NPS-AM-10-004

ACQUISITION RESEARCH SPONSORED REPORT SERIES

Integrating Cellular Handset Capabilities with Marine Corps Tactical Communications

4 May 2010

by

Joshua S. Dixon, Capt., USMC

Advisors: Dr. Geoffrey G. Xie, Professor, and
Dr. Frank Kragh, Associate Professor
Graduate School of Operational and Information Sciences

Naval Postgraduate School

Prepared for: Naval Postgraduate School, Monterey, California 93943

The research presented in this report was supported by the Acquisition Chair of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request Defense Acquisition Research or to become a research sponsor, please contact:

NPS Acquisition Research Program
Attn: James B. Greene, RADM, USN, (Ret)
Acquisition Chair
Graduate School of Business and Public Policy
Naval Postgraduate School
555 Dyer Road, Room 332
Monterey, CA 93943-5103
Tel: (831) 656-2092
Fax: (831) 656-2253
e-mail: jbgreene@nps.edu

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.acquisitionresearch.org

Abstract

Stateside, communication is as easy as picking up a cell phone and dialing from virtually anywhere. A cell phone has the capability to send and receive real-time voice communication, voice messaging, text messaging, and e-mail as well as to capture videos/pictures. However, the cost of this technology in a field environment has traditionally been too heavily weighted toward permanent infrastructure or other non-cost-efficient solutions. Imagine the communication benefits for highly mobile units either providing disaster relief and humanitarian assistance or conducting full-scale combat operations. These missions share similar characteristics, which routinely require a highly mobile, ad-hoc wireless network to provide successful communication within and among participating units. This thesis investigates three approaches of integrating COTS cellular technology with Marine Corps tactical radio networks: reconfiguring a hand-held device, adding a modular bridge device, and reconfiguring current Marine Corps tactical radios. The majority of the experiment chapter is devoted to evaluating current military radios and commercial cellular devices as extensions. Because the military does not currently field cellular technology, the main focus was the measurement and comparison of the throughput limitations and device emissions. The risks associated with COTS cellular handsets are not as significant as the normal misconceptions.

Keywords: Cellular, Phone, Telephone, PRC-117G, AN/PRC-117G, Harris, Cell Phone, Tactical Radio, Base Station, Security, LPD, LPI, LPE

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

There are many people I would like to thank for their assistance and support. I will start with my biggest supporters, my wife and children. My wife Abbey trudged through the trenches with our twin boys day in and day out, while I spent countless hours on the computer and in the lab. I could not have completed this endeavor without her. I would like to applaud my kids, Bryce and Cole, who spent their nights entertaining me and replenishing my motivation with their silly activities.

On the professional-development side, I would like to thank my two advisors, Professor Geoffrey Xie and Assistant Professor Frank Kragh, for allocating extra time and energy towards answering my constant and recurring questions.

For all the hands-on help and stimulating thoughts, I would like to thank, John H Gibson, NPS lecturer, for assisting me throughout the thesis. He not only provided a third perspective, but also attended and assisted in the execution of the experiments.

For their consistent support and professional guidance, I would like to thank, Major James Robinson (HQMC C4) and Major James Neushul (I MEF IMO). They both provided support with specific guidance in promoting and validating the concepts in this project.

For his consistent, valuable, military advisory direction, I would like to thank LtCol Carl Oros (Ret). He not only supported me with relevant input, but also provided additional resources as needed.

I would like to thank Marine Corps System Command, Product Group 12, Communications, Intelligence, and Networking Systems (CINS) section and the Joint Program Executive Office (JPEO), Joint Tactical Radio Systems (JTRS) for their support with funding and/or equipment.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-AM-10-004

ACQUISITION RESEARCH SPONSORED REPORT SERIES

Integrating Cellular Handset Capabilities with Marine Corps Tactical Communications

4 May 2010

by

Joshua S. Dixon, Capt., USMC

Advisors: Dr. Geoffrey G. Xie, Professor, and

Dr. Frank Kragh, Associate Professor

Graduate School of Operational and Information Sciences

Naval Postgraduate School

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the Federal Government.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Acronyms and Abbreviations

2.5G	2.5 Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
AES	Advanced Encryption Standard
AJ	Anti-Jam
AN/PRC	Army Navy / Portable Radio Communication
ANW2	Advanced Network Wideband Waveform
API	Application Programming Interfaces
BFT	Blue Force Tracker
BLOS	Beyond Line of Sight
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
C2	Command and Control
C4	Command, Control, Communication, and Computers
CAC	Common Access Card
CAI	Common Air Interface
CBE	Capabilities Based Experimentation
CCI	Controlled Cryptographic Item
CDMA	Code Division Multiple Access
CERCEC	Communications-Electronics Research, Development, and Engineering Center
CNSS	Committee on National Security Systems
COC	Combat Operations Center
COMSEC	Communication Security
CONUS	Continental United States
COTS	Commercial off the Shelf
CSCHR	Consolidated Single-channel Handheld Radio
CTIA	Cellular Telephone Industries Association

DACT	Digital Automated Communication Terminal
dBm	decibel milliwatt
DDACT	Dismounted Digital Automated Communication Terminal
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DNS	Domain Name Server
DoD	Department of Defense
DSP	Digital Signal Processor
DSSS	Direct Sequence Spread Spectrum
ECDH	Elliptic Curve Diffie-Hellman
FHSS	Frequency Hopping Spread Spectrum
FIFO	First-in First-out
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
GHz	Gigahertz
GOTS	Government Off-the-Shelf
GPR	Government Purpose Rights
GSM	Groupe Spécial Mobile or Global System for Mobile Communications
H&S	Headquarters and Service
HAIPE	High Assurance Internet Protocol Encrypter
HF	High Frequency
HLR	Home Location Register
IEEE	Institute of Electrical and Electronics Engineers
IISR	Integrated Intra-squad Radio
INFOSEC	Information Security
IntServ	Integrated Services
JP	Joint Publication
JPEO	Joint Program Executive Office
JSIC	Joint Systems Integration Center
JSOC	Joint Special Operations Command
JTRS	Joint Tactical Radio System

Kbps	Kilobytes per second
LAN	Local Area Network
LOA	Limited Operational Assessment
LOS	Line of Sight
LPD	Low Probability of Detection
LPE	Low Probability of Exploitation
LPI	Low Probability of Interception
LTE	Long Term Evolution
LUA	Limited User Assessment
MAC	Medium Access Control
MANET	Mobile Adhoc Network
MBITR	Multi-band Inter/Intra Team Radio
MBMMR	Multi-band Multi-mission Manpack Radio
Mbps	Megabytes per Second
MDACT	Mounted Digital Automated Communication Terminal
MHz	Megahertz
MILSATCOM	Military Satellite Communication
MIMO	Multiple-Input Multiple-Output
MMHR	Multi-band Multi-mission Handheld Radio
MSC	Mobile Switching Center
MTU	Maximum Transmission Unit
mW	milliwatt
NSA	National Security Agency
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnectivity
OTG	On-the-Go
P2P	Peer to Peer
PAN	Personal Area Network
PCS	Personal Communication Services
PDA	Personal Digital Assistant
PPLI	Precise Position Location Information
QoS	Quality of Service

RDECOM	Research Development and Engineering Command
RDN	Rapidly Deployable Network
RF	Radio Frequency
RN	Radio Node
RNC	Radio Network Controller
SCA	Software Communication Architecture
SDR	Software Defined Radio
SHA	Secure Hash Algorithm
SME PED	Secure Mobile Environment Portable Electronic Device
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
TacBSR	Tactical Base Station Radio
TCP	Transmission Control Protocol
TH	Time Hopping
TNT	Tactical Network Topology
UDP	User Datagram Protocol
UHF	Ultra High Frequency
USB	Universal Serial Bus
USRP	Universal Software Radio Peripheral
VHF	Very High Frequency
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WID	Waveform Identification
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Executive Summary

Communications are essential for maintaining the tempo of operations in modern warfare. Nonetheless, Marines are consistently required to fight battles with outdated communication technology. For example, dismounted tactical radios are primarily used for voice-only communications, because of an inconvenient data side. This thesis research started with the premise that the discrepancy is not simply the demands of operational security, but compounded by the inability of military-oriented communications systems to keep pace with the capabilities of ever-emerging commercial and consumer-oriented systems. Major corporations daily leverage Web email, other messaging services, video and picture sharing, telephony, collaborative applications and teleconferencing—all from commodity cellular handsets. Furthermore, the individual customers receive a plethora of services from a variety of providers, which significantly enhance their everyday life. However, commodity cellular devices are few and far between in the Marine Corps. Only select commanders, recruiters, or acquisition officers, while in a garrison environment, are issued consumer-grade cellular handsets for official use. There are many reasons for this phenomenon, but the most prevalent in this author's opinion is the poor cost-to-benefit return on investment given current operations constraints including security vulnerabilities on the use of such devices. Simply stated, it would cost the government too much money within the current market to retrofit every Marine, Sailor, Soldier, and Airman with cellular handsets, when their use would be limited to garrison environments. However, if all Service members were issued a cellular handset included in their initial seabag to be used with full capability:

- for the duration of their service time,
- in a garrison environment with either a commercial carrier or military installation network, or
- in a combat environment,

the benefit would outweigh the cost. The idea leverages one cellular handset to function and operate in every situation. To offset the cost even more, certain personnel would not receive a carrier service plan and therefore would be restricted to on-base military-owned cellular networks. These implementations may seem idealistic and impractical; however, with the current technology and establishment of appropriate user-level agreements this capability is attainable.

