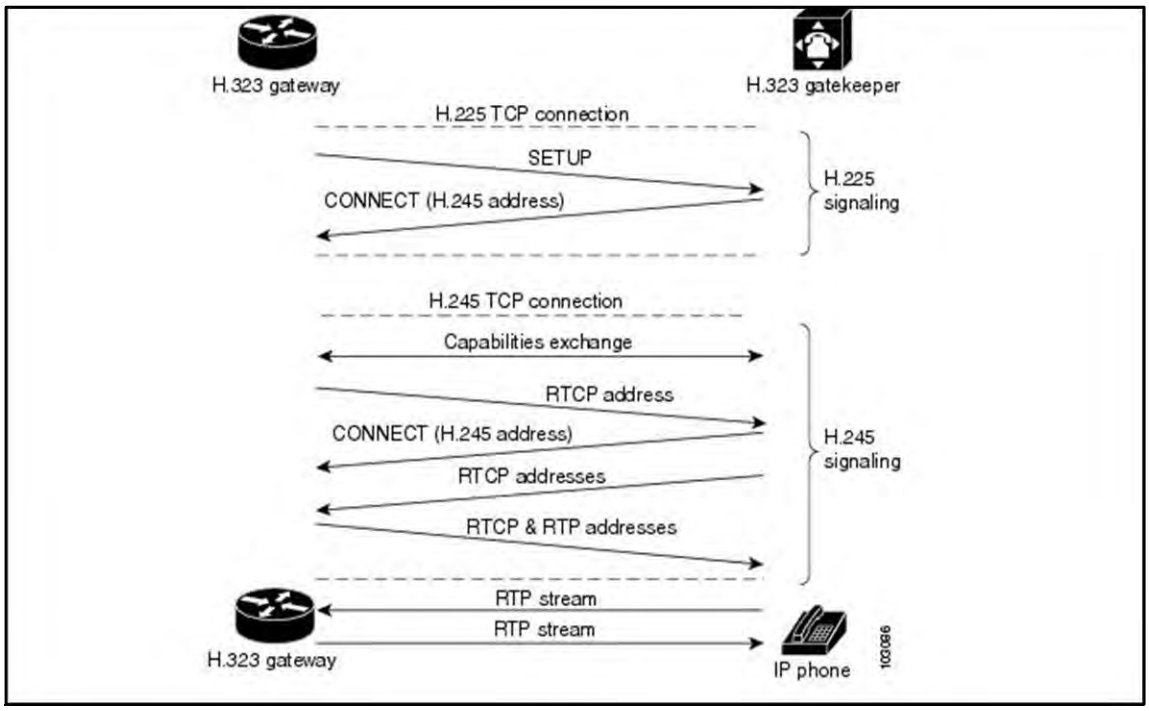

Figure 5. Typical H.323 Session Establishment, from [19]

Another of the most prevalent signaling protocols used in VoIP systems is SIP. Defined in RFC 3261, SIP is a text-based application protocol for VoIP signaling, specifically for call setup and tear down [20]. Being text based, it is similar to the popular Hyper Text Transmission Protocol (HTTP). This characteristic also makes it a very versatile and simple-to-implement signaling protocol. Some of the major text-based functions, or request types, of SIP are: INVITE, ACK, BYE, CANCEL, REGISTER, OPTIONS, SUBSCRIBE, and NOTIFY. The possible responses are categorized by series numbers corresponding to response types as follows: 100—informational, 200—success, 300—redirection, 400—client error, 500—server error, and 600—global failure. The reader may note that these are also very similar to the categorization of HTTP responses. SIP uses a process semantically similar to the transmission control protocol (TCP) three-way handshake. Much like H.323, SIP relies on other protocols to provide security for its transmissions.

SIP VoIP networks tend to be smaller in scale than H.323 networks, due to the simplicity of the underlying protocol. That is not to say that they cannot be scaled to

larger or multiple networks, though. To expand a SIP network, a SIP proxy is used. The SIP proxy performs many of the same functions as the H.323 gateway, gatekeeper and call manager. A typical SIP network and a message flow diagram are depicted in Figures 6 and 7.

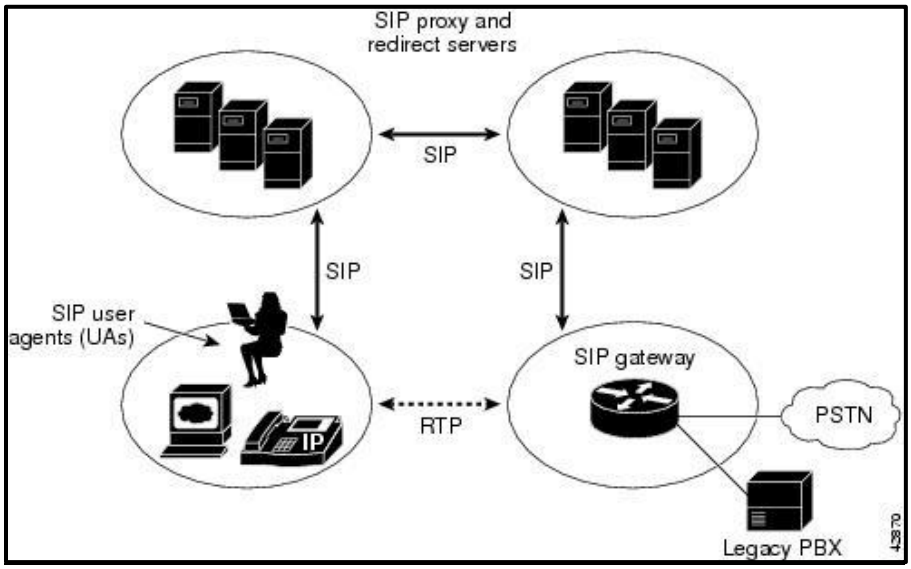

Figure 6. Basic SIP Network Diagram, from [18]

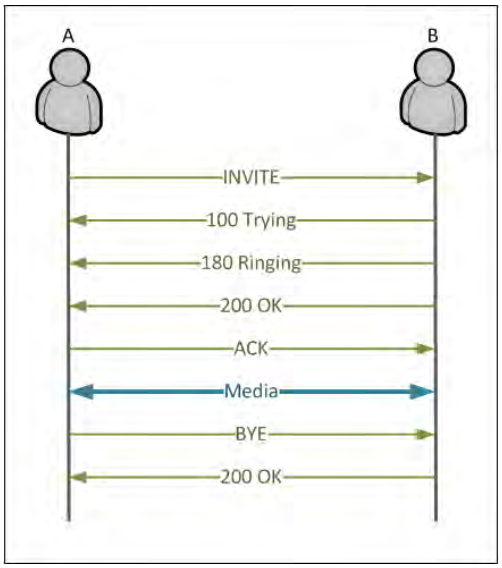

Figure 7. Typical SIP Session Message Flow, from [21]

In addition to the two major signaling protocols, VoIP relies on a slew of other application layer protocols for a variety of different functions. Some other signaling protocols (most of which are typically proprietary) used are Skype, the Inter Asterisk Exchange protocol, and the Microsoft Live Communications Server protocol. There are also protocols designed to specifically support SIP and H.323, such as Session Description Protocol for session description information, H.245 for call control, and H.235 for authentication security. Real-time Transport Protocol (RTP) is the primary protocol used for streaming the audio or video data over TCP or User Datagram Protocol (UDP). The details of RTP are described in RFC 3550 [22]. The RTP Control Protocol is another heavily relied on protocol [17]. It is used for quality control and tracks things like jitter, packet loss and synchronization data [17].

Not only does VoIP use IP protocols like TCP and UDP to transmit its information, it relies on other non-VoIP-specific protocols for support as well. These are protocols such as Domain Name System for address resolution, Dynamic Host Control Protocol for dynamic address assignment, and Trivial File Transfer Protocol to transfer configuration information. By relying on so many major IP-based protocols, VoIP services are affected by threats to these protocols as well as those specific to VoIP.

A typical VoIP system can consist of anywhere from two basic softphone end devices, to a suite of multiple gateways and networks that are integrated with a Private Branch Exchange (PBX) system bridging to the PSTN. The minimum VoIP components required to extend tactical radio communications are end devices, a proxy server, a gateway, and a form of inter-connection for radio integration. The end devices must provide services like push-to-talk and conferencing. The proxy server or call manager provides specific services to associated devices, call control, and various other functions. The gateway provides versatility to connect to other VoIP networks [17]. The ability to bridge calls to the PSTN is unnecessary; however, with the enormous interoperability of VoIP, this feature could be looked at in future research as a means to further expand system capabilities. Radio integration components are required to translate RF audio into

digital data. Finally, various other components such as gatekeepers, wireless access points, and IDSs, may be necessary depending on the specific systems, protocols used, and capabilities required.

3. VoIP Cyber Security

Similar to TCP/IP, the VoIP protocol has its own unique set of vulnerabilities, attacks targeting those vulnerabilities, risks, and mitigations for those risks.

a. Vulnerabilities

The protocols used in IP networks upon which VoIP relies are known to contain potentially exploitable vulnerabilities [23]. There are three major areas in a VoIP system that can create vulnerabilities: device or network misconfigurations, underlying OS and protocol vulnerabilities, and VoIP-specific vulnerabilities. All network systems can suffer either of the first two types of vulnerabilities; however, this research will focus on those specific to VoIP.

106 VoIP-associated vulnerabilities have been reported since 2002 by the DHS-sponsored National Vulnerability Database [23]. Compared to the entire list of over 64,000 vulnerabilities reported since 1999, this may seem insignificant. However, since most VoIP systems rely on the same set of protocols and standards as a typical network, in addition to those specific to VoIP, the number of potential vulnerabilities in a VoIP system are actually quite large.

One unique aspect of VoIP is that most of its functionality resides in the end devices, as opposed to servers. This means that security and authenticity must be pushed to, and focused on, the end devices. Another unique security aspect of VoIP is that it uses multiple port and protocol combinations, creating a much larger potential attack surface.

Many protocols used by VoIP have similar functionality to other major network protocols, which means there are similar types of vulnerabilities. However, with the technology's large need to provide QoS, the primary focus of VoIP-based attacks is denial of service (DoS) oriented. It does not help that DoS attacks are some of the easiest and most popular to employ.

The dynamic nature of VoIP makes it extremely difficult to protect using typical IP security methods. Therefore, various VoIP-specific security protocols have been created. H.235 is one of the few security protocols specifically for VoIP traffic. It provides only authentication protection. There are, however, issues with H.235's supporting protocols. Many of them use elements of variable lengths, and many VoIP systems are not programmed to have bounds checking on these elements. This leaves H.235 vulnerable to buffer overflow attacks leading to DoS, system crashes, and possible unintentional code execution [17].

b. Attacks

Many VoIP-specific attacks focus on the SIP, H.323, and RTP protocols. SIP and H.323 depend on trust relationships between nodes for security. They do not have any built-in authentication and rely on protocols like H.235, Transport Layer Security (TLS), and Internet Protocol Security (IPSec) for such security aspects. The protocol that carries the content, RTP, is connectionless and has no means of determining whether or not its packets are received. This makes it extremely difficult to track the state of ongoing conversations in VoIP systems, which creates a perfect situation for DoS attacks.

Popular DoS attacks can be targeted at both the stateful VoIP signaling protocols and the stateless media transfer protocols. The INVITE Attack [24] sends a large number of INVITE requests to a specific host in an attempt to both overwhelm the number of calls it can manage and to exhaust the proxy server's resources for storing information on all calls. The BYE Attack [24] sends false tear down messages to either party in a call in an attempt to make either one falsely believe the other is ready to stop transmitting, thus ending the call. The CANCEL Attack [24] is similar; however, it attempts to send a CANCEL response to the UAC before the UAS can respond, which prevents the call from being established. The Call Hijack Attack [25] sends a false re-INVITE message to the caller with a new IP and port configuration, redirecting the establishment of the call to a potentially malevolent party, in an attempt to kill or intercept the call.

Similar to the INVITE Attack, there are also many VoIP-based DoS flooding attacks. These attacks aim to exhaust the resources of either the server, end device, or the

path between them. The Reflector Attack [24] (similar to a Smurf Attack) uses zombie computers to send spoofed messages to open SIP servers with the victim as the source, thus having the servers flood the victim with false responses. RTP Flooding [24] is an extremely popular and easy means of denying service to a system due to RTP's stateless nature. This attack simply uses brute force to send as many RTP packets to the target as possible in an attempt to exhaust bandwidth and other resources. Not only does this deny the target, it denies or degrades the connections of other users on the network, especially those with VoIP connections requiring little to no delay. TCP, UDP, and other IP-based flooding attacks can hurt the availability of VoIP connections as well.

Flash crowds can also create major flood-like problems for VoIP. A flash crowd occurs when a large number of legitimate users attempt to access the VoIP server or services at the same time. The primary issue is that it becomes extremely difficult for the VoIP server to distinguish between real traffic and traffic from a flooding attack [26].

There are a number of other attacks, not necessarily DoS-based, specifically targeted against VoIP as well. These attacks range from simple scanning and enumeration to actual manipulation of the data being transmitted. The previously mentioned Call Hijack Attack, for example, can be used for more than just denial. By redirecting the caller to a malicious callee, a third party can reestablish the call and listen in without the caller ever knowing. Similar to the Call Hijack Attack, Registration Hijacking [25] can place a false callee into the conversation. However, it does this by convincing the registration server to replace the real callee's address with its own. Much like other major protocol attacks, VoIP attacks can falsify data for financial gain. The Billing and Toll Fraud Attacks [24] send a false BYE message to a proxy server to make it believe, and record, that the call has ended, when in fact it has not ended.

One VoIP-specific attack that is similar to other telecom and IP-based attacks is called Spam-over-Internet-Telephony (SPIT) [26]. SPIT is the VoIP version of spam (i.e., unsolicited emails), and telemarketing or political action calls. Instead of receiving a barrage of unwanted e-mails, the victim receives a number of unwanted VoIP phone calls.

A number of tools have been developed to carry out such attacks, both VoIP and non-VoIP specific [27]. These tools and their functions include but are not necessarily limited to:

- Sniffing (e.g, VOIPong, VoMIT, SIPomatic)
- Scanning and enumeration (e.g., SIP-Scan, SIPcrack, SMAP)
- Packet creation/ flooding (e.g., SIPNess, SIPBomber, RTP Flooder)
- VoIP fuzzing (e.g., Asteroid, PROTOS, Sip-Proxy)
- VoIP signaling manipulation (e.g., IAXAuthJack, IAXHangup, SIP-Kill)
- VoIP media manipulation (e.g., RTP MixSound, RTPInject, RTPProxy)

Various other tools exist as well from those that carry out dictionary attacks to those that are specifically for spamming. Although not unique to VoIP data, tools like Wireshark and nmap are also quite popular. It is worth noting that in addition to malicious use, many of these tools can also be used for things like penetration testing in order to find vulnerabilities in a VoIP system before they are exploited.

c. Risks to the Navy

As new technologies are deployed, new ways of exploiting them for various malicious activities are also developed. Defending against these new attacks and fixing the vulnerabilities will forever be a burden to the Navy. Incorporating VoIP technology into Navy systems creates the potential for new exploitable vulnerabilities within those systems, thus increasing the risks to those systems overall. Aside from the known vulnerabilities related to the technology, introducing an Internet-connected VoIP network into the tactical communications realm could create some unique exploits of its own.