For each relevant environment, including garrison, operational, forward operating base, etc., a different communication architecture is suggested. For example, while in a garrison environment, most military bases have commercial cell towers that provide limited coverage, since some installations occupy large unimproved training areas. This environment would be suitable for a mobile base station, which contains all the services in two man-portable cases. These base station devices are vehicle mountable and could be driven to the training site when required. Alternatively, the military could purchase permanent infrastructure to support military-owned base station towers. Such implementations also carry the potential to reduce wired-infrastructure maintenance or replacement requirements.

Currently, forward deployed fire-teams and patrols are very limited in their communications options, usually relying on multipoint-to-multipoint push-to-talk voice radios. Commercial technologies offer a means to catapult the current operational tactics, techniques, and procedures by integrating very mobile cellular systems and handsets into the software defined radio architecture. In so doing, very light, highly mobile forces can be supported in the field without a significant outlay of communications infrastructure.

An important issue to consider is frequency allocations. Commercial cellular handsets are configured to operate on specific bands, which mostly are not owned by the government. However, some bands still exist and could be leveraged. Alternatively, perhaps a licensing of the frequency space could be acquired for areas within the confinement of military installations.

In consideration of all these issues, the most realistic approach leverages preexisting cellular infrastructure, either in a garrison or tactical environment. The industrialized world has already spent a significant amount of money to allocate fixed telecommunications infrastructure for the densely populated areas. Therefore, any additional equipment would just increase the coverage and reliability of the existing network. However, for all other areas this thesis develops three main approaches to integrating the cellular handset capability, (i) tethered, (ii) indirect (bridging), (iii) direct (wireless) through a commercial standard, military waveform, or modified commercial wireless protocol.

The tethered concept would facilitate immediate procurement and adoption of the cellular handset capabilities for highly controlled emission environments. Within a convoy vehicle or during foot-mobile movement-to-contact scenarios, the handsets could be plugged into tactical radios via a tethered cable to provide communication. This method would essentially give the operator, based on a mission-based permission scheme, access to a worldwide network of data (classified or unclassified), without compromising any emission security, because all inherent wireless interface on the handset would be disabled.

The second concept (indirect or bridging) leverages commercial cellular mobile base stations, as mentioned in the first example, to communicate with cellular handsets, simultaneously interconnecting with the backhaul via military tactical radios. This concept will provide forward operating bases or military training areas with high-capacity cellular connectivity without the dependency of commercial service providers. These individual base station nodes range from having a small squad size to battalion-level network capacities, with the ability to interconnect multiple legacy devices and form modular, base-level infrastructures.

The third concept (direct) leverages inherent military tactical communication devices (radios) to host the local cellular networks. This can be accomplished by adding a commercial standard protocol to suitable radios that have already been purchased. However, this capability would need to be restricted to non-essential missions, as the standard cellular protocols do not use typical emission controls to prevent or limit the enemy's signal interception or exploitation. Alternatively, a military wireless protocol (waveform) could be used for hosting the cellular networks, if the handsets were equipped with the protocol. However, this approach seems unrealistic considering most handsets are not designed with the radio frequency front end to support such protocols. Finally, the preferable solution is a modified commercial cellular protocol. This concept evaluates commercial cellular and military protocols for their desirable traits from an integration perspective. Based on these traits, the Marine Corps could integrate essential secure characteristics and low-cost methods to form a new standard, which would only require firmware upgrades to host the cellular networks directly from tactical radios.

Based on these concepts, the experiments explore the suitability, feasibility, and complexity of integrating these two domains—commercial cellular technology and mission-oriented tactical military communications architecture. The insights gained strongly suggest great potential for securely integrating cellular technology without incurring unmanageable vulnerabilities or costly solutions. Starting at the lowest layer, most people would blindly assume that the emissions from 3G cellular technology would be too vulnerable for use in a tactical environment. However, as the results in Chapter IV suggest, cellular handsets with power control capabilities significantly reduce their transmission power when they are relatively close to the base station, potentially masking the handset emissions. In a side-by-side comparison, it appears that tactical radios capable of producing low probability of intercept and exploitation signals can be more detectable than a standard WCDMA cell phone (i.e., when leveraging the power control functionality). Additionally, if the signal is not detectable, then it is not possible to intercept or exploit the emissions. This conclusion only holds true for the cellular handset, because standard cellular base stations are not capable of absolute power control. This makes sense, because the power control functionality was designed to minimize interference between CDMA channels including extending the battery life on handsets. This is not necessary for the base station, since it provisions multiple devices simultaneously and the power supply is not typically limited. This insight is extremely valuable, because this low-complexity solution increases the desirability of integrating cellular handset by modifying the cellular protocol to operate on military tactical radios.

Another key concern is the traditional throughput rates normally found in military communications. Over the past decade, our tactical radios have made monumental advances, which allow wireless, multi-hop networks to autonomously develop without human interaction. In addition to multiple nodes, these interoperable networks are capable of surpassing megabits per second transmission speeds; at this rate, live streaming video is possible without any significant, perceptible delays. However, without traffic policing at the flow level, certain applications might monopolize the link. This capability is not normally found on modern dismounted tactical radios. Therefore, it is important for the radios to have a robust implementation of buffer overflow management to prevent crashing in the middle of congestion.

There are a significant number of other concerns with integrating the cellular handset capability; however, these concerns seem manageable through software configuration adjustments or programming of additional security layers. In the end, this research strongly suggests leveraging commercial cellular handsets in order to enhance battlefield operations capabilities; the return on investment in terms of improved or added operational capabilities is well worth the expense. Consider the ramifications of troops on the ground being able to see a bird's eye view of the battlespace while negotiating through an urban environment. In order to keep up with the highly evolving and innovative world, the military should continue to evaluate commercial technology for possible solutions to an ever-increasing collection of operational-use-cases.

THIS PAGE INTENTIONALLY LEFT BLANK

I. Introduction

A. Problem

The research idea was motivated by the current lack of communication capabilities observed by Marines while in a tactical/field environment. In a non-field environment (garrison), worldwide communication is possible by dialing or texting from a wireless device such as a cell phone that is readily available today. A cell phone has the capability to send and receive real-time voice communication, voice messaging, text messaging, and e-mail and to capture/send videos or pictures, in addition to possessing a long list of other features. However, the cost of using this technology in a field environment has traditionally been too high because of the need for permanent infrastructure or sophisticated hardware requirements.

Imagine highly mobile units either providing disaster relief and humanitarian assistance or conducting full-scale combat operations. These missions share similar characteristics, which routinely require a highly mobile, ad-hoc wireless network to provide successful communication. Normally, cell phone towers and/or pre-laid cables could provide a solid communication backbone for a commercial network. However, these assets in a tactical environment are usually unsecure, unavailable, or inefficient. Therefore, the units are forced to use internal wireless communication assets. Today, technology exists within the commercial industry enabling stand-alone (cellular infrastructure independent) cellular networks. The mobile base stations that host these networks are man-portable and modular by design. The modular design allows the cellular Local Area Network (LAN) to extend the existing Wide Area Network (WAN) through a common interface based on the Internetworking Protocol (IP) standard. Therefore, if Marine Corps tactical communication networks were IP-based, the interoperability problem would be reduced in magnitude. However, these mobile base stations still broadcast with vulnerable wireless protocols.

The purpose of this thesis is to accomplish the following: (1) highlight the limitations of the military's wireless communications, (2) explain the advantages of commercial cellular technology, and (3) identify various solutions to leverage these advantages, reduce these limitations, and, ultimately, integrate the technologies without compromising security or reliability. This thesis explores the idea of wirelessly connecting cell phones to a Marines Corps tactical radio network by manipulating the software stacks on both the standard cell phone and the software defined tactical radio to enable secure wireless connectivity to pre-established military networks. The Marine Corps' communication infrastructure was chosen because of readily available resources including the author's background as a Marine Officer; however, the results from the research are applicable to every US Military Service.

In various missions ranging from jungle to urban to desert environments, all Marines on the ground share a common need for reliable and secure communications. Typically, infantry units, regardless of mission, are spread out across a diverse battlefield and are extremely dependent on their ability to communicate with US and Allied Forces.