Integrating VoIP systems with afloat radio communication systems would introduce new vulnerabilities into tactical communications. It would create a potential avenue for adversaries to eavesdrop into tactical warfighting decisions by call hijacking and registration hijacking. It would provide yet another way to deny communications altogether, through VoIP DoS and call flooding. Finally, it could create another avenue for degrading communications with CANCEL attacks, VoIP fuzzing, and many of the other methods listed above.

The Navy has been taking steps to move away from increasing the risk factor of its systems and towards reducing risk by all means necessary. The Navy has initiated efforts for improvement in mitigating threats to critical command and control systems, such as command and control in a denied or degraded environment and electromagnetic maneuver warfare. These efforts seek to enhance the Navy's ability to operate in a contested environment. Opening more avenues for attack by incorporating exploitable technologies into existing systems is counter to such goals.

With the potential to create so many new hazards, one might jump to the conclusion that a risk such as VoIP should not be adopted. However, even though VoIP does create new threat vectors, the risks are minuscule in comparison to the advantages it brings. VoIP threats only make up approximately 0.2 percent of the known vulnerabilities in all networked systems today [23]. Many of the vulnerabilities in VoIP are some of the same that are being defended against through various security systems and best practices already in place. In 2009, the CNO issued a mandate stating that we "must be organized to achieve the integration and innovation necessary for warfighting dominance across the full spectrum of operations" [28]. Like any new technology, VoIP does carry risks; however, through mitigation, this technology may be harnessed to help the Navy achieve desired warfighting dominance.

d. Limiting the Risks (Mitigations)

Like most protocols, VoIP was not built with security in mind, and therefore must rely on other protocols to provide it. As mentioned earlier, protocols like H.323 and SIP rely on other protocols for security, such as H.235 and TLS. Aside from leveraging more protocols, many types of VoIP intrusion detection and intrusion prevention systems (IDS and IPS) have been created. Many of these systems have been geared towards mitigating DoS and flooding attacks as well.

Protocols like TLS and IPSec are available for authentication and integrity security. Unfortunately, these protocols require additional processing, and thus can slow transmissions and effect voice quality. Guo et al. developed a hierarchical data security

protection scheme that can maintain voice quality while providing additional security [29]. This scheme is capable of providing both data encryption and error recovery.

Many VoIP intrusion systems provide security through measures that are not built directly into the protocol. These systems include: VoIP intrusion detection systems (vIDS) with protocol-specific detection methodologies, VoIP flooding detection systems (vFDS), VoIP overload prevention mechanisms, and various other intrusion prevention systems tailored for VoIP traffic [26]. They are categorized as either stateful or stateless, and behavioral- or anomaly-based. Behavioral-based systems have low false positives but often fail to identify new attack types; whereas, anomaly-based systems can detect new attacks but generate a higher number of false positives [26].

Some of the vIDSs are just normal IDSs that have been put on a VoIP network or designed to only look at VoIP traffic. The stateful vIDS suggested by Wu et al. is a good example [30]. This anomaly-based vIDS determines connection states by gathering protocol-dependent information from packets, and matches the information to predefined rules. Available rules might include ones providing alerts when there is an irregular sequence number on consecutive RTP packets or when a specific high number of SIP INVITE messages have been received within a certain period of time.

The vIDS suggested by Sengar is much more unique and specifically tailored towards the synchronization of VoIP traffic [24]. This behavior-based vIDS uses different protocol state machines to gather information on the state of a connection as well, but instead of just matching the information to rules, it compares synchronization information between the protocols to determine if the traffic is performing as designed. As an example, if a SIP BYE message is sent to end a call while RTP voice traffic is still being sent, the vIDS will detect that the conversation is no longer in-sync and an alert will be triggered. This technique can detect CANCEL, Call Hijack, and RTP flooding attacks, as well. Sengar's vIDS does not introduce significant processing delays, call delays, or false positives [24].

Similar to circuit switched PBX systems, overloading and Call Flooding attacks are some of the most damaging and difficult to defend-against a VoIP system can

experience. A SIP proxy can maintain the state of an INVITE request for up to 3 minutes [26]. This leaves an extremely long window to be abused by potential flood attacks. Traditionally, systems from companies like Cisco and Oracle have used rate limits to drop calls when the traffic volume is too high. This is simple and effective; however, it has the potential to drop legitimate traffic, too.

Many methods have been suggested for distinguishing flooding from flash-crowds. Besides just using a single predefined rate limit, a more dynamic "safe limit," which is governed by factors, such as server type, the number of subscribers, peak hour call rates, and many other parameters can be used [26]. Also, a flash crowd can be distinguished from a DoS attack by a much slower buildup of INVITE/ACK messages. Flash crowds also retransmit any unanswered INVITE requests at protocol-compliant back-off timer limits, whereas flood attacks do not. Finally, non-malicious INVITE requests will be sent to UAs with real addresses, while DoS attacks tend to be sent with bogus information.

As DoS attacks have become more sophisticated, many new and innovative methods for detection have been developed as well. One such procedure involves comparing response and request rates with their long-term averages [31]. Sengar has also suggested a new methodology for detecting and preventing VoIP DoS [24]. Sengar's vFDS looks for abnormally high amounts of RTP voice traffic in relation to the SIP session data being sent. He also has methods for overload prevention that work by randomly dropping a set of INVITE packets in an attempt to see if they are legitimate, or if they are just being recreated to flood a system. These methods put little drain or delay on the VoIP network upon which they are implemented.

e. Limiting the Risks through Network Design

One simple way to secure a VoIP network is to air-gap it, or segregate it from other networks. This may be feasible with a small infrastructure, but when using VoIP across multiple networks or adding VoIP to an existing network, this is not physically possible. VoIP traffic can, however, be logically separated from normal traffic by using a virtual local area network (VLAN) or similar technique. Secure voice over IP (SVoIP),

which uses secure phones to encrypt and transmit the conversation from end-to-end can also be used to achieve this segregation. Another technique is voice over secure IP (VoSIP) which uses secure devices elsewhere in the network to provide encryption (see Figure 8). An example would be using a VoIP phone on the secret IP router network (SIPRNet) to talk to another VoIP phone on the SIPRNet. Here the normal network encryptors would provide the segregation.

Figure 8. SVoIP vs. VoSIP Comparison, from [32]

f. Limiting the Risks through Operational Policies

Using a more secure protocol or adding a vIDS to a network will not provide adequate VoIP security alone. Like any hardened network, smart security practices and policies are also required. VoIP systems can have very similar policies to other major network systems ranging from log monitoring and penetration testing requirements, to well-defined implementation of specific VoIP protocols and protection against specific attacks. There are guidelines from credible organizations with suggested VoIP policies and procedures [33], [34].

Since RTP is connectionless and extremely difficult to protect with traditional IDSs, enforcing smart policies when implementing the protocol can help provide some

security. Correct implementation of secure RTP (SRTP) is one such policy [35]. If properly implemented, SRTP can provide confidentiality, message authentication, and replay protection, but key distribution in SRTP must be carefully managed in order to maintain confidentiality. Also, the framework must be able to upgrade to new cryptographic algorithms in order to avoid potential vulnerabilities in those that become outdated.

There are various other VoIP- and non-VoIP-specific policies that can help maintain security. Ahson and Ilyas suggest the use of a Security Certificate Authority to verify VoIP security policies, much like a typical certificate authority verifies digital signatures and certificates [26]. Blacklists and white-lists based on caller reputation can be implemented in order to prevent VoIP SPIT traffic. There are also many generic network security policies and best practices that should be followed on a VoIP network such as changing default passwords, using an IDS or IPS, regularly patching systems, and following vendor checklists.

Many national organizations have published their list of VoIP policies to provide the public with a baseline for securely implementing VoIP technology. Cisco's *Unified Communications Manager Security Guide* and information assurance reports are an excellent resource [33]. Also, the DOD Information Assurance Certification and Accreditation Process (DIACAP) Package and DIACAP Scorecard can help ensure a DOD organization's VoIP system is in keeping with current security practices [34].

A more risk-oriented process, known as the DOD Information Assurance Risk Management Framework is currently replacing DIACAP [36]. However, VoIP guides are not quite the same as other available security publications, as many are old, outdated, and somewhat inadequate. One of the most inclusive and in-depth VoIP security publications available is National Institute of Standards and Technology SP800-58 (*Security Considerations for Voice over IP systems*) [37]. Although it is extremely detailed, the last time it was updated was in 2005. The problem of outdated guidelines includes such publications as the Federal Deposit Insurance Corporation financial institution letter 69-2005 on *Voice over Internet Protocol Guidance on the Security Risks of VoIP* from 2005

[38], and the National Security Agency (NSA) Report Number: I332-009R-2006 on *Recommended IP Telephony Architecture* from 2006 [39].

III. EXTENDING VOIP TO COMMUNICATIONS CHALLENGED AREAS

This chapter identifies potential ways in which VoIP can be implemented to best extend tactical communications, particularly for large afloat units. Specific areas associated with this are: VoIP QoS, network and radio integration, and reaching the areas that are not easily accessible. Many of these techniques can be used individually or in conjunction with one another to provide reliable, high-quality tactical communications.

A. VOIP QOS

One of the most sought after features of any VoIP system is quality of service. Excellent QoS is one of the main reasons that VoIP technology has become so widespread. VoIP signals are able to achieve such outstanding qualities through the use of the codecs. A codec, which simply means coder-decoder, is a program that encodes and decodes (digital to analog or analog to digital) a signal for efficient transmission. In VoIP terminology the term codec describes the standard used to compress the signal for transmission. As with any compression technology, codec standards must balance a tradeoff between payload size, speech quality, and processing power and speed [40].

There are numerous different codec standards; some are proprietary and others are open source. Some of the most commonly used open source standards are G.711, G.729, and G.723.1. G.711 offers good quality with high bandwidth requirements, but requires no compression [40]. G.729 provides medium quality with low bandwidth requirements but requires more processing [40]. G.723.1 offers only medium quality with fast encoding and decoding and also requires a large amount of processing power [40]. Other available open source standards include G.728, iLBC, and Speex [41]. Available proprietary standards include Skype's SILK and Microsoft's RTAudio [42]. Figure 9 lists some of the most commonly used standards and their specific data and quality parameters.

VOIP-SIP.ORG Codec and Bit Rate	Sample Size (Bytes)	Sample rate (ms)	MOS Quality	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80 Bytes	10 ms	4.3	160 Bytes	20 ms	50	**87.2 Kbps**
G.729 (8 Kbps)	10 Bytes	10 ms	3.7	20 Bytes	20 ms	50	**31.2 Kbps**
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	**21.9 Kbps**
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	**20.8 Kbps**
G.726 (32 Kbps)	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	**55.2 Kbps**
G.726 (24 Kbps)	15 Bytes	5 ms	---	60 Bytes	20 ms	50	**47.2 Kbps**
G.728 (16 Kbps)	10 Bytes	5 ms	3.61	60 Bytes	30 ms	33.3	**31.5 Kbps**
G.722 (64 Kbps)	80 Bytes	10 ms	4.13	160 Bytes	20 ms	50	**87.2 Kbps**
iLBC (15.2Kbps)	38 Bytes	20 ms	4.14	38 Bytes	20 ms	50	**38.4Kbps**
iLBC (13.33Kbps)	50 Bytes	30 ms	---	50 Bytes	30 ms	33.3	**28.8 Kbps**

Figure 9. VoIP Codec Standards Statistics, from [43]

Quality of service in a packet switched network is somewhat different from that in a circuit switched network. Circuit switched network resources are allocated (dedicated) to the call. If insufficient resources are available when the call is requested the call is rejected. However, in a packet switched network, the resources (primarily bandwidth) are shared and can change throughout the duration of a call. Since VoIP is designed to run over packet switched networks, it has to share resources with everything else on the network and thus has a greater potential for transmission delay or even total denial of service. The three major issues this raises for voice quality in VoIP are latency, jitter, and packet loss. Latency is the delay in packet transmission between call-end-points [17]. Jitter is caused by varying latencies during a conversation [26]. Packet loss can occur for various reasons, but the most common culprit is congestion within the network [26]. These are three of the most important factors to reduce for any reliable packet switched network, not just VoIP.

In order to have any merit, VoIP must offer the same, if not better QoS as the PSTN. To do so, latency, jitter, and packet loss must be kept below an intolerable level. With typical VoIP packets containing 20 milliseconds of voice on average, Porter suggests that latency should not be allowed to go above 150 milliseconds [17]. Ahson and Ilyas state that the variation in jitter should stay between one and 50 milliseconds,

while packet loss should stay below three to five percent [26]. If a VoIP system cannot maintain these standards, its fidelity will be dramatically reduced, and one may be reluctant to use it at all.

1. Shipboard VoIP QoS

The correct prioritization of applications is vital for successful communications. As an example, the Navy's Common Access Card management system, Real-time Automated Personnel Identification System (RAPIDS), experienced numerous communication issues when it was first deployed onboard large-deck ships [5]. These issues were primarily due to incorrect prioritization labels of the system's network traffic. Specifically, the RAPIDS priority was too low to efficiently deliver its traffic on and off the ship. This, in turn, caused most of the RAPIDS traffic to be dropped and lowered network performance overall. The issue was resolved after laboratory testing revealed a more efficient higher prioritization label for the system.

a. ADNS QoS

To provide QoS, ADNS implements an all-IP based communications solution by using Cisco Weighted Random Early Detection (WRED) to prioritize TCP/IP traffic and by rate limiting UDP/IP traffic [5]. WRED can slow low priority traffic through the use of a rate control mechanism specific to TCP traffic, to provide additional bandwidth to high priority traffic [44]. Since WRED depends on the underlying congestion control mechanism employed by TCP, it does not address congestion issues caused by UDP traffic.

b. ADNS UDP and VoIP QoS

Since UDP traffic, such as VoIP, is connectionless, it is much more difficult to regulate the bandwidth that it consumes. In fact, "[t]here is no direct way for an IP network to regulate the flow of UDP" [5]. Specifically, the Type of Service field of the TCP header that is used to assert routing priority and preference (i.e., reliability, throughput, or delay) is not available with UDP. Thus, UDP traffic must be categorized

by some other non-standardized method, such as either IP and port number pairs or fields added to the application data content encapsulated by the UDP header.

ADNS is currently configured to provide QoS for UDP traffic through a pre-assigned allocation of bandwidth. This sets a limit on the number of UDP sessions allowed through the network. Any UDP traffic that surpasses the limit is dropped. This simply prevents the non-prioritized UDP traffic from overwhelming the prioritized TCP traffic.

c. ADNS QoS between LANs

Afloat networks support the use of multiple LANs, known as enclaves, each with a separate level of security. ADNS provides the management of off-ship bandwidth for the separate enclaves through the use of class based weighted fair queuing (CBWFQ) on its Cisco routers [45]. CBWFQ is a feature that provides bandwidth management between different user-defined classes of traffic. It works by giving one traffic level priority over another, and by loaning out excess bandwidth from the higher classes to the lower classes. This prevents a single enclave from using all of the bandwidth available.

d. ADNS QoS within LANs

ADNS is primarily configured to provide QoS for internetwork communications between the ship's LANs and the multiple paths off-ship. It also has the capability to provide QoS for intra-network communications within a LAN, but this capability is not currently used on afloat networks.

Effective bandwidth management within a LAN can significantly improve overall network performance by prioritizing application-specific traffic in a congested or degraded environment. This allows for limited high priority emails, or even high priority VoIP traffic to flow through a network during times of high usage or limited availability.

Internetwork bandwidth management can be achieved in the same way the Blue Coat Packet Shaper currently uses WRED to prioritize traffic through the rate control marker [5], [7]. An application traffic management device can control and monitor prioritizations across multiple applications, much like an application-level firewall can

filter traffic based on the specific protocol being used. It need not understand the types of traffic within every application, but will only need to understand the types of traffic that will benefit from detailed prioritization based on the source and destination IP address and transport layer port entities.

B. RADIO INTEGRATION

Extending tactical communications from a radio to a VoIP network is not a small task. Typical radios are not configured to interact with VoIP and operate according to different non-interoperable protocols and standards. In order to translate these signals into something that is compatible with a VoIP system, they must be properly converted. Since most of the Navy's afloat platforms are currently being upgraded to the DMR, this research will examine its potential for VoIP integration.

The DMR has four digital data ports, one for each channel, that share an output data switch. These ports use the TIA/EIA-530 interface protocol [46]. EIA-530 is a Telecommunications Industry Association standard for balanced serial interfaces typically using a 25-pin, "D-type," connector that is commonly used for synchronous signaling over long cable runs. TIA/EIA-530 signaling rates range from 0.020 Mbps to 2 Mbps. The DMR also has four analog data ports that are used for tactical voice. These four lines lead to an analog audio switch. The four digital data ports and the four analog audio ports could be used to send either digital or analog audio to a VoIP system.

Since VoIP systems do not interact with these types of analog audio signals, a converter is necessary to translate the analog audio into a VoIP-compatible signal. The Cisco Land Mobile Radio (LMR) Gateway was designed for this purpose [47]. It takes an analog audio signal on a voice interface port and converts it to RTP audio packets for digital transmission. Each voice interface port corresponds to a specific multicast IP address so that a signal can be uniquely identified on the network. A VoIP system can be configured to associate these multicast addresses to a specific VoIP number or even a conference number to communicate with everyone on the network [47].

Cisco is not the only company that has produced a solution for communicating between VoIP systems and radios. Orion Systems' RCS-4-IP and Omnitronics's IPR100

VoIP adaptor are just two examples of systems that bridge the VoIP/RF gap. These systems are less expensive and intricate than a typical Cisco VoIP system; however, they do not offer the same expandability, reliability, and capability as that offered by a Cisco system [48], [49].

C. NETWORK INTEGRATION

Integrating a VoIP capability with an existing network may require some limited equipment addition, depending on whether or not a VoIP capability already exists on the target network, along with making some software and network configuration changes. The primary decision for afloat platforms, particularly those in the Navy, is whether or not to integrate a new VoIP system onto a pre-existing network, or to configure the current VoIP system to transmit tactical communications. The latter would be the logical choice, since it would not involve adding an additional VoIP system to a network like CANES that already has one.

CANES is currently configured with Cisco-based handsets, call managers, and gateways. Little configuration will be required to pass tactical communications through the CANES network, although an IP Interoperability and Collaboration System (IPICS) server would need to be added to the network [50]. The IPICS server will allow virtual push-to-talk conferencing, so that conference channels can be established that will simulate radio communication circuits. Also, the VoIP handsets will need to be configured to get the necessary IPICS services.

If a separate VoIP system is used for tactical communications, more equipment and configuration will be required. An additional call manager, IPICS Server and possibly new VoIP handsets will be necessary to incorporate a different system. The additional equipment and configuration will incur significant implementation costs that may outweigh any benefits of a dedicated system.

D. COMMUNICATIONS CHALLENGED AREAS

After tactical radio communications are integrated into the network in VoIP format, the audio packets must then be able to reach the intended UA, who might be a

user in a location that typically does not have network access. These areas include the well-decks of amphibious transports, far-off engineering spaces, and other areas that were not envisioned to have network access but could benefit from staying informed regarding the ship's current tactical and operational status. A number of systems and technologies are available to provide network access to these areas, including Wi-Fi access points and handsets, Cellular, Secured Bluetooth, and the Common Optical Distribution Architecture (CODA) being engineered by SPAWAR Systems Center San Diego [51]. An analysis of Wi-Fi, Cellular and the CODA wireless systems is provided in the sections below.

1. Wi-Fi

Wi-Fi has evolved into one of the most common mechanisms for connecting mobile devices to a network. It provides a flexibility that wired networks cannot and allows network access from anywhere within a certain radius without cumbersome cable runs.

Cisco has conducted an assessment on the ability to run VoIP through wireless networks onboard Navy ships with results demonstrating the existence of potential coverage and quality issues [52]. Wi-Fi does suffer from many of the same issues as wired networks as well as some unique issues. For instance, the previously discussed QoS issues of jitter, delay, and packet loss must be addressed. Also, Wi-Fi relies on IP and is thus susceptible to many of the same attacks as a wired network. Further, it opens avenues to new attacks, such as spoofed traffic that fails a wireless gateway's integrity checks in order to make the gateway refuse a real UA for a certain period of time. Wi-Fi also requires efficient use of the electro-magnetic (EM) spectrum since it does not traverse a dedicated physical path. Another unique pitfall of Wi-Fi is that coverage is heavily dependent upon power available. These factors must be properly accounted for if Wi-Fi is to be a viable option for reliable communications.

802.11e is a Wi-Fi standard that was developed to provide improved QoS through four tunable parameters: Arbitration Inter-Frame Spacing (AIFS), Contention Window minimum (CWmin), and Contention Window maximum (CWmax), and Transmit Opportunity (TXOP) [26]. AIFS helps QoS by shortening or lengthening the amount of

time a node must wait before transmitting its next frame. CWmin and CWmax are used to adjust the period that a station must wait if the channel is busy, thereby allowing for the optimization of the carrier sense multiple access with collision avoidance protocol for the specific wireless environment in which the system is employed. The TXOP parameter sets the amount of time that a station is allowed to transmit. Ahson and Ilyas suggest that "in order to reduce delay the AIFS parameter should be the smallest possible" [26]. They also suggest that the TXOP should be minimized and CWmax should be equal to CWmin in order to reduce queuing delays.

Numerous studies have been conducted on the best way to transport VoIP over Wi-Fi. These have been performed on all iterations of the 802.11 standard, from 802.11a up to 802.11n. Most tests use the G.711 codec, since it produces the largest frame size as a worst case scenario. Researchers like Jeong et al. using the 802.11b standard, found that it could only handle five calls without major quality degradations [53]. Ahson and Ilyas found that after properly implementing the 802.11e standard, the maximum number of calls went from approximately eight up to eleven [26]. By using one of the most recent Wi-Fi standards (802.11n), Krym found that a system could maintain anywhere from 40 to 106 VoIP sessions using the G.711 codec with 240-byte voice frames [54]. Given these results, VoIP over Wi-Fi appears capable of supporting the tactical communications requirements on naval vessels.

Previous VoIP over Wi-Fi studies primarily focus on the 802.11b, g, and n standards with very few analyzing the newest Wi-Fi standard, 802.11ac. This standard was approved by the Institute of Electrical and Electronics Engineers in January of 2014 [55] and offers numerous enhancements over previous versions. 802.11ac uses a large channel bandwidth (80 MHz and 160 MHz), higher order modulation, and an increased number of spatial streams to achieve increased data rates of up to 3.477 Gbps [56]. This is a vast improvement over previous standards. Since 802.11ac is designed with these advancements over previous Wi-Fi standards, it will be looked at as a potential use case for this research.

One potential Wi-Fi option for extending tactical VoIP communications would be to utilize one wireless access point (WAP) connected directly to wireless VoIP phones.

This would require one WAP directly connected to the ship's network, near the area that needs to receive the extended communications (i.e., the communications challenged area of the ship). Wi-Fi enabled VoIP phones could then be used to connect directly to the WAP on the ship's network. This option is addressed during the testing portion of this thesis.

The CANES Network is already equipped with WAPs that provide a secure wireless network. Users are required to have a National Security Agency High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Standard-compliant device in order to connect to the secure network [5]. Although the capability is present, wireless communications afloat are still not the norm. They have been tested on Navy networks since 2009 but are still not being used regularly because of the potential associated security risks [57]. With so many concerns, the technology may not be enabled on CANES for some time.

Many companies are now starting to provide wireless VoIP handsets as an option for connecting directly to a WAP. Two of the more popular early ones were CISCO's Wi-Fi-only handset and Polycom's SpectraLink Voice Priority handset. CISCO's Wi-Fi-only handsets use a proprietary protocol for communications to various CISCO WAPs. Many of CISCO's new model VoIP phones now come with wired and wireless variants as well. The Polycom SVP also uses a proprietary protocol, but its protocol was developed to handle wireless QoS issues [58]. Many other wireless handsets are available today and are excellent options for wireless VoIP communications.

2. Cellular

With the development of 3G and 4G technologies, reliable cellular IP data transmission has become very popular, and it is now possible to use this technology to stream all types of multimedia to mobile devices. In particular, sending VoIP data is becoming widespread, offering cellular customers the ability to make wireless calls anywhere on the globe through a data plan while avoiding the need to use costly "international minutes." This same technology can be implemented in a shipboard

environment to wirelessly extend tactical VoIP communications, particularly in international waters where frequency licensing is not an issue.

The most current cellular standards are 3rd Generation Partnership Project (3GPP) and 3GPP2, also known as 3G, LTE and Ultra-mobile Broadband, also known as 4G. 3G uses standards such as Evolution Data Optimized to provide high-speed packet delivery while 4G uses technologies such as Orthogonal Frequency Division Multiple Access [26].

In order to combat many of the same QoS issues that affect other wireless technologies, cellular has developed unique ways for improving RF capacity and wireless performance. The Enhanced Variable Rate Codec was created to combat the large fluctuation in cellular network activity. It uses a rate reduction mechanism to alter its encoding rate based on talking activity [26]. Another QoS improvement for cellular is known as hybrid automatic repeat request, which aims to increase transmission efficiency. With so many enhancements to QoS and its growing popularity, cellular is poised to be an excellent way to pass VoIP traffic to specific locations.

3. Common Optical Distribution Architecture

There are numerous other wireless technologies that may offer potential to extend shipboard networks such as WiMAX, Bluetooth, and infrared [51][2]. Systems are being created that incorporate various combinations of these technologies to provide an integrated solution. The Navy has been developing one of these systems for shipboard use, called the Common Optical Distribution Architecture (CODA).

The CODA was designed by SPAWAR System Center Pacific's shipboard wireless communications division, to consolidate numerous wired and wireless media onto a single network. Instead of having a segregated group of networks for various systems, CODA consolidates them onto one network through the high capacity capabilities of fiber optics. Various systems data can be fed into the CODA head end and

[2] CODA is currently a developmental Navy system. It is not yet a program of record. The facts provided in section "c" are from the October 2013 CODA Executive Brief, and statements taken from system developers Brian Lovell and Rowell Bacani at SPAWAR Systems Center Pacific. [51]

then seamlessly delivered to multiple endpoints throughout the ship at near light speed. Each end point is currently being designed to deliver the following types of signals: 4G LTE, Digital Enhanced Cordless Telecommunications wireless phones, radio frequency identification, Wi-Fi, IP video, UHF RF, IP telephony, and more.

CODA offers numerous benefits by incorporating many systems into one medium rather than having each one segregated. Some of these advantages are increased power efficiency, RF flexibility, better security, scalability, and space and weight reductions. Its modular design makes it easy to incorporate current and legacy technologies, as well as expand to those that are developed in the future. Further, the proposed switched fiber infrastructure offers redundant paths to ensure survivability. CODA would be an excellent solution for extending tactical VoIP communications within afloat platforms.

E. EXTENDING VOIP SUMMARY

The technologies discussed above are all capable options for passing VoIP data to communications challenged areas onboard ships without requiring additional wiring. Each has numerous benefits that can be exploited. Wi-Fi is already commonly used to efficiently transmit VoIP data and is straightforward to implement in standard IP networks. Cellular networks are increasing in popularity in the consumer market, and offer numerous technologies for improved QoS. Systems like CODA can offer numerous options for IP data transmission, and are presently being developed for shipboard deployment.

The next chapter provides a proof-of-concept design and test strategy to explore the VoIP utility for wirelessly extending shipboard communications. It will compare the above mentioned 802.11n and 802.11ac wireless protocols, as well as the wired Ethernet link layer protocol.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TEST DESIGN AND EXECUTION

This chapter identifies the architecture used, and the tests conducted to assess the feasibility of extending tactical communications through secure wireless VoIP networks. The tests were designed to not only assess the capabilities and limitations of these networks, but to evaluate the overall performance of the 802.11n and 802.11ac Wi-Fi protocols as well.

A. DEMO TEST BED

The test bed consisted of three major sections: the client, the access point, and the server. The client machine was used to simulate an end device connecting to a VoIP network. The access point acted as the means of routing VoIP communications from the client to the server. Finally, the server was used for multiple functions throughout the testing including VoIP call manager, VoIP IDS, traffic generation, and traffic analysis. Figure 10 depicts the three major components and their functions.