B. Research Questions

The thesis research attempts to answer the following questions. The first three are the primary research questions—essentially, all things considered, is it feasible to connect a commercial cellular handset to a military communication network? The remaining questions attempt to answer more specific areas of concern: How much risk is evolved, how much will it cost, and what is the benefit received, given the risk?

1. Is it possible, while maintaining cost efficiency and security integrity, for Service personnel to communicate via a standard cell-phone device to an ad-hoc, wireless, highly mobile tactical network, with the ability to send data or voice across the attached Wide Area Network?

2. Is it possible to create a secure, wireless cellular handset network from a tactical radio via standard military waveforms (i.e., not through standard cellular signals) without significant hardware changes, while maintaining Low Probability of Detection (LPD), Low Probability of Interception (LPI), Low Probability of Exploitation (LPE) and Anti-jam (AJ) signal requirements?

3. Is it possible to create a secure, wireless cellular network from a tactical radio via an external 3G/4G bridge device without significant hardware changes to standard cell phones, while maintaining LPD, LPI, LPE, AJ requirements?

4. Is it possible to connect wirelessly to a cell phone to a dual-mode/channel tactical radio via a Radio Frequency (RF) 3G/4G chip-set, internal to the tactical radio?

5. Which of the three topologies listed as the first three questions in this section is more effective in delivering information to end-host?

6. Is it possible to create an ad-hoc, wireless network of cell phones without the attachment of cell towers (base stations)?

7. Is it possible to reprogram the radio stack onboard open-source smart phones?

8. Is it possible to reprogram the radio stack onboard inherent tactical radios?

9. Is it possible to configure a Software Defined Radio (SDR) to communicate with both a smart phone and a network of tactical radios?

10. If any, given the chosen wireless configuration from above, what would be the limitations of the new wireless link?

11. What capabilities can the smart phone bring to the network?

12. What is the data throughput for each of the proposed topologies?

13. What security questions arise?

14. Of the new security vulnerabilities, what actions can be taken to minimize risk?

C. Thesis Organization

This chapter provides an overview of the known problems within the military's communication infrastructure. The chapter suggests some objectives that can be achieved after a successful integration of technologies. Finally, the chapter outlines the research questions most of which were evaluated by the Naval Postgraduate School, Military Wireless Communications research group.

Chapter II. The background chapter provides definitions and a general understanding of information surrounding the area of military wireless and commercial cellular communications. The main purpose of this chapter is to define, clarify, or eliminate any ambiguous terms. The chapter will attempt to highlight advantages and disadvantages within military and commercial communications, compare each of the technologies, and explain related work surrounding the research area.

Chapter III. This chapter describes three concepts: tethering, indirect, and direct, which all seem feasible for integrating the technologies. Some additional concepts are mentioned in this chapter to provide a comprehensive review, but seem infeasible for a long-term solution from a theoretical perspective (i.e., some concepts were not explored enough to determine feasibility).

Chapter IV. This chapter explains two exploratory studies and two experiments that were conducted to evaluate the concepts identified in Chapter III. Since this technology is relatively new and undeveloped in the military, the indirect (bridging) concept was chosen to highlight common misnomers and identify possible solutions for mitigating the risk. By identifying some solutions, this should facilitate shorter acquisition schedules for procuring the technology.

Chapter V. This chapter consolidates the concepts developed in Chapter III with the results found in Chapter IV to conclude on possible routes for future work.

II. Background

This chapter identifies and characterizes military and commercial communication assets normally allocated to company-level units, and details the limitations specific to each device. Additionally, the chapter defines a set of metrics for comparing military and commercial communications. Finally, the remainder of the chapter explains prior work surrounding the integration of cellular communication integration with military wireless communication networks.

A. Military Wireless Communications

1. Unit Composition

A traditional Marine Corps infantry battalion is comprised of four companies: a Headquarters and Service (H&S) Company, three Rifle Companies, and a Weapons Company. For this work, the communication assets available to the H&S Company are not considered because these assets can be similar to the company-level units, but not generally (i.e., tailored by the battalion's mission requirements). In addition, these assets are normally used to establish intra- and backhaul communications. Normally, the remaining four companies are an extension (i.e., child node) to the H&S Company (i.e., parent node). Although mission-dependent, the Weapons Company assets (i.e., personnel and equipment) are usually attached to a Rifle Company. Therefore, for this thesis, I will discuss methods to leverage company-level communication assets by integrating cellular technology in order to enhance a typical Rifle Company's mission. A company-sized element consists of four Platoons (three Rifle and one Weapons Platoon), totaling about 150-180 personnel. Each Platoon consist of three squads, totaling about 33–45 personnel. Each squad consists of 12–15 personnel, divided into three or four teams. (Command, 2010)

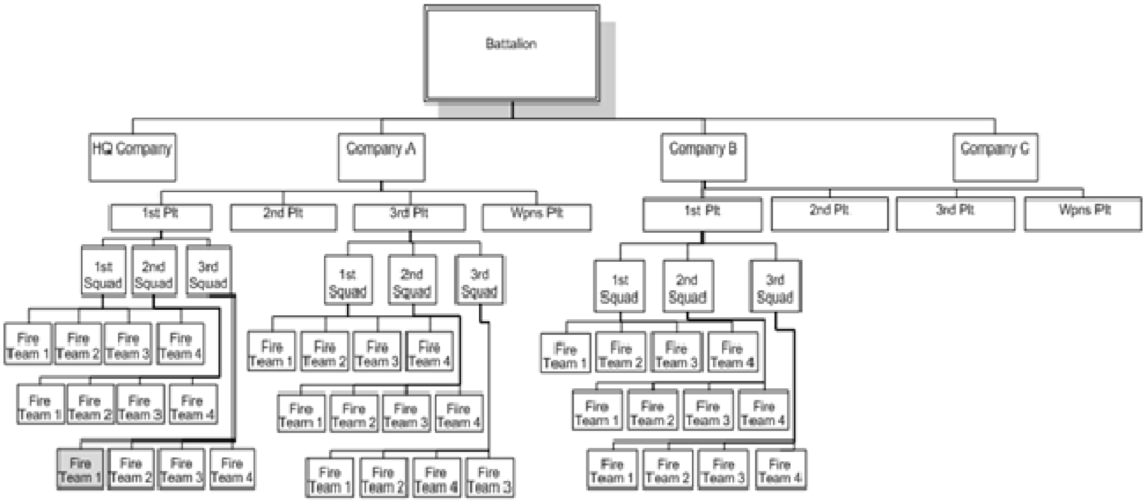


Figure 1. Unit Composition Breakdown[1]

2. Communication Assets

A company-sized element’s communication assets can be categorized into two groups: manpack (man-portable) and vehicle-mounted. The assets associated with manpack allocations are as follows: four High Frequency (HF)/Very High Frequency (VHF) AN/PRC-150(C) High Frequency Manpack Radios (HFMRs), 21 VHF/Ultra High Frequency (UHF) AN/PRC-148 V2(C) Multi-band Inter/Intra Team Radios (MBITRs), and four VHF/UHF AN/PRC-117F V1(C) Multi-band Multi-mission Manpack Radios (MBMMRs). The assets normally connected within vehicles are mounted with amplifiers, which cradle the radios listed above to increase radio frequency (RF) transmission power. Some additional assets that are available to infantry companies, depending on assigned missions, could include the following: the Blue Force Tracker (BFT) with a Dismounted Data Automated Communications Terminal (D-DACT), the AN/PRC-152 Multi-band Multi-mission Handheld Radios (MMHRs) as an alternative to the PRC-148, and the AN/PRC-153 Integrated Intra-squad Radios (IISRs) as common fillers for intra-squad communications. The above list is not an all-inclusive list, but it highlights the common communication assets normally available to ground infantry units. Units that are more mobile and missions of greater communications dependency will require a significant deviation from the above composition. (Command, 2010)

a. Limitations

(1) Cost. Given the austere environments, high tempo, and high mobility associated with every mission, Marines require extremely sophisticated wireless communication devices. Due to the level of sophistication needed (i.e., security and reliability requirements) these devices are designed specifically for desired military applications; as a result of the limited consumer base (i.e., not enough product volume to offset cost), the production cost is much higher than for the commercial equivalent. According to acquisition managers, in an attempt to mitigate the high associated cost for Government Off the Shelf (GOTS) equipment, the conventional requirements are placed up for bid, with the lowest bidder sometimes receiving the contract. Once the vendor is chosen, those initial requirements are refined throughout the acquisition lifecycle of the technology, which inadvertently drives the cost back up and drags the production time out across multiple years. Additionally, with the emerging technology radically fluctuating throughout the acquisition process, the fleet ultimately ends up with overpriced, outdated technology.