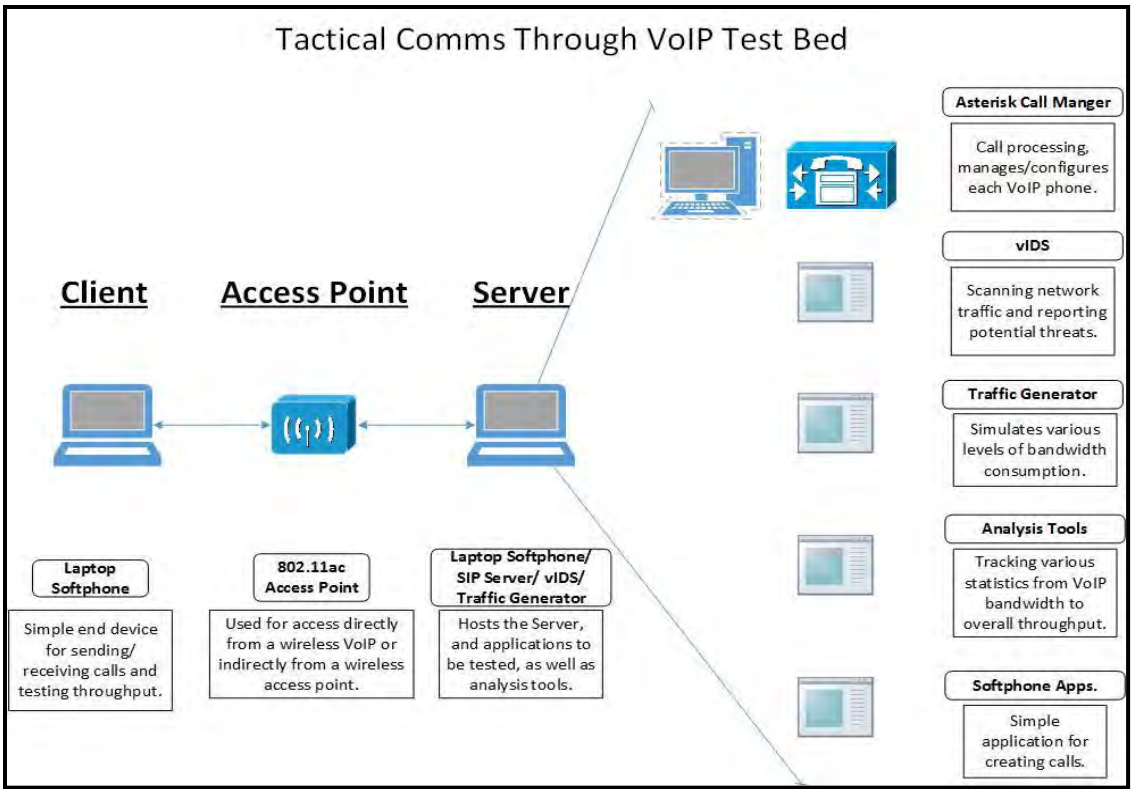

Figure 10. Logical Design of VoIP Test Bed Components and Functions

The client machine was a Hewlett-Packard Pavilion dv7 with a 2.27 GHz Dual Core Intel i5 processor and 4 Gigabytes of random access memory (RAM) running the Windows 8.1 64-bit operating system. The two main applications used for testing were JPerf 2.0.2 and Zoiper 3.2. JPerf is a network performance measurement and traffic generating tool. Zoiper is a popular VoIP softphone that supports various VoIP features, protocols, and codecs.

The access point was a Linksys WRT1900AC Wireless AC Router. The following link protocols were used in the experiments: wired Ethernet, 802.11n, 2.4 GHz 802.11ac and 5GHz 802.11ac. The Linksys Smart Wi-Fi application was used for configuring the router's wireless signal properties, wireless security properties, and various other settings.

The VoIP server was a Dell Latitude E6510 with a 1.60 GHz Quad Core Intel i7 processor and 8 Gigabytes of RAM running the Windows 7 64-bit operating system. The VoIP softphone applications used were Zoiper 3.2, X-Lite 4.7.0, and SJphone 1.65.2637. Network traffic analysis was conducted using Wireshark 1.10.8. JPerf 2.0.2 was used for

network performance monitoring and traffic generation with the client machine. Finally, VMware Workstation 9.0.4 was used to create the virtual machine which hosted the VoIP Proxy Server and IDS.

Trixbox 2.8.0.4 was used as the virtual VoIP Proxy Server. Trixbox is a complete VoIP phone system package that includes CentOS Linux, MySQL, a web server, an Asterisk PBX, and various other applications. The K Desktop Environment was installed for ease of access. Snort 2.9.6.2 was also installed on the virtual machine to function as the vIDS. The Snort application was put in Network Intrusion Detection System Mode with the packet display, logging, and alert options enabled whenever it was in use.

B. TEST DESIGN AND EXPECTED RESULTS

Seven sets of tests were performed upon VoIP traffic within four different link protocols in an attempt to determine the capabilities, limitations, and feasibility of each.

1. Network Baseline

Before starting the various VoIP tests bellow, it was necessary to observe how the test network performed without any VoIP calls being processed. This created a baseline for comparing the network behavior and performance of VoIP traffic. Wireshark was used to capture and measure the average network traffic (i.e., bits per second) during various 30-second intervals in which no VoIP data was transmitted.

Since the network baseline test was only analyzing non-VoIP traffic and there was not a lot of network activity required when not processing VoIP calls, it was expected to show very little traffic overall.

2. Network Throughput

This test was designed to examine the overall throughput of the various link protocols within the network. This showed the capabilities and limitations of the different types of transmission media. In this test four types of link transmission protocols (Ethernet, 802.11n, 2.4 GHz 802.11ac, and 5 GHz 802.11ac) were examined. JPerf was used to send as many TCP/IP packets from client to server, as possible. The specific JPerf

settings used for the throughput test were as follows: one parallel stream, 30 second intervals, TCP protocol, 64 KB buffer length, 56 KB TCP window size, 1 KB max segment size, TCP no delay unchecked and all default IP layer options. The test was run on each link protocol, until a consistent average throughput was obtained.

Since nothing else was supposed to be happening on the network, this test was expected to show results with numbers very close to the maximum capacities of the four different link protocols. Wireless protocols can be affected by numerous environmental variables which would likely affect the tests as well. This expectation is captured well by the Linksys wireless products disclaimer that states:

> Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions [59].

Consequently, the test network would likely have shown rates lower than each link protocol's stated maximum.

3. VoIP Throughput

The VoIP throughput test examined the average bandwidth consumption of a typical VoIP call using a SIP proxy server. By calculating the typical bandwidth usage of one VoIP call, a maximum call capacity for each protocol type was determined as well. This was done by observing the average maximum throughput of each link protocol during a single VoIP call. Since VoIP server capabilities were outside of the scope of this research, this test did not take in to account whether or not the server was actually able to efficiently process all of those calls.

Before testing the bandwidth consumption of a VoIP call, three separate popular VoIP softphone applications were examined: SJphone, Zoiper and X-Lite. This was done in order to find the software that gave the most consistent results. In the end, Zoiper was used because of its consistency, many features, and user-friendly interface. Zoiper's

default audio Codec (G.711 A-law) was used. After the softphone was chosen, Wireshark was used to calculate the average amount of VoIP traffic being sent during a 30-second VoIP call.

Since each VoIP codec has a specific packet size and packets per second (pps), the test was expected to show that the VoIP traffic had the same rate as the codec being used. In this case the codec was G.711 A-law, which has a 160 byte packet and is supposed to send each packet at 50 pps. This means the tests should have resulted in a VoIP throughput of both transmitting and receiving 0.064 Mbps for each user agent on a call.

4. Additional Network Traffic

This test was designed to examine the effects of non-VoIP network traffic on VoIP call throughput. JPerf was used to send specified amounts of generic UDP traffic from the client to the server. The traffic generated was intended to simulate the average traffic seen within the network of a typical Navy aircraft carrier and was based on the actual numbers used for simulating traffic in the SPAWAR Systems Center Pacific network labs [60]. The three amounts generated were based on a percentage of the average network traffic seen on a typical Navy carrier: 60 percent of the average was 1.575 Mbps; 80 percent of the average was 2.163 Mbps; and 100 percent of the average was 2.699 Mbps. Wireshark was used to measure the average network bandwidth during 30-second intervals of various call types, while the different levels of traffic were being generated.

Since the additional traffic data rate was so low in comparison to the maximum capable data rates for the link protocols used, little-to-no effect upon the network's VoIP traffic was expected.

5. VoIP Codecs

The VoIP codec test examined the different network effects of five separate types of popular codecs: G.711 A-law, G.711 U-law, Global System for Mobile Communications (GSM), Speex, and Internet Low Bitrate Codec 30 (iLBC30). For this

test, each codec was used to generate one call with the SIP proxy during three separate 30-second intervals. Wireshark was then used to measure the average bits per frame and pps of the different types of VoIP traffic being sent during all three intervals. This information was then used to determine the actual data rates generated by each codec.

These results should have been similar to those of the VoIP throughput test in that each codec should have had a data rate closely related to its packet size multiplied by its pps rate.

6. VoIP Calls

This test analyzed the effects of various call types, amounts, times, and functions. Different combinations of end-to-end calls and conference calls were examined to see if they performed differently across the network. JPerf was used to simulate the presence of simultaneous calls in sets ranging from two to 50. 30-second and 60-second intervals were tested to see if the length of the call made a difference on network performance. The effects of functions like "mute" and "hold" were tested as well. In all cases, Wireshark was used to capture and analyze the average network consumption of VoIP traffic.

The VoIP conference call (i.e., a call hosted by the VoIP server and not a UA) would likely have consumed half the amount of bandwidth as the normal call, since it only involves one UA. The VoIP network throughput would have likely increased proportionally with the number VoIP calls ongoing at any one time. The length of a VoIP call was expected to have little effect, since VoIP data rates do not vary over time. Finally, the VoIP functions such as "mute" and "hold" were expected to have little impact, because VoIP packet data rates are dependent upon the codec used instead of audio levels.

7. vIDS Effects

The vIDS test analyzed how a vIDS affects the performance of VoIP traffic traversing a network. This test compared the data rates of various amounts of VoIP traffic while the vIDS was on and off. Wireshark was used to examine the different 30-second intervals of vIDS and non-vIDS usage. The test also compared the effects of a vIDS on

the maximum network throughput using the four link protocols tested earlier. This was done by having JPerf send as many TCP/IP packets as possible from the client to the server. Snort was used as the vIDS. It is a very effective IDS with numerous VoIP attack definitions. Its purpose was not to actually detect VoIP attacks, rather to test how a vIDS affects VoIP call performance on a network.

Since the vIDS was only being used passively and not actually blocking malicious traffic, it was expected to have little effect on the flow of VoIP data through the test network. However, since the throughput test was designed to send as many TCP packets across the network as possible, the vIDS would likely see this as an attack and generate alerts accordingly. With the vIDS machine processing so much data, the performance of the proxy server on the same machine might be reduced as well, thus reducing the throughput of VoIP network traffic overall.

C. TEST DESIGN AND EXECUTION SUMMARY

The tests conducted for this research were designed to assess the feasibility of extending tactical communications using afloat naval networks. Specifically, tests were geared towards using wireless networks to extend VoIP traffic to potential hard-to-reach areas onboard large deck naval platforms. The tests compared the capabilities, limitations, and overall performance of various VoIP network configurations in order to determine the most suitable VoIP architecture for extending afloat tactical communications.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RESULTS AND ANALYSIS

A. RESULTS

Seven major groups of tests were performed to analyze the capabilities, limitations, and overall performance of VoIP within different types of networks. A detailed analysis of the seven sets of tests are given in the following subsections.

1. Network Baseline

This test used Wireshark to observe demo network performance without any VoIP calls being processed by measuring the average throughput of all network traffic during three separate 30-second intervals. The test showed that a very low amount of traffic was being sent over the network while inactive. On average, only 0.0078 Mbps of data was sent. This ranged anywhere from broadcast traffic being sent to maintain routing paths, to traffic from the virtual machine to maintain connectivity.

2. Network Throughput

This test used JPerf to examine the overall throughput of the various link protocols by sending as many TCP/IP packets, from client to server, as possible. The test was run between five and ten times for each protocol, until a consistent range of values was detected. The high, low and average throughputs for each protocol are shown in Table 1.

Table 1. Low, High, and Average Protocol Throughput in Mbps

	Low	High	Average
Ethernet	613	641	627
802.11n	33.4	40.0	36.7
2.4 GHz 802.11ac	59.4	82.6	71
5 GHz 802.11ac	89.7	91.0	90.35

The data shows that 802.11n is the least capable link protocol, with an average throughput of 36.7 Mbps. 2.4 GHz 802.11ac has double the capacity at an average of 71

Mbps. 5 GHz 802.11ac has nearly three times the throughput of 802.11n with an average throughput of 90.4 Mbps. Finally, wired Ethernet had 17 times the capacity of 802.11n at an average of 627 Mbps.

None of the results revealed capacities approaching their advertised capabilities: 1 Gbps for Ethernet, 600 Mbps for 802.11n, and 867 Mbps for 802.11ac [59]. This could be due to a number of factors. One factor would be that in the Ethernet test, the router may have been capable of a larger throughput, but the actual machines sending and receiving the data may not have been able to process it at such great speeds. The wireless networks (especially the 802.11ac network) were performing much lower than what was expected. The wireless tests were likely affected by factors such as distance between end points, building design and material signal absorption, wireless interference, router misconfiguration, and other adverse conditions. Many of these wireless factors have been tested in complementary thesis research performed by Anibal Intini titled "Performance of Wireless Networks in Highly Reflective Rooms with Variable Absorption" [61].

3. VoIP Throughput

This test used Wireshark to determine the average bandwidth consumption of a typical VoIP call using a SIP proxy server. After recording the traffic generated during 30 seconds of a VoIP call (see figure 11), Wireshark's conversation statistics were used to calculate the average amount of traffic being sent in four directions: from UAC to SIP server, from SIP Server to UAC, from UAS to SIP Server, and from SIP Server to UAS. Test results from conversations recorded during a 30-second capture of 2 simultaneous VoIP calls are shown in Figure 12. For this test, the UAC was at IP address 192.168.1.146, the SIP Server had IP address 192.168.1.126, and the UAS's IP address was 192.168.1.117.