(2) Voice Channel Limitation. Traditionally, at the lowest level, a ground unit radio has the capability to communicate via a voice channel, usually half duplex (i.e., only one side communicates at a time) and circuit switched (i.e., one frequency per group of connected nodes). These limitations cause voice communications to be conducted in a push-to-talk fashion. This push-to-talk function causes problems either due to unintentional "keying of the handset" (i.e., someone holds the handset button down for an extended period of time) or an extended transmission (i.e., the sender fails to un-key the handset or pause in a long message).

[1] Hypothetical and self-generated graphic from author's knowledge of the internal Battalion-level

(3) Data Channel Limitation. The radios allow a data channel in addition to a voice channel; however, these channels are limited in throughput (mostly attributable to the lower bandwidth of the lower military frequency bands). To communicate through the data port, an external device is required, normally a laptop computer. When conducting foot-mobile missions, the possibility of conducting a security halt to connect a laptop to the manpack radio is normally impractical or not desirable; this leads the foot mobile missions usually relying solely on voice communications.

(4) Form-factor. Over the years, the form-factor of military tactical radios has significantly improved. According to multiple senior military officers, the purpose of radio asset from their inception has historically been backhaul communication and the internal communications were accomplished by wire. This was the case because radios were in limited supply and therefore only dedicated for situations where wire communications were not convenient or suitable. Today, ground units deploy multiple manpack radios (backpack size), supplemented with handheld radios in order to effectively coordinate complex operations. However, the size of the handheld is roughly similar to the size of a common red builder's brick. From observation of currently fielded handheld devices, it seems that the level of security directly corresponds to the physical size and weight of the device. The current form-factor facilitates ease of use for voice communications, but fails to provide data accessibility.

(5) Interoperability. At the fire-team level, as displayed in Figure 1, teams are normally given handheld IISRs. By design, these devices only communicate with other IISRs. This creates a human-in-the-loop architecture beyond the fire-team level. In addition to the IISRs, squad leaders are normally allocated Joint Tactical Radio System (JTRS)-compliant Consolidated Single-channel Handheld Radios (CSCHR) (i.e., Army Navy / Portable Radio Communication 148's (AN/PRC-148s) or

manpower structure; data supported by (Command, 2010).

AN/PRC-152s) to communicate with higher levels. These devices permit cross-unit communications via frequency tuning and within specific communication ranges. The limitation exists when fire-team levels wish to communicate directly with other personnel outside of their IISR range. Because units normally try to maintain communications with at least their higher-command unit, as depicted in Figure 1, lower levels can only communicate laterally via the human-in-the-loop tree structure. This can cause problems when it is essential for timely information to be distributed across units. For example, suppose a unit has artillery guns in direct support of their mission. Direct, continuous communication is essential when maneuvering through mission phases and negotiating between the different battlefield positions. If the squad-leader's radio fails, then a platoon's radio may be used. However, if all nodes were interoperable and interconnected, then the fireteam's could transmit the valuable information. When information is required to traverse multiple networks before reaching its final destination, the human-in–the-loop method is not adequate under time constraints. These limitations severely restrict Commercial Off-the-shelf (COTS) cellular handset integration attributable to the associated ubiquitous networking requirements of modern data capabilities.

b. Device Profiles

(1) HF Asset. The intent of an HF asset is for long-haul communications. The HF band allows the signal to travel Beyond Line of Sight (BLOS), with the ionosphere acting as a reflector (Couch, 1990). The PRC-150 (Figure 2) radio (frequency range 1.6 to 59.99 MHz) is normally setup as a reach back to the Combat Operations Center (COC) or other distant units (Harris Corporation, 2009). Although the HF band allows longer distances (i.e., exploiting ionosphere reflecting) the associated channels are limited in throughput. Claude Shannon's channel-capacity equation[2] directly ties the bandwidth of the single-input single-output channel to the

[2] $C = B \log_2 (1 + S/N)$, C is channel capacity (bits/sec), where B is bandwidth in Hz, S is the average signal power in Watts, and N is the average noise power on the channel (Couch, 1990).

maximum possible data rate (i.e., more bandwidth is available at the higher-frequency bands, 27MHz in HF vice 2.7GHz in UHF) (Couch, 1990). Due to limited data rates available in the HF band, the radios are normally only utilized during long distance circumstances. Even on a voice-only transmission, the HF band is less desirable due to its short delay. The sender is required to speak slowly and clearly to ensure the message is effectively passed. The PRC-150 is capable of transmitting above the HF band. However, its signal is no longer reflected but, instead, scattered by the ionosphere allowing it to achieve similar distances (Couch, 1990).

Figure 2. AN/PRC-150C
(Harris Corporation, 2009)

(2) VHF Asset. Unless the conditions require HF assets, foot-mobile troops traditionally use the PRC-148 (Figure 3) / PRC-152 (Figure 4) radios due to VHF/UHF capabilities. The radios are more user-friendly because of their lighter weight[3] and smaller size[4]. However, due to the frequency range (30 – 512 MHz) and power capacity (emits ~0.1–5 Watts (W), except the PRC-152 has a SATCOM capability at 10W) the radios are limited in range (Harris, 2009; Thales, 2005). Both radios are considered Type 1 level devices. These radios can be very useful for voice communications, but for data transmissions, the devices need a dongle attached to the side. The data capability is not designed for use while on the move. For foot-mobile troops, this capability does not seem feasible without a long security halt.

[3] PRC-148 - ~2 lbs; PRC-152 - ~2.5 lbs (Harris, 2009; Thales, 2005)

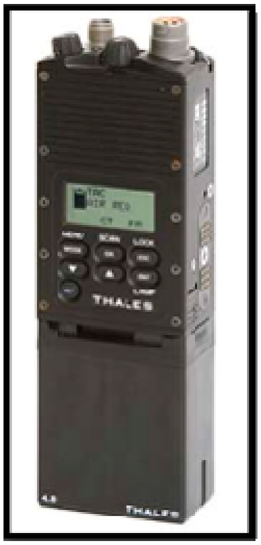


Figure 3. AN/PRC-148 V2(C)
(Thales, 2005)

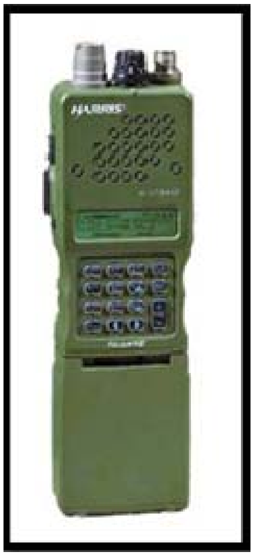


Figure 4. AN/PRC-152
(Harris, 2009)

(3) UHF Asset. Although the majority of Marine Corps units are currently fielded with the AN/PRC-117F, the AN/PRC-117G (Figure 5) is shortly expected to replace this older version (Command, 2010). The PRC-117G version will be explored and evaluated for the remainder of this thesis due to its ground-breaking technology compared to historical assets. This radio is the functional equivalent of the radio illustrated in Figure 4 (VHF / UHF asset). In addition to the visible size/weight increases between models, the AN/PRC-117G contains a proprietary waveform (Adaptive Networking Wideband Waveform (ANW2)) which facilitates a wireless Mobile Ad hoc Network (MANET) capability and extends the frequency range up to 2 GHz. The AN/PRC-152 and AN/PRC-117G are part of the Harris Falcon III family, which is one of the Marine Corps first Software Communication Architecture (SCA) compliant Software-Defined Radios (SDR) (Command, 2010; Turner, 2006; Thales, 2010). The JTRS SCA functionality allows firmware upgrades to include future-undeveloped protocols (Turner, 2006). Therefore, if cellular

[4] PRC-148 - ~8.5”H X 2.6”W X 1.5”D; PRC-152 - ~10”H X 3”W X 2”D (Harris, 2009; Thales, 2005)

technology is plausible for military applications, the software solution must also include the capability to upgrade to future undeveloped protocols.

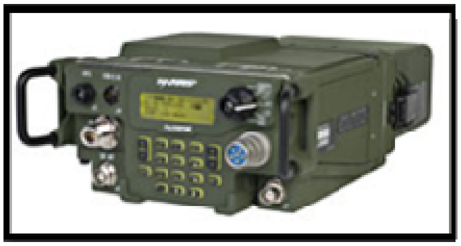


Figure 5. AN/PRC-117 V1(C)
(Harris Corporation, 2009)

(4) Data Asset. Within a battalion-level or higher COC, data can be passed via an established computer network with switches, routers, and laptop computers. However, although generally mission-dependent, the mobile war-fighter can utilize the Blue Force Tracking System for data transfers via an external Data Automated Communications Terminal (DACT). The COC establishes the command node with all subordinate units in order to send communications or location information via text messages on a near-real-time basis. The vehicles are equipped with a Mounted DACT (M-DACT) that provides mapping functionality with a texting capability. The D-DACT (Figure 6) provides the same information as the M-DACT, but in a handheld form-factor. This device is essentially an enhanced Personal Digital Assistant (PDA) (Operator's and Organizational Maintenance Manual - Dismounted Data Automated Communications Terminal, 2006). A reoccurring theme with the D-DACT is the cost-to-benefit argument. These devices support GPS functionalities, an extremely useful tool when navigating through unfamiliar territory. However, beyond the map overlays and texting advantages, the devices are not used. According to a shipping invoice document, the D-DACT is listed at about $10,000 per unit (Stanley Associates, 2009). In addition to the tethering requirement for data transmissions, the device is extremely expensive, given that the average utilization provides only texting functionality or map overlays. Although the devices

are extremely useful, they are underutilized because of their size, tethering requirements, and high production cost.