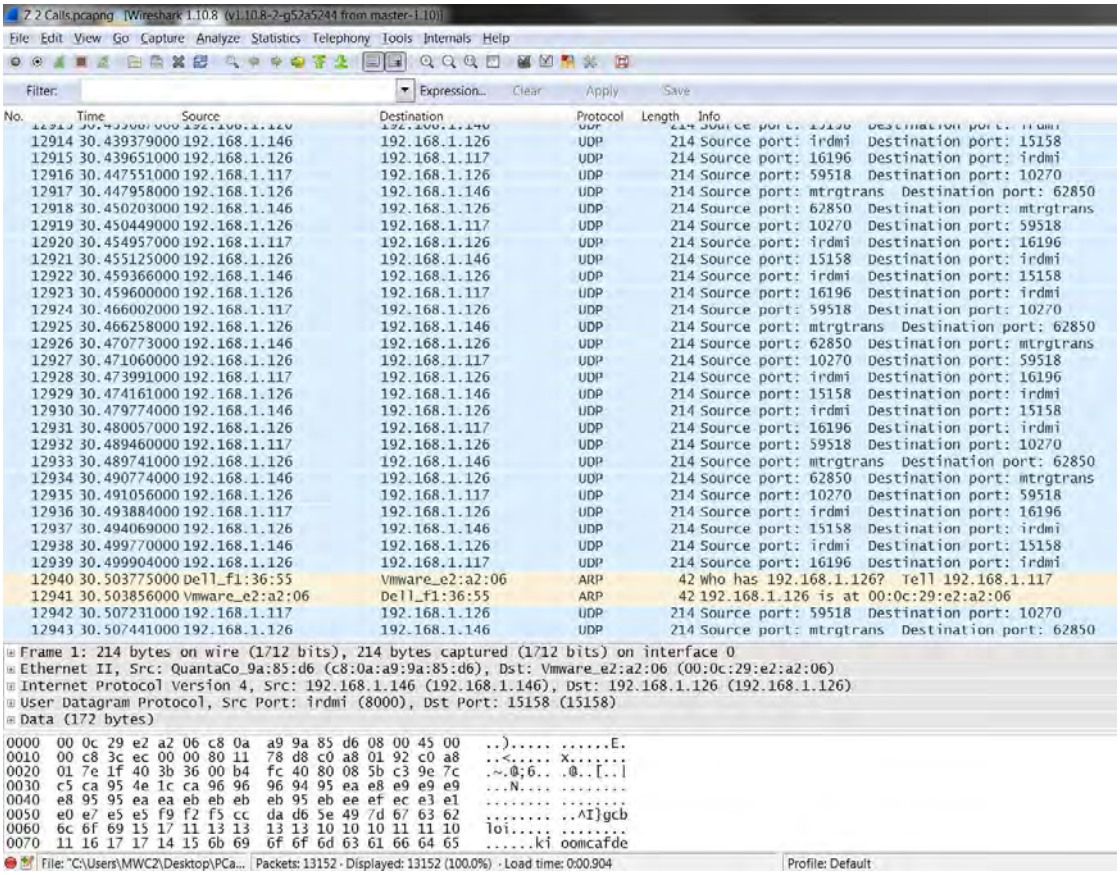

Figure 11. Wireshark VoIP Call Snapshot

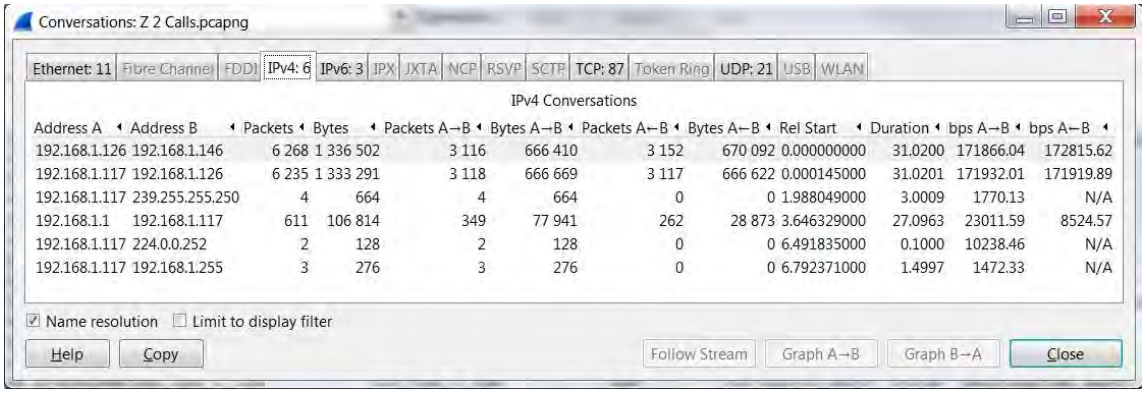

Figure 12. Wireshark Conversation Statistics for 2 VoIP Calls

After performing this test on numerous 30-second periods of a single VoIP call, it was determined that the average amount of VoIP network traffic was 0.334 Mbps. This was composed of 0.0835 Mbps of VoIP traffic in each of the four directions described above. This is somewhat higher than the expected value of 0.064 Mbps. This was due to

the fact that the VoIP packets were actually 1,712 bits in size versus the 1,280 bit size stated by the G.711 standard. This makes sense, considering the fact that the IP packets included 1,376 bits of application data, a 64 bit UDP header, a 160 bit IPv4 header and 112 bits of link layer header and footer data. The actual amount of application data transmitted was 1,376 bits vice 1,280 bits indicating an additional 96 bits of non-voice data per packet, likely consisting of application layer header information.

4. Additional Network Traffic

This test used JPerf and Wireshark to determine the effects of non-VoIP network traffic on VoIP call throughput. The three amounts of additional non-VoIP traffic tested were 1.575 Mbps, 2.163 Mbps, and 2.699 Mbps. The results showing the total average network consumption of a VoIP call with different levels of additional network traffic are shown in Figure 13.

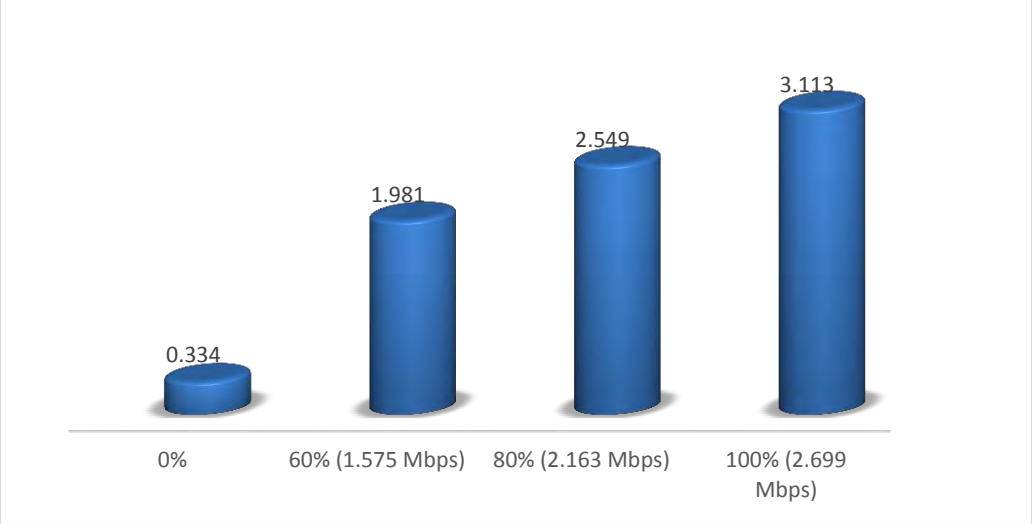

Figure 13. Network Consumption with Increasing Traffic in Mbps

These results show that network consumption increases in parallel with increasing levels of traffic. When 1.575 Mbps of traffic were added, overall network consumption went up by nearly the same rate as when no network traffic was introduced. The 2.163 and 2.699 Mbps traffic levels show similar results. This indicates that additional network

traffic increases bandwidth consumption additively. This means that the overall VoIP call capacity is reduced by one for every 0.334 Mbps of additional network traffic.

5. VoIP Codecs

This test used Wireshark to examine VoIP throughput using five different codec standards: G.711 A-law, G.711 U-law, GSM, Speex, and iLBC30. The results of the test are shown in Figure 14.

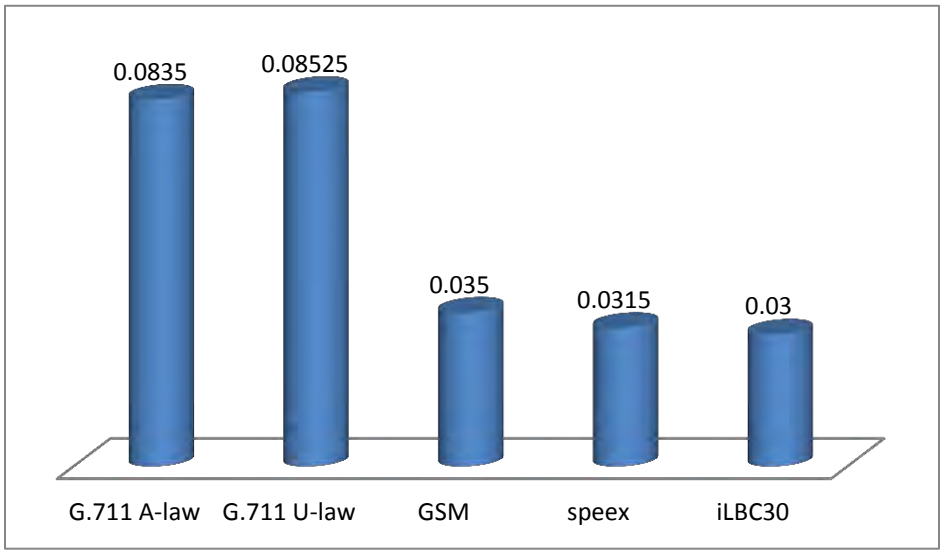

Figure 14. VoIP Throughput per Codec Standard in Mbps

The results for this test are similar to the results from the original VoIP throughput test. Each codec standard shows a rate slightly higher than what was expected. G.711 had rates of 0.0835 and 0.0853 Mbps when it was expected to have application layer data at a fixed rate of 0.064 Mbps. GSM had a rate of 0.035 Mbps vice the expected variable rate of around 0.0122 Mbps. Speex had a rate of 0.0315, while its standard is designed to use a variable rate between 0.002 and 0.044 Mbps. Finally, iLBC30 resulted in a rate of 0.03 Mbps when it is designed to function at a fixed rate of 0.013 Mbps. The higher rates are due to the addition of IP and UDP header information, such as source, destination, protocol, checksum, etc. This means each codec standard was actually operating within its design specifications.

6. VoIP Calls

This test used Wireshark to analyze the effects of VoIP call types and functions such as end-to-end versus conference calls, "mute," and "hold." Figures 15 and 16 show the throughputs seen in each test.

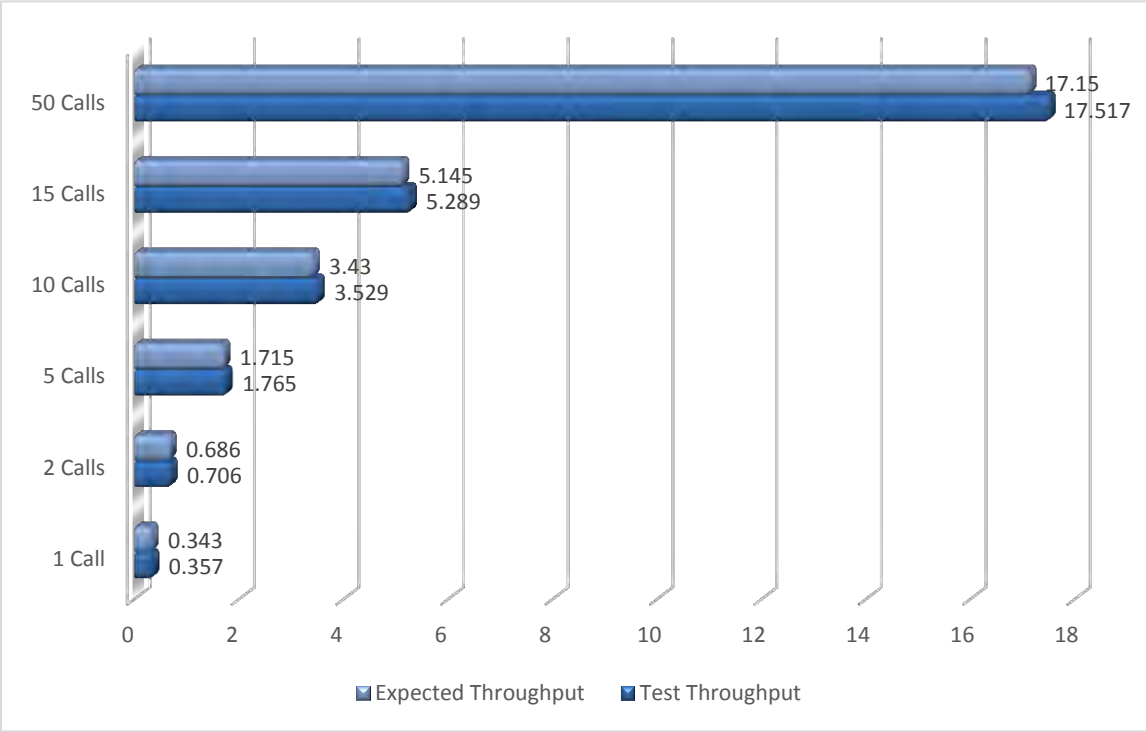

Figure 15. Throughput Comparison of Simultaneous VoIP Calls in Mbps

This tests reveals an apparent equality between simultaneous VoIP calls. VoIP throughput consumption increases by around 0.35 Mbps when another call is added to the network. This shows a linear growth trend in throughput consumption versus the number of VoIP calls. Also, the tested values show a minor increase over what was expected. This was largely due to the fact that the program producing the simultaneous streams of traffic sent small amounts of additional traffic used to monitor the progress of each stream.

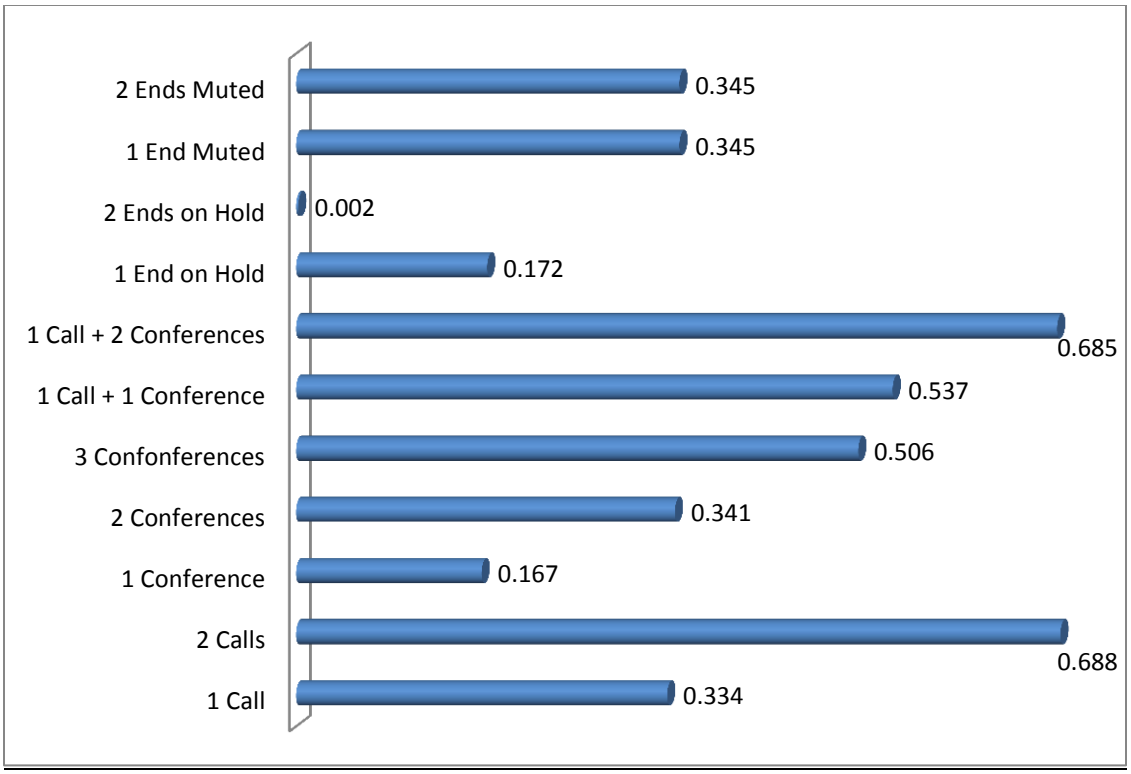

Figure 16. Throughput of Various VoIP Call Types and Features in Mbps

These results show a number of different characteristics of VoIP calls. A conference call consumes about half of the bandwidth (0.167 Mbps) of a normal VoIP call. This makes perfect sense, considering each participant in a conference call speaks directly to, and not through, the VoIP server. It increases linearly (from 0.167 to 0.341 to 0.506 Mbps) as the number of conference calls increases. This linear trend seems to hold with different combinations of full end-to-end calls and conference calls as well. These results show that for every one-way VoIP call, an additional 0.167 Mbps of bandwidth is consumed.