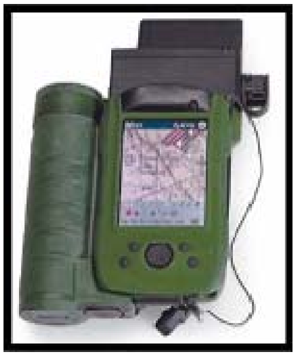


Figure 6. D-DACT
(Halenda, 2004)

B. Commercial Wireless Communication Assets

For internal communications (within a corporation, for example), security departments can use some variant of a walkie-talkie. These communication networks are not interoperable with other networks. In other words, they were intentionally built to operate on a circuit-based voice channel without data capabilities. These non-data, non-interoperable, and voice-only constraints are similar to the military's IISR limitations. Since modern warfare demands an extensive intelligence network dependent on data capabilities, these types of devices are insufficient.

What is the most widely used, handheld wireless, highly capable, and data-equipped, communication device throughout the commercial industry? According to a Cellular Telephone Industries Association (CTIA) 2009 volunteer survey (representing data from 95.9% of service providers) there existed over 273 million US wireless subscribers that year (CTIA - The Wireless Association, 2010). According to the US Census Bureau, the US population for 2009 is estimated at 307 million people (US Census Bureau, 2009). These numbers seem to suggest cell phones are the most popular communication device in the country. The traditional

Global System for Mobile Communications formally known as Groupe Spécial Mobile (GSM) cellular infrastructure is designed around a reliable land-base centralized architecture, as depicted in Figure 7. The architecture is dependent on the Mobile Switching Center for cell phones in order to provide communication with outside networks. If a Base Transceiver Station (BTS) fails, then all the nodes in its own cell will stop working unless another neighboring BTS is within range of the cell phone. If components higher up the tree structure fail, then the branch is down until the component is back up or another BTS takes over (Lin & Chlamtac, 2001).

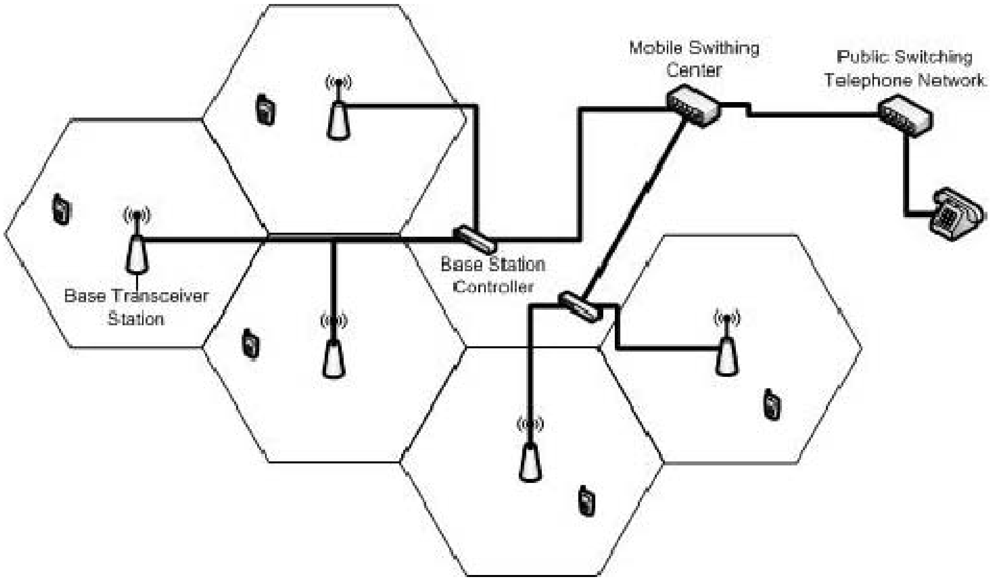


Figure 7. Typical MSC-BSC Architecture[5]

1. Cell (Smart) Phone Capabilities

Rated by *PCWorld*, the top-ten cell phones on the market as of June 2009 were three versions of the Blackberry (made by Research in Motion), the Motozine (made by Motorola), the Omnia (made by Samsung), the G1 and Sidekick (made by T-Mobile), the PRE (made by Palm), the iPhone (made by Apple), and Cable (made by Monster) (PCWorld, 2009). All phones were priced at $200 or less except for one

[5] Author-generated graphic based on (Lin & Chlamtac, 2001)

phone, which was priced at $400. The average battery life for the top five phones was nine hours of talk time. The average dimensions were approximately 2 inches wide by 4 ½ inches high by 1/2 an inch deep. As shown in Figure 8, these devices were designed as small form-factor wireless cellular devices.

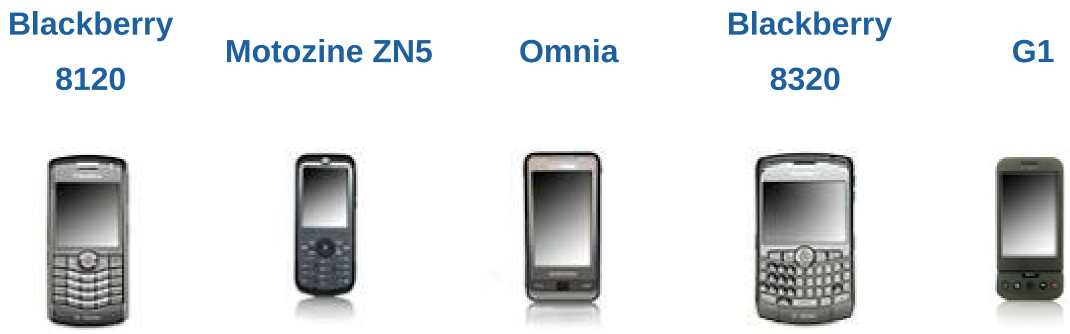


Figure 8. Top Five *PCWorld* Ranked Cell Phones, June 2009
(PCWorld, 2009)

These third-generation (3G) cell phones utilize either a GSM or Code Division Multiple Access (CDMA) variation for cellular connectivity. The traditional quad-band frequencies utilized for communications are 850/900/1800/1900 Mhz. The common data rates observed by a 3G network varies significantly, but at the high end (more applied rate vice theoretical ceiling), the ceiling is around 386 Kbps (Ergen, 2009). Furthermore, these devices are capable of sending data across a Wireless Fidelity (WiFi) connection. This capability is extremely valuable for areas without traditional GSM/CDMA coverage, but with Wi-Fi access. Using this Wi-Fi capability, phones are able to transmit data. One of the Blackberry phones leverages voice-over-Wi-Fi--meaning that in areas with weak cellular signal the phone is able to leverage the Wi-Fi connection to enhance the quality of the connection. The majority of these phones have an internal Global Positioning System (GPS) receiver. This feature enables Precise Position Location Information (PPLI) to be distributed when needed. All these phones share a common screen size of approximately 2.5 inches in diagonal length and equipped with a color display. The larger screen size permits user-friendly graphics in addition to simple Web browsing. The Blackberry phones allow email delivery with signatures and encryptions via a Common Access Card (CAC).

All devices contain features including text messaging, e-mail, instant messaging (social networking), an additional expansion card (more memory), a digital camera for video and pictures, an internal microphone, multimedia capabilities (i.e., MS Word, PowerPoint, Excel, Video/Audio player, etc.), and personal computer (PC) synchronization capability via Bluetooth or a Universal Serial Bus (USB) cable. The Blackberry allows PC synchronization through an over-the-air connection. This allows all synchronizations and backups to occur routinely through the normal data channels. Essentially, all phones could have a personal server that would maintain updated backups in the case of a lost or destroyed phone, thus eliminating long turnaround times for the replacement phone. The majority of these phones contain a keyboard (either on the face or a pull-out version), increasing the ease of composing long text or e-mail correspondence. Also, although not listed as a feature of one of the top phones, there exists the capability to participate in video teleconferences. These phones (e.g., the Nokia N95 model) contain two cameras—one on the front and one on the back for normal pictures and video media.

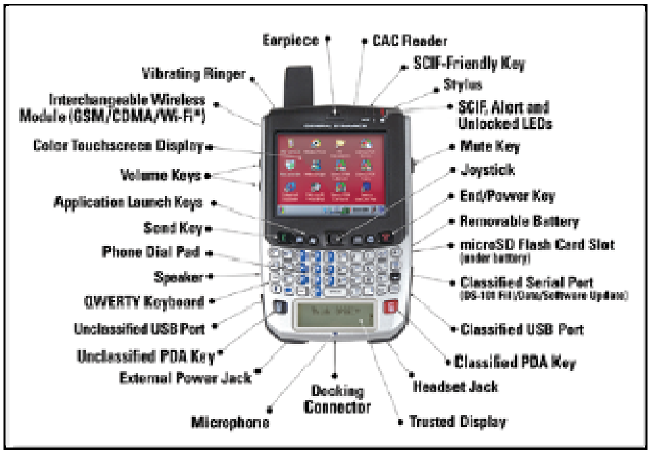


Figure 9. Sectera Edge Smartphone (SME PED)
(General Dynamics, 2009)

The commercial industry does sell a secure wireless cell phone (Figure 9, Sectera Edge Smartphone or the Secure Mobile Environment Portable Electronic Device (SME PED)), made by General Dynamic C4 Systems. The device is certified by the National Security Agency (NSA) for protecting classified information at the "Top Secret" level and below. The phone is capable of Type 1 and non-Type 1 encryption, and it meets the MIL-STD-810F specifications for environmental consideration. The phone runs on a Windows Mobile variant; however, the cost per device is listed at $3000 per unit (General Dynamics, 2009). Other devices in the commercial market have similar characteristics; therefore, this device is representing that category of cellular handsets (Sierra Nevada Corporation, 2006; L-3 Communications, 2009).

A new generation of cellular technology is emerging called Fourth Generation (4G). The major difference between 3G and 4G is the throughput rates; the 3G advertises rates just over 1 Mbps and the 4G proposes to scale above 50 Mbps (these are theoretical rates vice applied). The most promising standards are the Institute of Electrical and Electronics Engineers' (IEEEs) 802.16e, also known as Worldwide Interoperability for Microwave Access (WiMAX) and 3rd Generation Partnership Project's (3GPPs) Long Term Evolution (LTE) variants. By design, the 4G signals are drastically different than the 3G signals in order to account for the desired data rates. These 4G standards leverage Orthogonal Frequency Division Multiplexing (OFDM) and Multiple-Input and Multiple-Output (MIMO) to enhance the air interfaces (Ergen, 2009).

C. Military versus Commercial Communications

What is the difference between military communication and its commercial equivalent? To effectively evaluate this question, a set of criteria needs to be established for comparison. This section outlines and defines the criteria, which includes the following: architecture, security, Quality of Service (QoS), interoperability, modularity, portability, and design features.

1. Architecture

Architecture is defined within the *Joint Publication (JP 1-02)* as, "a framework or structure that portrays relationships among all the elements of the subject force, system, or activity”(DoD, 2009). Therefore, communication architectures include all assets required to form a communication network. Within a company-sized unit, two radios are the minimal assets required to form a communication network. Military communications need to have the ability to communicate in an ad-hoc manner. Although all radios within a company are not interoperable, the ability for two people to communicate directly without an intermediate node does exist (e.g., a squad with IISRs can communicate through a common channel, or squad leaders with MBITRS can communicate). However, the typical cellular infrastructure is not setup this way in the commercial sector. The traditional Personal Communications Services (PCS) network architecture includes base stations (BS), Mobile Switching Centers, and Publicly Switched Telephone Networks. For a cell phone call to be initialized, the call needs to traverse this PCS network (Lin & Chlamtac, 2001). However, to create a minimal cellular network (i.e., two connected cell phones) only one mobile base station (i.e., a pico cell) is required. The primary limitation with all cellular architectures is this intermediate node (i.e., peer-to-peer communication is non-existent)—as opposed to most military tactical radios, which do not require an access point for network connectivity. Given the limitation, there are exceptions in which a fixed base station would be acceptable (e.g., on an established military base, or if the radio operator carried the base station with interoperable backhaul communications).

2. Security

Since this thesis deals with radio communications, the security focus will be on wireless Communication Security (COMSEC) concerns. The bulk of the security categories discussed in this thesis were derived from the following definition of communication security: “measure and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security…” (DoD 2009; CNSS Glossary Working Group, 2006).

a. Cryptosecurity

Cryptosecurity is sometimes referred to as content protection or information security. Information systems security (INFOSEC) is defined as "protection of information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to unauthorized users, including those measures necessary to detect, document, and counter such threats" (DoD, 2009). Based on this definition and on the fundamental principles of security, a system must maintain confidentiality, integrity, and availability in order to ensure effective protection of the information (Harris, 2008)—additionally, authenticity and non-repudiation of parties should be considered when discussing electronic transaction security (NSTISSP, 2003).

According to the NSA there are three approved cryptographic protections for military applications, the Federal Information Processing Standards (FIPS) 140-2, FIPS 140-2 with High Assurance Internet Protocol Encryptor (HAIPE), and NSA Suite B (NSA, 2009). The National Institute of Standards and Technology (NIST) established FIPS to protect against INFOSEC threats. The FIPS 140-2 classifications have multiple levels, starting with hardware characteristic requirements beyond the first level (Information Technology Laboratory, 2002).

The NSA defines Suite B as a category of security standards and protocols to protect classified information up to and including the secret level (NSA, 2009). The category was designed to allow flexibility and interoperability of communication assets between the US and US partners. The idea is to allow NSA-certified, Type-1 secure products the flexibility of connecting to the same device without the same controlled cryptographic item (CCI) restrictions. For example, when US Allied Forces partner with US Troops in an operational capacity, the communications assets will no longer hinder interoperability. CCI restrictions have traditionally prohibited the transferring of NSA–certified, Type-1 cryptographic devices to non-US personnel; the Suite B category was created to alleviate this hindrance. Now under the "GOTS for secret process," manufacturers can create two variations of the same device

(NSA, 2009). Therefore, instead of US Troops embedding a communication team, they can distribute just the non-CCI device (Suite B certified) as the interoperable alternative.

b. Transmission Security and Emission Security

This section considers both transmission and emission security, because they are so closely related. Transmission security is defined by JP 1-02 as “the component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis” (DoD, 2009). Transmission security only involves security methods used during the transmission of a signal and, therefore, only protects against layer 1 (physical layer) of the OSI model. One important note is that full-duplex radios can transmit and receive simultaneously, which increases potential for non-stop transmissions, while half-duplex radios can only access one mode at a time.

Emission security differs from transmission security because it refers to security measures for protecting against radiating energy (Wolfe, 1998). The Committee on National Security Systems (CNSS) defines emission security as, “the component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto equipment and telecommunication systems”(CNSS Glossary Working Group, 2006). Essentially, any energy emitting from a radio can be protected in the same way.

In order to protect energy emissions from a radio, the following types of signals are desirable: (i) Low Probability of Detection (LPD), (ii) Low Probability of Intercept (LPI), (iii) Low Probability of Exploitation (LPE), and (iv) Anti-jam (Poisel, 2004). This section refers to the jamming introduced at the physical layer, but jamming at higher layers does exist as well (i.e., jamming the protocol vice the energy). LPD is defined by the CNSS as the “Result of measures used to hide or disguise intentional electromagnetic transmissions” (CNSS Glossary Working Group, 2006). A signal is considered an LPD signal if the adversary is delayed or prevented from determining if a signal exists (Poisel, 2004). This is extremely important for most traditional military applications. LPD can be accomplished by applying a Direct Sequence Spread Spectrum (DSSS) scheme and transmitting at a very low power level. LPI is defined by the CNSS as “the result of measures to prevent the intercept of intentional electromagnetic transmissions” (CNSS Glossary Working Group, 2006). A signal is considered an LPI signal if the adversary is hindered or prevented from capturing the detected signal (Poisel, 2004). LPI can be accomplished by applying a frequency hopping scheme. In some cases, an LPE signal is included within LPD and LPI definitions, but for this thesis the author separates the terms. Since emission security is combined with transmission security, the researcher will consider unintentional and intentional emissions under LPD and LPI. An LPE signal prevents the adversary from leveraging and identifying useful information based on the transmission (Poisel, 2004). For example, if a signal is detected and intercepted by an adversary, but the information is uninterpretable due to cryptography the transmission has some level of LPE. Some of the measures available for reducing vulnerability include the following: reduce emissions (especially when transmitting) power, use narrow beam antennas or antennas with suppressed side-lobes, limit signal duration per frequency, or apply a spread spectrum variant (i.e., spread the signal across a wide-band where adversaries are without synchronization schemes) (Adamy, 2001). By reducing the transmission power, the energy signature is reduced (i.e., limiting transmission power based on the furthest receiving node) and in turn decreases the chances of detectability. In the simplest form, this could prevent or limit an adversary from exploiting the intentional transmissions. However, other factors, such as antenna gain, height, and size, can affect the receivers perceived signal strength, thus allowing the adversary to detect the emissions at a greater distance. Using a narrow band (directional) antenna can prevent signal detection outside of the antenna’s beamwidth (e.g., a 30-degree directional antenna would prevent detection outside of the 30-degrees range). By limiting the duration of transmission per frequency, the likelihood of interception is greatly reduced. This technique prevents frequency scanners from fixing on the transmitted frequency long enough for detection. Techniques for spreading the signal across the frequency band include: Frequency Hopping Spread Spectrum (FHSS), chirping (i.e., sweeping across large frequency range at pseudorandom start times), and DSSS (Adamy, 2001).