The testing also showed interesting results for the "mute" and "hold" features. Whenever a UA puts a call on "mute" the normal amount of VoIP traffic is still sent and received. However, whenever a UA puts a call on "hold" that UA will no longer be sending or receiving VoIP traffic. This shows that it is more efficient to put calls on "hold" rather than "muting" a microphone.

7. vIDS Effects

This test used Wireshark and JPerf to analyze how a vIDS affects the performance of VoIP traffic on a network, as well as its effects on network performance overall. Figures 17 through 20 show the results of the throughput tests on the different link protocols with and without the use of a vIDS. Each figure shows a high and low range, and average throughput in Mbps. Four sets of tests were performed for each link protocol. One set was for throughput while the vIDS was running and a VoIP call was in progress. Another set was for throughput while a vIDS was running but while no VoIP calls were in progress. The last two were identical to the first sets, although they were performed without the vIDS running at all.

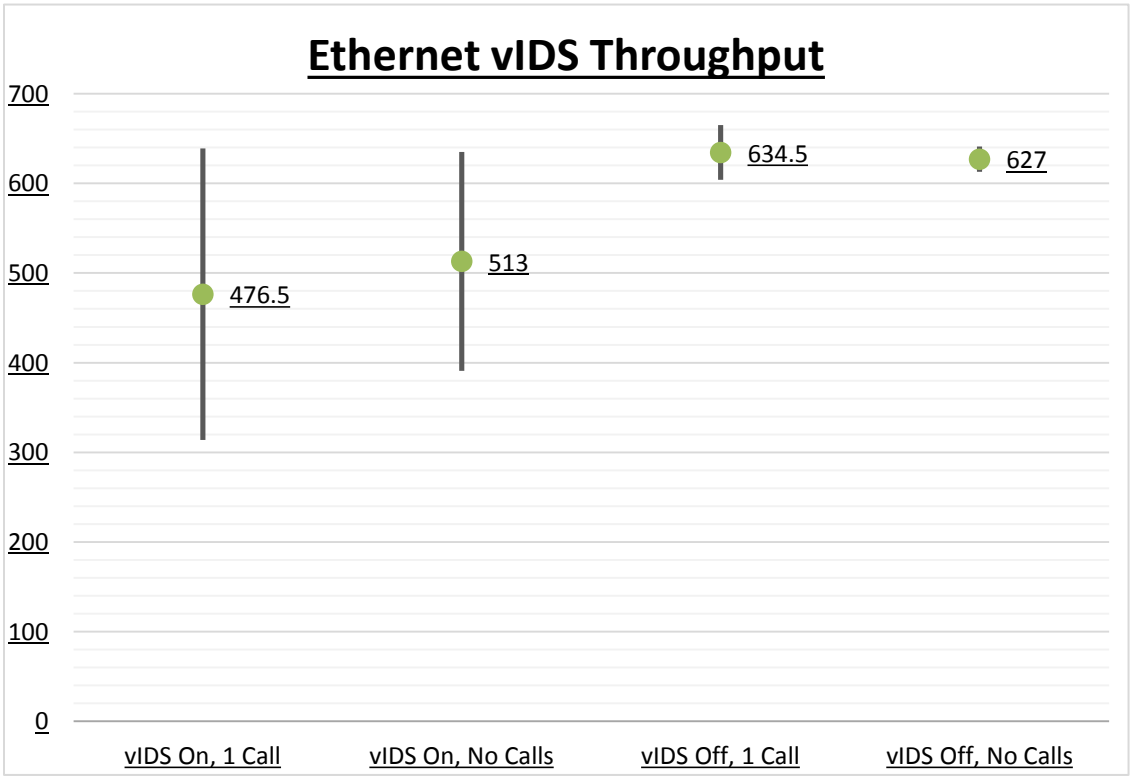

Figure 17. Ethernet vIDS Throughput Range in Mbps

The Ethernet test resulted in very high throughputs with huge variances overall. The larger variances were seen while the vIDS was running; 325 and 244 Mbps while running, versus 61 and 28 Mbps when off. There was also less throughput on average

while the vIDS was running. This shows that a vIDS may adversely affect network performance. Also, there did not seem to be any correlation between throughput and whether or not a call was in progress.

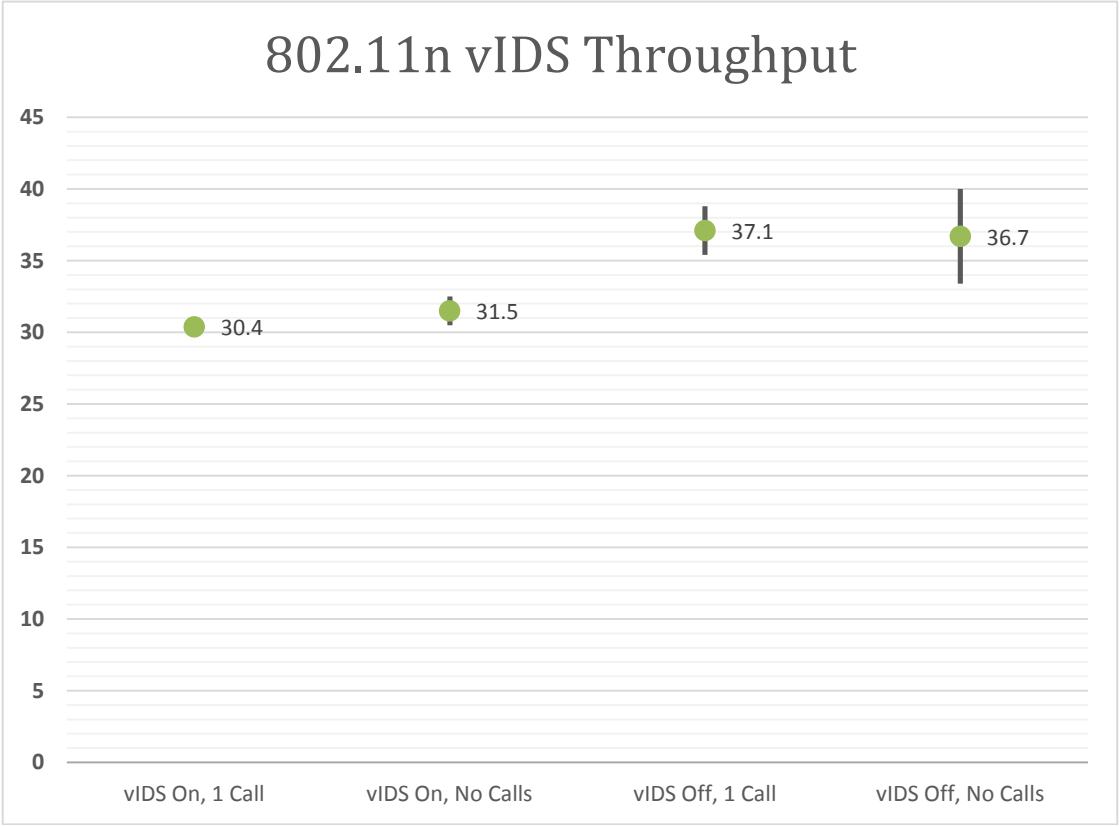

Figure 18. 802.11n vIDS Throughput Range in Mbps

The tests on the 802.11n protocol had the lowest throughput results overall. These showed trends similar to those in the Ethernet tests. There was a decrease in network performance while the vIDS was on, and calls seem to have minimal effects on throughput. However, there were larger variances in throughput while the vIDS was off; 3.4 and 6.6 Mbps while off, versus 0.8 and 2 Mbps while turned on.

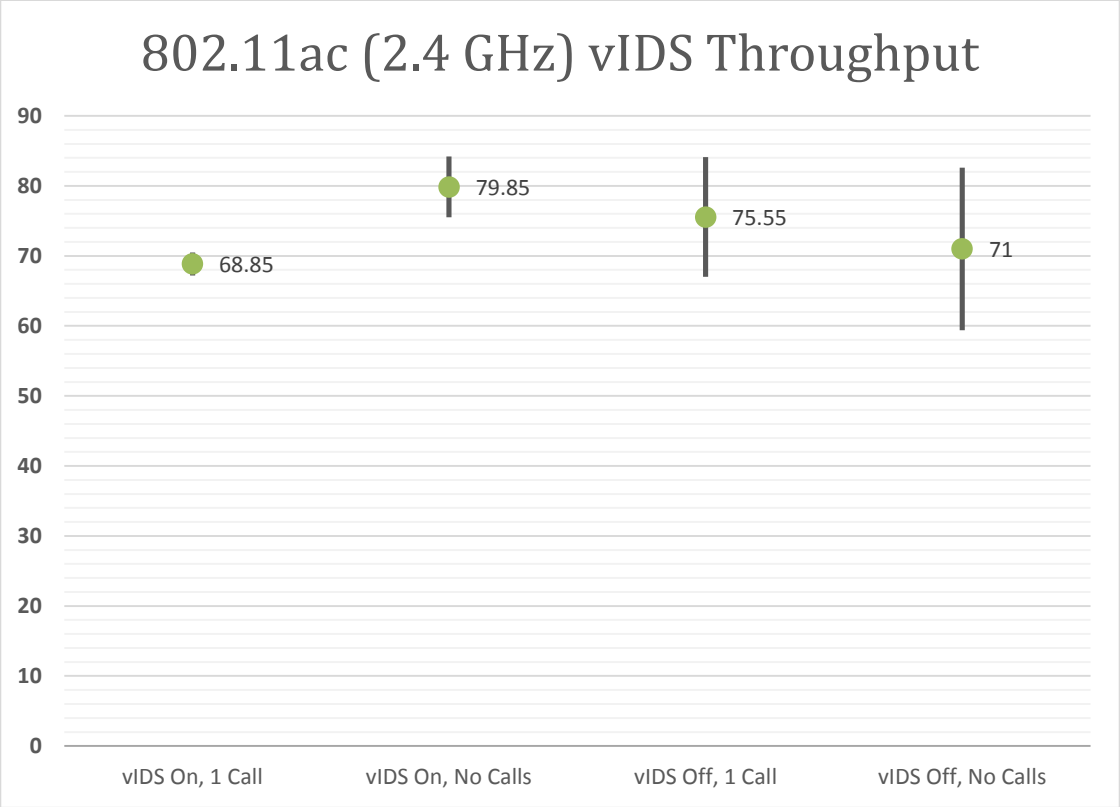

Figure 19. 802.11ac (2.4 GHz) vIDS Throughput Range in Mbps

The results for the 2.4GHz 802.11ac protocol were slightly different than the others. There were no clear trends associated with throughput and the vIDS being on or off, or whether calls were being progressed or not. The only observable characteristic was that there were larger variances while the vIDS was off; 17.1 and 23.2 Mbps while off, versus 3.3 and 8.7 Mbps while turned on. This was similar to the 802.11n tests but differed from the Ethernet tests.

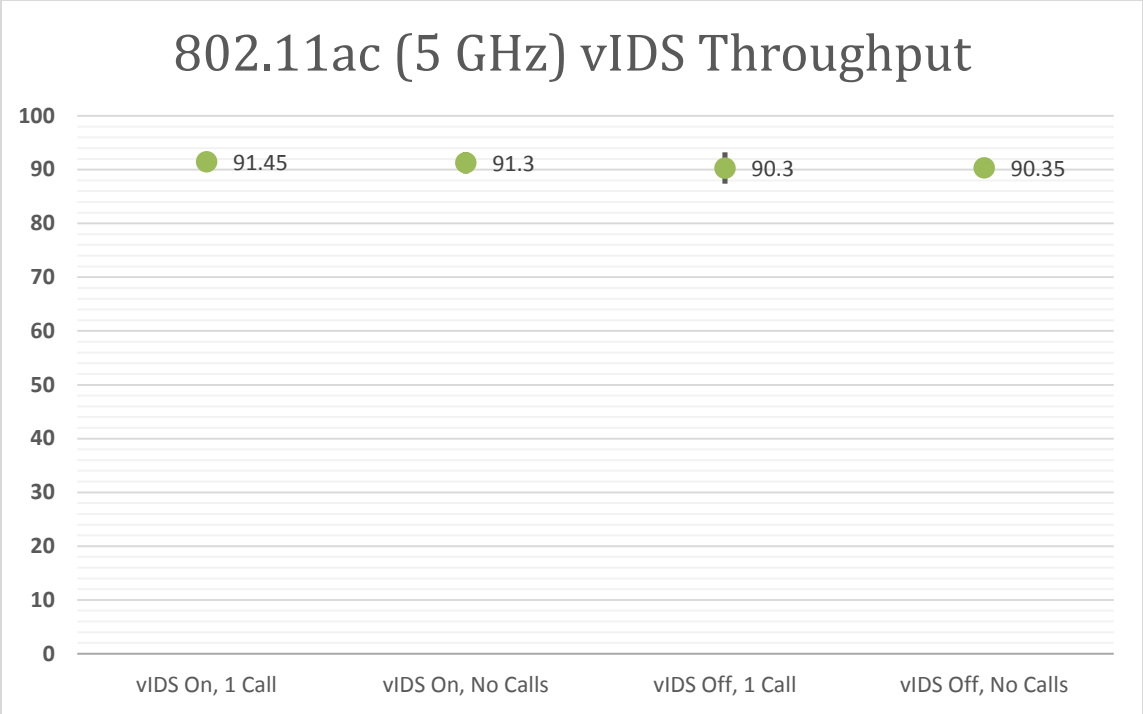

Figure 20. 802.11ac (5GHz) vIDS Throughput Range in Mbps

The final throughput tests were on the 5 GHz 802.11ac protocol. These showed very different results from the other tests. There were higher throughputs while the vIDS was running, having a call in progress had no major effect, and there were small variances throughout; 3.3, 4.0, 5.8 and 1.3 Mbps shown from left to right in Figure 20. Figure 21 shows the combined results of all of the wireless protocol tests.