A jammer can eliminate communications by applying various jam strategies: noise, tone, sweep, pulse, or smart jamming (Poisel, 2004). Essentially, the purpose of jamming is to increase the noise level to prevent the receiver from differentiating the noise from the signal. Although smart jamming can be the most successful method, it requires significant knowledge of the emitted signal. For example, the IS 95 signal, which requires a separate channel for synchronization, is vulnerable because degradation on this channel could prevent desired communications (Poisel, 2004). However, the jammer would need to know the type of signal being transmitted and specifically jam the synchronization channel. For commercial cellular signals, this method is easily attainable because the standards are, for the most part, readily available.

An anti-jam signal is specifically designed to operate concurrently in a jamming environment. This is normally accomplished by applying DSSS, FHSS, or Time Hopping (TH). A common problem when applying Anti-jam techniques is the synchronization issue. For military applications, due to the nature of a highly mobile, ad hoc wireless network, it is necessary to add and drop nodes on demand. This is fairly easy for non-Spread Spectrum signals, because synchronization can occur during any transmission break. However, for DSSS, the new node does not know the specific net within the spreading sequence. For FHSS, the new node does not know at what frequency the net is set to during entry (Poisel, 2004).

c. Physical Security

Within the military, the primary component of most communication assets is normally considered COMSEC material. This classification requires a higher level of physical security in order to prevent a loss. The hardened physical security policies are established primarily to protect from theft. If an adversary captures or obtains COMSEC material, the likelihood of compromise is imminent even if the device(s) are FIPS 140-2 level 4 compliant. All COTS equipment is not considered COMSEC material until loaded with classified data. As a result, if a cell phone containing only unclassified data were lost or stolen, the level of compromise would be considered minimal in comparison to the loss of a Type 1 secure military radio even without a cryptographic fill.

3. Quality of Service

Every military communication network requires some type of assurances. To ensure reliable communications at the highest level, a Quality of Service (QoS) framework needs to be is established. The current internet is built around a best-effort QoS (Davie & Peterson, 2003). Essentially, the routers implement a First-in First-out (FIFO) queue, and if the routers become overwhelmed, then specific packets are dropped. This is not a problem because at the transport layer, Transmission Control Protocol (TCP) can implement some assurances with an inherent three-way handshake. For military applications, the traditional IP-based networks might not be sufficient. Military networks are based on the individual missions, which are categorized by a real-time, near-real-time, or non-real-time requirement. For example, aviation Command and Control (C2) radar traffic might demand a real-time flow, and general administrative e-mail traffic might only require a non-real-time flow.

When a guarantee is required, two QoS methods are widely accepted within the commercial sector: Integrated Services (IntServ) and Differentiated Services (DiffServ). IntServ provides application or per-flow-level guarantees, where DiffServ provides network traffic class based or service-provider-level guarantees.(Kurose, 2008) The major point for this thesis is that DiffServ will allow the initial DiffServ router to classify the packets based on IP address, while IntServ provides a finer-tuned QoS. IntServ can classify each packet, which, in turn, can allow dynamic scheduling schemes. As explained in the above example, our C2 missions require specific data (air tracks) to have higher assurances than others (email traffic). Therefore, IntServ seems a more desirable method, especially considering that handset data pipes (wireless) are significantly smaller in available throughput in comparison to backbone pipes (fiber).

4. Interoperability

Interoperability is defined by *JP 1-02* as “the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users” (DoD, 2009). For a communication device to be interoperable with other assets, it must at least be able to pass usable information between both nodes at the lowest levels. A level or degree of interoperability greatly depends on the interpretation of the definition of interoperability. For the purposes of this thesis, a system is interoperable if it can effectively exchange useful information between the required layers of the Open System Interconnection (OSI) reference model for sufficient data transfers. For example, radio A is interoperable with radio B if radio A is successful in transferring voice and data communications across a wireless medium to radio B. Today’s military radios require many wireless protocols in order to be interoperable with numerous other military radios; the level of interoperability can be quantified as the number of identical wireless protocols over the total number of wireless protocols. The PRC-152 is completely interoperable with the PRC-148, because they share some identical waveforms.

- Harris PRC-152 waveforms: SINCGARS + AM/FM + APCO P25 + ANDVT + DAMA SATCOM + HPW.
- Thales PRC-148 waveforms: SINCGARS + AM/FM + APCO P25 + ANDVT + DAMA SATCOM

5. Modularity

The IEEE defines modularity as the degree to which a system has independent interchangeable components (IEEE, 2000). Within the Marine Corps, wireless communications assets, the standard military battery (BB-2590/U) for the majority of military manpacks is considered to have high modularity. It does not seem efficient to build interoperable wireless communications with specific batteries in mind. This policy would not only require multiple chargers, but also would prevent spread loading. Consider a company-sized unit with three or four different types of radios and with each platoon spread across the battlefield using equally divided radio assets. Eventually, the busiest radios will deplete the supply of associated batteries. Instead of the unit being able to internally redistribute batteries, because the batteries are specific to certain radio models, they would require another unit to consolidate and redistribute that specific type of battery. Modularity is an extremely important component for military systems. If one component stops working, then Warfighters need the ability to swap parts between internal assets. Otherwise, mission failures will occur due to the incompatibility of specialized systems.

Military radios hold up fairly well in the modularity category. Most requirements are created with backward compatibility in mind. It would be extremely inefficient to replace all associated accessories every time new models are distributed throughout the fleet. Consider the lifecycle of a military communication device. Traditionally, these assets are designed to last a long time. For example, the PRC-117G has a warranty of 5 years, which is extremely significant compared to the one-year limited warranty of today’s most-common cell phones (e.g., the popular Nokia phones) (Harris Corporation, 2009; Nokia, 2009). If a new model or version is produced by the end of every phone’s lifecycle, then we could expect a new cell phone to exist every year. This scenario would produce an inefficient product with low modularity.

6. Portability

The most important characteristic that should be required for all future software acquisitions is portability: the ability to transfer a program (application) from one device to another without having compatibility issues. This is extremely important in the cellular handset world. Since most handsets are relatively new, the developed applications are normally designed for one operating system. For example, this can be a critical issue when the military acquisition cycle takes years to procure a system that the commercial market might make obsolete with the release of a new operating system. Therefore, this specifically designed software would now need to be completely rebuilt.

D. Related Works

1. Tactical Mobile Base Stations

Over the past decade, many commercial vendors have created solutions for a tactical, mobile base station. These base stations provide the same functionality of the traditional cellular infrastructure, except without the large footprint. These devices were designed to mount within a mobile asset and integrate with packet networks. Until recently, none of the vendors have been successful at either selling their product and or at demonstrating an operational requirement, both of which are needed for acquisition procurements.

The Joint Systems Integration Center (JSIC) leads a project called Tacticell, which is tasked with evaluating a cellular system for the Joint Special Operations Command (JSOC). The purpose of the project is to “enhance the situational awareness of the dismounted Special Operations Forces (SOF) teams by providing hand-held wideband communications systems capable of voice, data, and video” (JSIC, 2009). Since 2008, the project has completed three Limited User’s Assessments (LUAs) and one Limited Operational Assessment (LOA) (JSOC, 2009). The purpose of these tests was to assess the effectiveness of Qualcomm’s mobile broadband cellular base stations (BS) against JSOCs mission requirements.

Qualcomm assembled these BSs based on the traditional cellular architecture; however, they compressed the networks into two man-portable containers (Radio Node (RN) and Radio Network Controller (RNC)) by collocating multiple services. The first container (RN) is essentially the mobile cell tower, and the second container (RNC) is the switch component. Figure 10 is an illustration of the BS. Qualcomm advertises a 3.1 Mbps uplink and 1.8 Mbps downlink capacity. Each RN supports 120 channels, and each RNC supports 12 RNs and 2,500 users (Qualcomm, 2005). The device is a CDMA broadband data communication system.