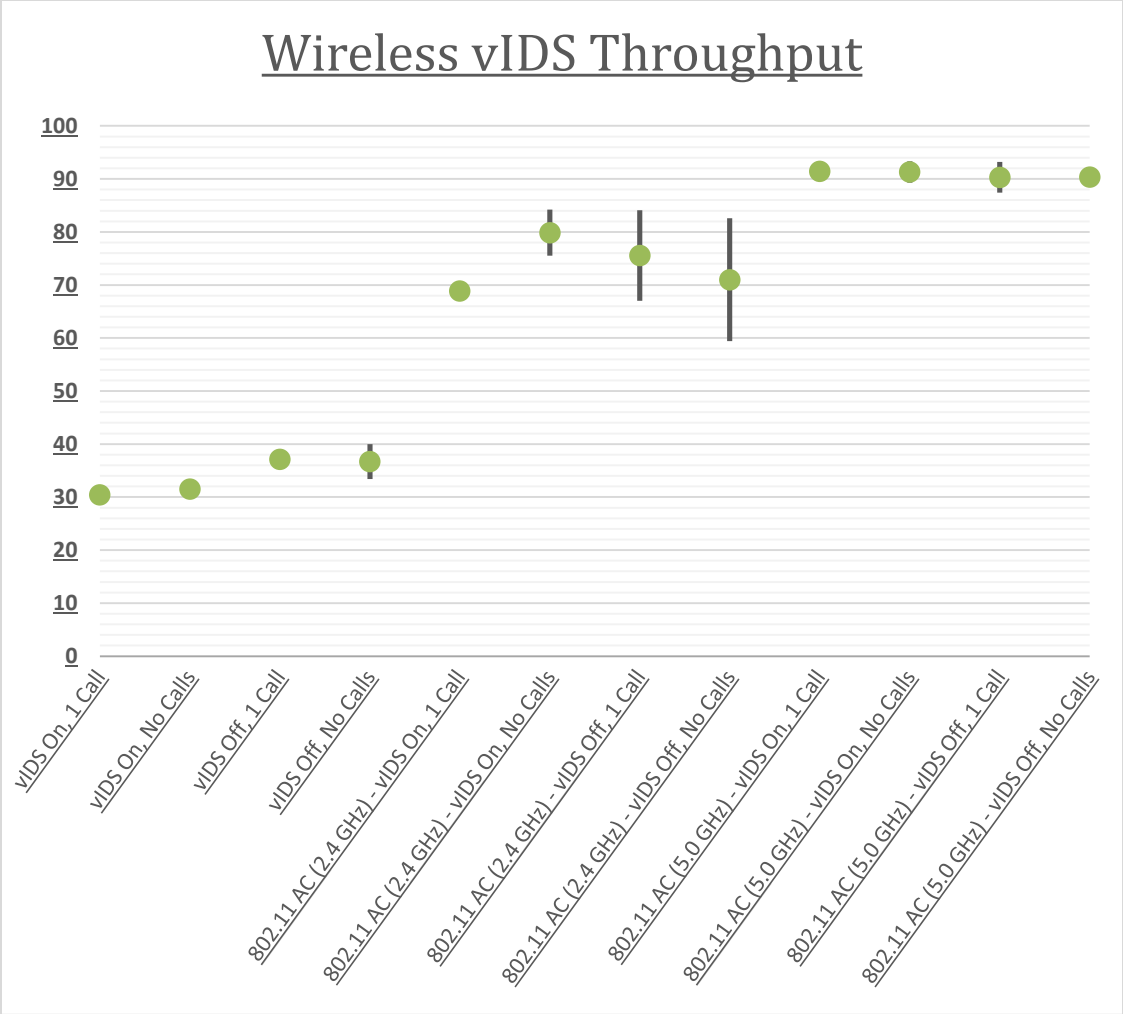

Figure 21. Combined Wireless vIDS Throughput Ranges in Mbps

Overall, the test results show some interesting aspects of using a vIDS, the most obvious being that the faster the protocol the higher the throughput whether or not a vIDS is running. Another aspect is that running a vIDS does not seem to have a major effect on wireless protocols overall, nor does it matter if calls are in progress while running the vIDS. The 2.4 GHz 802.11ac protocol did not seem to have very consistent network throughput with or without the use of a vIDS. Lastly, the Ethernet link protocol seemed to be affected the most by the use of a vIDS, both in the average throughput and the variance in throughput overall.

B. LESSONS LEARNED

There were many interesting takeaways from the testing process. Most of these had to do with Wi-Fi optimization, which was not the focus of this research. It was, however, important to gathering consistent results. Specifically, these lessons learned had to do with network configurations and led to the following list of configuration recommendations: change to the least used wireless channel in your operating area; find a space with as little EM interference as possible; keep a consistent distance from the access point; do not place the end device close (less than 15 feet) to the access point; stay clear of objects blocking the path; and run the tests long enough to obtain consistent results (60 seconds or longer).

Another lesson learned was that different VoIP softphone programs behave very differently. Some produce audio delays while others may not. Some implement different codec standards than others. Some programs implement the "mute" and "hold" functions differently (i.e., whether or not the function continues to transmit and receive data). Another major difference among VoIP softphones is that some have features (e.g., push-to-talk, security) that others do not. The primary lesson learned from this is that a consistent and dependable application that has all of the features and codec standards being tested is required.

One final lesson learned had to do with how Wireshark summarizes the average throughput during a capture. Wireshark has numerous ways of viewing network throughput for packet captures. One way is through the "Summary" tool. This tool gives many relevant statistics, one of which is the total average throughput. This is not always consistent with other throughput statistics in the program. The "Conversations" tool list average throughput per protocol and for each IP address. When these are all summed up, they do not always equal the same value given by the "Summary" tool. It is unclear how Wireshark calculates the average total throughput. The main lesson learned from this highlights the importance of understanding the data being analyzed. In this case, use of the "Conversation" tool's values for a more detailed analysis of network traffic was imperative.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This thesis analyzed multiple aspects of communications systems, networks, VoIP systems, protocols and security. It attempted to determine the feasibility of integrating these systems to extend tactical communications afloat. The tests were designed and conducted to provide statistical information towards this end.

The tests reveal that VoIP network traffic consumes around 0.334 Mbps of throughput on average for one call using the G.711 codec standard. This number changes according to the codec standard used. The results also indicate a linear rate change between the number of calls in progress and network throughput consumption. Some other important findings were that the 5 GHz 802.11ac wireless link protocol out performs other 802.11-derived wireless protocols and is able to handle an average throughput of around 90.4 Mbps or approximately 270 VoIP phone calls. Consuming the entire network's bandwidth would introduce issues not addressed in this research, notwithstanding, these results demonstrate the capability of an 802.11ac network for this purpose. Another interesting result from the testing was that implementing a vIDS on a wireless VoIP network has little effect on network performance overall.

To determine if a wireless VoIP solution would be feasible for extending tactical communications afloat, its capabilities, limitations, and applicability must be understood. Many of the capabilities and limitations have already been discussed. To grasp the applicability of such a system, the capabilities of a typical tactical communications system must also be understood. The primary afloat tactical communications system currently used in the Navy, the DMR, is capable of supporting up to 128 simultaneous channels. As shown, a VoIP system should be able to support as many calls.

The wireless VoIP system tested in this thesis had the capacity for 270 simultaneous calls and was more than capable of handling a robust VoIP architecture. Therefore, a wireless VoIP system using the 5 GHz 802.11ac link protocol is a viable solution for solving the issue of extending tactical communication afloat.

B. RECOMMENDATIONS

In order to extend tactical communications within afloat platforms, it is recommended that a vIDS-monitored wireless VoIP system such as the one outlined in Figure 22, be integrated with current afloat communications systems and networks. Since afloat networks already have some Cisco VoIP components, it would be most beneficial if the additional components were Cisco-compatible products.

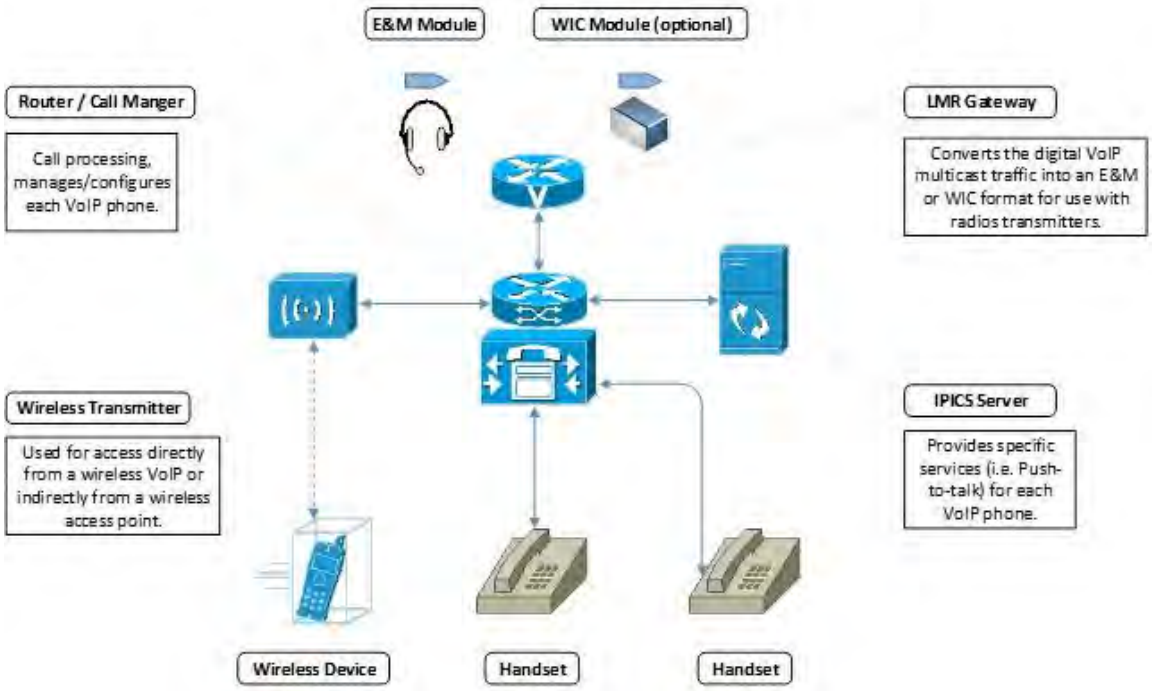

Figure 22. Recommended Afloat Tactical Integrated VoIP System

A call manager is recommended to handle call processing and configuration of all networked VoIP devices. Specifically, a device commensurate with the Cisco 2900 or 3900 series call managers should be used. A LMR Gateway is recommended for converting between digital VoIP traffic and audio formatted for radio transmitters. This should also be of similar capability to a Cisco 2900 or 3900 series device. An IPICS Server is recommended to provide capabilities such as push-to-talk, conferencing, and admin/policy configuration. The IPICS server could be run on the same device as the

LMR Gateway, depending on the amount of traffic it needs to support. Figure 23 depicts how an IPICS server can support a highly heterogeneous VoIP network.

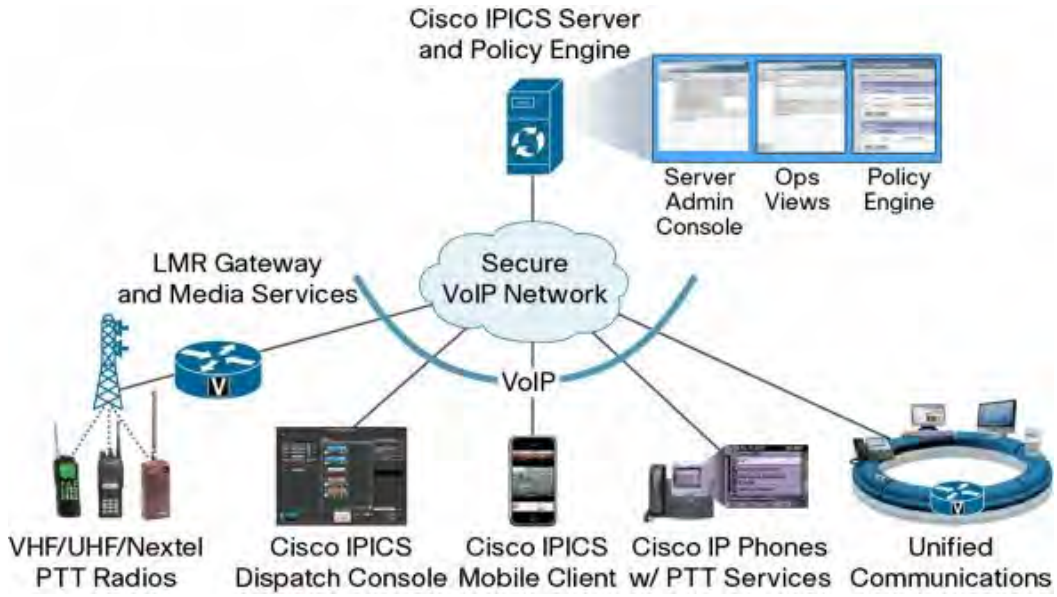

Figure 23. Cisco IPICS Services, from [50]

Some other recommended components for this system would be a wireless access point, wireless adapter, VoIP end-devices, and a vIDS. The wireless access point should be any 5 GHz 802.11ac device, capable of handling a minimum of 128 simultaneous VoIP channels. The wireless adapter is only necessary if the end devices are not Wi-Fi capable. The wireless adapter should also be a 5 GHz 802.11ac compatible device. The end-devices could be anything from a softphone on a laptop to a wireless handheld VoIP phone. The primary recommendation for the end-devices is that they use an efficient, variable bit-rate codec, such as Speex or GSM. Finally, a sophisticated vIDS is recommended in order to mitigate the potential security vulnerabilities of the VoIP system. A multiprotocol and multistate aware vIDS similar to the one suggested by Sengar [24] is recommended for this highly integrated system.

C. FUTURE WORK

This research was focused on comparing the capabilities and limitations of the four link protocols used, with an end goal of determining the most feasible VoIP

architecture for extending tactical communications afloat. However, there are still many topics that can be assessed for transmission of tactical communications through VoIP networks. Some of these additional research topics include radio integration; VoIP protocol comparisons; vIDS capabilities and limitations; Wi-Fi optimization and emissions control; and full scale simulation of integrated VoIP, radio, and network systems.

1. Radio Integration

VoIP radio integration should be further studied to better understand not only how to integrate specific radio systems with VoIP systems but also to learn the capabilities and limitations that come from integrating these two audio transmissions systems as well. This would involve a detailed study of current VoIP and radio integrated systems. This research should examine the technologies used to convert digital VoIP audio data into analog RF transmissions. A comparison and test of different VoIP over radio solutions would be useful as well.

2. VoIP Protocol Comparison

A detailed VoIP protocol comparison would be extremely helpful in order to determine the most efficient and secure means of transmitting VoIP data across wired and wireless networks. This research should examine past, present, and emerging VoIP protocols beyond SIP and H.323. It would need to look at both public and proprietary protocols. This study should also involve an examination of the supporting protocols used at different layers of the TCP/IP stack. Another area to be covered by this research would be a comparison of VoIP codec standards. An assessment and test of the capabilities and limitations of a variety of popular VoIP protocols should accompany the research as well.

3. vIDS Capabilities and Limitations

Further research in the area of VoIP security systems would be beneficial to this and future studies. Such research should analyze the capabilities, limitations, and accuracy of different vIDS and vIPS applications. Real-world production systems and conceptual systems should both be studied. The research should compare traditional IDS

and IPS systems designed to analyze VoIP and non-VoIP traffic, as well as vIDS and vIPS systems specifically designed for VoIP traffic only. The study should include a test of a variety of different IDS an IPS systems against a variety of malicious and non-malicious VoIP attacks. Security ramifications beyond vIDS integration are also of concern; in particular, the impact of encryption of the VoIP traffic should be investigated to assess whether the underlying VoIP protocols are sensitive to delays that might be caused by the encryption technology used. While not addressed directly by this thesis, such performance impacts are of particular concern to operators.

4. Wi-Fi Optimization

Another supporting research topic would be Wi-Fi optimization in afloat platforms. This study should compare current and past technologies and techniques used on board military and commercial vessels. It should identify the unique aspects of using wireless technologies at sea, as opposed to on land. It should examine a variety of case studies of organizations which adopted Wi-Fi technology on afloat platforms. The study should test some of the methods and technologies revealed during the research and compare the overall benefits of each. There have already been detailed studies performed on parts of this topic [52], which could be further expanded upon as well.

5. Full Scale VoIP Integration Test

A major future work study that could complement this thesis research would be a full-scale simulation of the suggested VoIP architecture. This could involve integrating a Cisco demo kit [62], with a LMR, an afloat radio system, and a wireless network. This study could even go as far as integrating a wireless VoIP system with a ship's network and radios, in order to simulate real world usage. However it is performed, a full-scale test would be the most beneficial way of discovering accurate capabilities, limitations, and interoperability of an integrated wireless VoIP system afloat.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] S. Anderson. (2013). U.S. Navy information dominance roadmap 2013–2028. U.S. Navy. [Online]. Available: http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4676. Accessed Mar. 02, 2014.

[2] Clark et al., "Coalition Fleet synthetic training," Defense Science & Technology Organization, Melbourne, Australia, Tech. Rep. 2007.

[3] L. Gebhard, "Evolution of naval radio-electronics and contributions of the naval research laboratory." Naval Research Laboratory, Washington, DC: Tech. Rep. NRL 8300, 1979.

[4] V. Beck, *Supercarriers of the US Navy.* Loschberg, Germany: Jazzybee, 2013.

[5] C. Suggs, "PEO C4I masterplan," Program Executive Officer, Command, Control, Communications, Computers and Intelligence, San Diego, CA, Tech. Rep. Version 6.0, 2012.

[6] General Dynamics, "Digital Modular Radio" General Dynamics C4 Systems, Falls Church, VA, Tech. Rep. 2007.

[7] Blue Coat Systems, Inc. (2014). Blue Coat—PacketShaper. [Online]. Available: https://www.bluecoat.com/products/packetshaper. Accessed Aug. 10, 2014.

[8] J. Riposo, J. Gordon, R. Murphy, B. Wilson, and I. Porche, "CANES contracting strategies for full deployment." RAND Corporation, Santa Monica, CA, 2012.

[9] Axvoice. (2012, May 10). US telecom industry from 2010 to 2015—A research by Axvoice. blog.axvoice.com. [Online]. Available: http://blog.axvoice.com/us-telecom-industry-from-2010-to-2015-a-research-by-axvoice/ Accessed Jun. 05, 2014.

[10] D. Scott, "The development of VoIP," Dept. GSEAS, Naval Postgraduate School, Monterey, CA, unpublished. 2014.

[11] VoIP—Voice Over Internet Protocol. (n.d.). 2voip.info. [Online]. Available: http://www.2voip.info/voip-history.htm. Accessed Aug. 2, 2013.

[12] M. Ward. (2014, Jan. 1). What the net did next. *BBC*. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/3292043.stm. Accessed Jun. 05, 2014.

[13] M. Toy, *Networks and Services: Carrier Ethernet, PBT, MPLS-TP, and VPLS.* Wiley, 2012.

[14] Alcatel-Lucent. (2014, Feb. 17). Alcatel-Lucent passes milestone of 125 million Voice over IP licenses as 4G service providers drive to deploy Voice over LTE. alcatel-lucent.com. [Online]. Available: http://www.alcatel-lucent.com/press/2014/alcatel-lucent-passes-milestone-125-million-voice-over-ip-licenses-4g-service-providers. Accessed Jun. 05, 2014.

[15] D. Carr. (2009, Jul. 02). How the military is unifying communications and collaboration. Defense Systems. [Online]. Available: http://defensesystems.com/articles/2009/07/08/cover-story-military-communications.aspx. Accessed Jun. 05, 2014.

[16] Kristen. (2014). Corporate world: Moving ahead with VoIP. Streetdirectory.com. [Online]. Available: http://www.streetdirectory.com/travel_guide/120862/voip/corporate_world_moving_ahead_with_voip.html. Accessed May. 17, 2014.

[17] T. Porter, *Practical VoIP Security.* Rockland, MA: Syngress Publishing Inc., Practical VoIP Security.

[18] Anonymous "Cisco IOS IP configuration guide," Cisco Systems, Inc., San Jose, CA, Tech. Rep. Release 12.2.

[19] Cisco. (16 October 2012). Cisco IOS voice troubleshooting and monitoring—H.323-related standards. docwiki.cisco.com. [Online]. Available: http://docwiki.cisco.com/wiki/Cisco_IOS_Voice_Troubleshooting_and_Monitoring_--_H.323-Related_Standards. Accessed May. 17, 2014.

[20] A. Mankin. (2013, Mar. 02). SIP: Session Initiation Protocol—RFC 3261. IETF. [Online]. Available: https://datatracker.ietf.org/doc/rfc3261/. Accessed Jun. 07, 2014.

[21] TelcoNotes. (2013, Mar. 13). SIP transactions vs. dialogs. World Press. [Online]. Available: http://telconotes.wordpress.com/2013/03/13/sip-transactions-vs-dialogs/. Accessed Jun. 07, 2014.

[22] A. Mankin. (2013, Mar. 02). RTP: A transport protocol for real-time applications—RFC 3550. IETF. [Online]. Available: https://datatracker.ietf.org/doc/rfc3550/. Accessed Jun. 07, 2014.

[23] National Institute of Standards and Technology. (2014, Aug. 15). National Vulnerability Database Version 2.2. nvd.nist.gov. [Online]. Available: http://nvd.nist.gov/. Accessed Jun. 7, 2014.

[24] H. Sengar, *Security of Public and IP Telephone Networks.* Saarbrucken, Germany: VDM Verlag Muller, 2008.

[25] P. Thermos. (2010, Nov. 2). Two attacks against VoIP. Symantec. [Online]. Available: http://www.symantec.com/connect/articles/two-attacks-against-voip. Accessed May. 17, 2014.

[26] S. Ahson and M. Ilyas, *VoIP Handbook: Applications, Technologies, Reliability, and Security.* Boca Raton, FL: CRC Press, 2009.

[27] VOIPSA, Inc. (2014). VoIP Security Tool List. voipsa.org. [Online].Available: http://www.voipsa.org/Resources/tools.php. Accessed May. 17, 2014.

[28] Roughead, G., "Reorganization of the Office of the Chief of Naval Operations (OPNAV) staff." Department of the Navy, Chief of Naval Operations, Washington, DC, Memo. 2009.

[29] J. Guo, J. Yen and H. Pai, "New voice over internet protocol technique with hierarchical data security protection," *Vision, Image and Signal Processing, IEE Proceedings,* vol. 149, pp. 2014, Mar. 6, 2002.

[30] Y. Wu, S. Bagchi, S. Garg, N. Singh and T. Tsai, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP environments," in *Proc. DSN*, 2004, pp.433-442.

[31] X. Chen and J. Heidemann, "Flash crowd mitigation via adaptive admission control based on application-level measurement," University of Southern California, Los Angeles, CA, Tech. Rep. ISI-TR-557, 2002.

[32] General Dynamics. (2010). Secure Voice over IP (SVoIP) vs. Voice over Secure IP (VoSIP) Installations. gdc4s.com. [Online]. Available: http://www.gdc4s.com/Documents/Products/SecureVoiceData/GD-SVOIP_FAQ-w.pdf. Accessed Jun. 07, 2014.

[33] Cisco Inc. "Cisco unified communications manager security guide," Cisco Systems, Inc., San Jose, CA, Tech. Rep. Release 8.6(1).

[34] DIACAP Services. DIACAP Services—Global Solution Provider. diacapservices.com. [Online]. Available: http://diacapservices.com/index.html. Accessed Jun. 05, 2014.

[35] Baugher, et al.. (2004, Mar.). The Secure Real-time Transport Protocol (SRTP). IETF. [Online]. Available: http://tools.ietf.org/html/rfc3711. Accessed Jun. 07, 2014.

[36] R. Onuskanich, "Out with the DIACAP, In with the DIARMF," Lunarline, Inc., Arlington, VA, Tech. Rep. 2011.

[37] R. Kuhn, T. Walsh and S. Fries, "Security considerations for Voice over IP systems," National Institute of Standards and Technology, Tech. Rep. Special Publication 800-58, 2005.

[38] M. Zamorski. (2005, Jul. 27). Voice over Internet Protocol Guidance on the Security Risks of VoIP. FDIC. [Online]. Available: https://www.fdic.gov/news/news/financial/2005/fil6905.html. Accessed Jun. 05, 2014.

[39] NSA's Systems and Network Attack Center, "Recommended IP telephony architecture," Tech. Rep. I332-009R-2006, 2006.

[40] World Press. (2008, Jul. 1). Understanding various Speech Codecs. wordpress.com. [Online]. Available: http://speechcodecs.wordpress.com/. Accessed Aug. 28, 2014.

[41] Voip Info. (2013, Mar. 16). Codecs. voip-info.org. [Online]. Available: http://www.voip-info.org/wiki/view/Codecs. Accessed Aug. 28, 2014.

[42] Microsoft. (2014). 3.1.5.3 Representing new Payload Types. [Online]. msdn.microsoft.com. Available: http://msdn.microsoft.com/en-us/library/dd949621(v=office.12).aspx. Accessed Aug. 28, 2014.

[43] NIK. (2011, Jun. 16). VoIP Codec: Payload size. voip-sip.org. [Online]. Available: http://www.voip-sip.org/voip-codec-payload-bandwidth-required/. Accessed Jun. 05, 2014.

[44] Cisco. Configuring Weighted Random Early Detection. (n.d.). cisco.com. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfwred.html. Accessed Aug. 19, 2014.

[45] Class-Based Weighted Fair Queueing. (n.d.). Cisco. [Online]. Available: http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html#wp17641. Accessed Aug. 19, 2014.

[46] L. Davis. (2012, Feb. 26). EIA-530 Cable bus. interfacebus.com. [Online]. Available: http://www.interfacebus.com/Design_Connector_EIA530.html. Accessed Jun. 05, 2014.

[47] Cisco Land Mobile Radio Gateway. (n.d.). Cisco. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/routers/2600-series-multiservice-platforms/product_data_sheet0900aecd8034ef85.html. Accessed Aug. 19, 2014.

[48] Radio Control System—VoIP /RoIP. (n.d.). Orion Systems Inc. [Online]. Available: http://www.orionsystemsinc.net/radio_control_system_voip.html. Accessed Aug. 28, 2014.

[49] Omnitronics. (2014). RoIP/VoIP connectivity products. omnitronicsworld.com. [Online]. Available: http://omnitronicsworld.com/voip-connectivity/. Accessed Aug. 28, 2014.

[50] Cisco IP interoperability and collaboration system release 4.8 data sheet. (n.d.). Cisco. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/physical-security/ipics-server-software/data_sheet_C78-728836.html. Accessed Aug. 19, 2014.

[51] B. Lovell, "Common Optical Distribution Architecture (CODA) shipboard wireless comms," SPAWAR Pacific, San Diego, CA, Tech. Rep. 2013.

[52] Cisco Systems, "Preliminary voice over wireless LAN radio frequency assessment for LHD-8 USS Makin Island," Cisco Systems, Inc., Herndon, VA, 2011.

[53] Y. Jeong, S. Kakumanu, C. Tsao, and R. Sivakumar. (n.d.). Improving VoIP call capacity over IEEE 802.11 networks. Georgia Institute of Technology. [Online]. Available: http://www.ece.gatech.edu/research/GNAN/archive/2007/broadnets07a.pdf. Accessed Jun. 05, 2014.

[54] M. Krym, "Efficiency of VoIP on 802.11n," Nortel Networks, Ottawa, Canada, Tech. Rep. IEEE 802.11-07/2704r0, 2007.

[55] V. Kelly. (2014, Jan. 7). New IEEE 802.11ac™ specification driven by evolving market need for higher, multi-user throughput in wireless LANS. IEEE. [Online]. Available: http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html. Accessed Jun. 05, 2014.

[56] 802.11ac—The fifth generation of Wi-Fi technical white paper. (n.d.). Cisco. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html. Accessed Aug. 19, 2014.

[57] S. Anderson, "CANES consolidated, dynamic and combat-ready," *Chips,* Jul.–Sep. 2009.

[58] Polycom, "Deploying enterprise-grade wi-fi telephony: Coverage, capacity, Quality of service, and security Considerations for delivering excellent voice quality on enterprise Wi-fi networks," Polycom, Inc., Pleasanton, CA, 2010.

[59] Linksys. (2014). Linksys WRT1900AC Wireless AC router. store.linksys.com. [Online]. Available: http://store.linksys.com/Linksys-WRT1900AC-App-Enabled-AC1900-Dual-Band-Wireless-Router_stcVVproductId158014980VVcatId553965VVviewprod.htm. Accessed Aug. 19, 2014.

[60] B. Cooper, "IXIA Loads," SPAWAR Pacific, San Diego, CA, Tech. Rep. 2013.

[61] A. Intini, "Performance of wireless networks in highly reflective rooms with variable absorption, MS thesis, Dept. Computer Science, Naval Postgraduate School. Monterey, CA, 2014.

[62] Cisco&Business&Edition&3000&Demo&Kit. (n.d.). Cisco. [Online]. Available: https://supportforums.cisco.com/sites/default/files/legacy/4/5/6/48654-Cisco_Business_Edition_3000_Demo_Kit.pdf. Accessed Aug. 19, 2014.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California