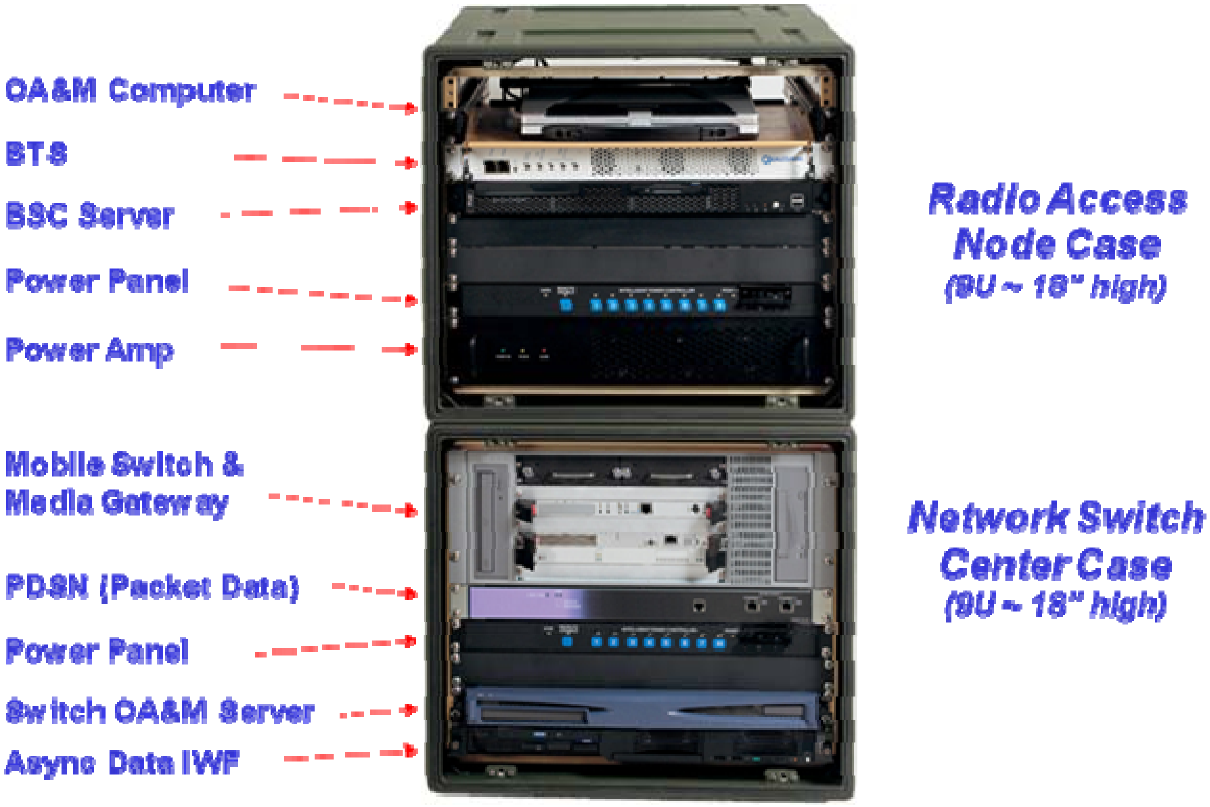


Figure 10. Qualcomm Cellular Base Station
(Qualcomm, 2005)

The results of their tests were successful overall. However, looking at it from a different perspective (i.e., as not being driven by specific unit requirements), is this system effective across service requirements for a general communication system? For foot-mobile units, this suite of communication equipment is impractical for mobility. However, for vehicle or air-mobile platforms, this form factor proved to suit the requirement. When JSIC tested the device for distance, the results for a vehicle-mounted system provided signal coverage for a follow-on vehicle up to two miles in trail. From an antenna mounted on a fixed building, they observed signal coverage of 7-10 miles, depending on the height of the antenna (JSOC, 2009). From a C-130 at 20,000 feet, signal coverage on the ground reached a radius of 60 nautical miles (JSIC, 2009). Based on the distance results, the mobile ground platforms are not very efficient or scalable—given the extreme cost per unit. However, these systems seem extremely plausible for a Forward Operating Base (FOB) or for airborne platform implementation. Most of our FOBs could be completely supported given their small sizes. Forward-deployed airbases usually have constant aerial tanker support. Therefore, if fitted with these BSs, the tankers could supplement the ground BS and extend the cellular coverage far beyond the base perimeter.

A product similar to the above BS and which falls within the same category is Ericsson's 3G QuicLINKs (Figure 11). This device is capable of providing the same functionality as the Qualcomm variant, with minor differences.

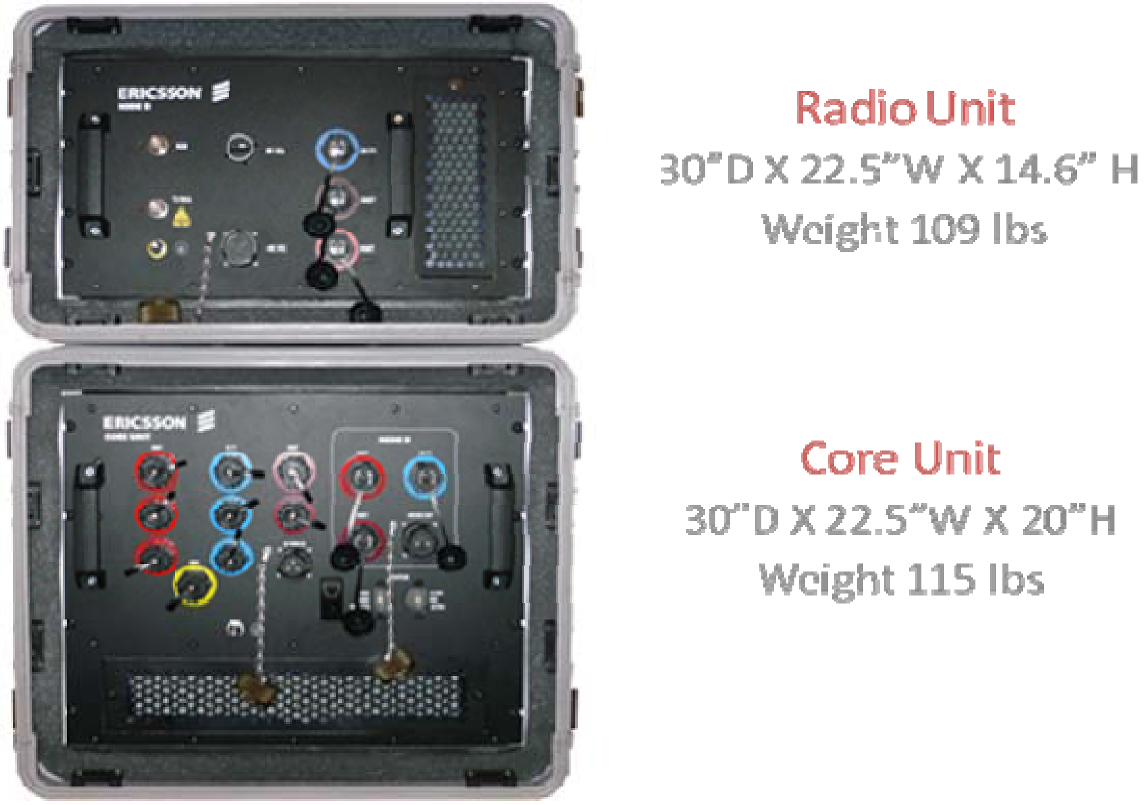


Figure 11. Ericsson QuicLINK (Mobile Base Station)
(Ericsson, 2009)

Another product developed as a solution to hosting tactical cellular networks is LGS Innovations' 2.5G TacBSR, pico and marco versions (Figure 12 and Figure 13). These devices were designed as pico and macro cells—therefore significantly less expensive than Qualcomm and Ericsson products. The price difference is partially because of the number of supported channels available (i.e., eight channels with six available for data or voice allocations) and partially, because the developers didn't include the functionality of a mobile switching center which could inhibit scalability. However, it is interoperable with a Voice-over-Internet-Protocol (VoIP) infrastructure (LGS Innovations, 2007); therefore, the potential does exist for large-scale networks. These devices differ from the above CDMA solutions because they operate on the GSM protocol.

Figure 12. TacBSR Pico (LGS Innovations, 2007)

Figure 13. TacBSR Macro (LGS Innovations, 2007)

Alternatively, the same vendor advertises a 4G mobile base station solution called the Rapidly Deployable Network (RDN) (Figure 14). This solution provides a mobile cellular base station to host 4G networks and supports a WiFi meshing capability (Kuhn, , 2009).

Figure 14. Rapidly Deployable Network (RDN)
(LGS Innovations, n.d.)

The US Army Research Development and Engineering Command (RDECOM), Communications-Electronics Research, Development and Engineering Center’s (CERDEC), Joint Cell Phone Project has manipulated a Base Transceiver Station and Mobile Switching Center (MSC) (Figure 15) to operate on the DoD’s UHF band (1755 – 1835 MHz). The biggest advantage to this technology is its ability to operate in the DoD-owned spectrum (Army CERDEC, 2009). This eliminates the need for leasing the spectrum of other service providers when the Marine Corps conducts training exercises in the continental United States (CONUS).

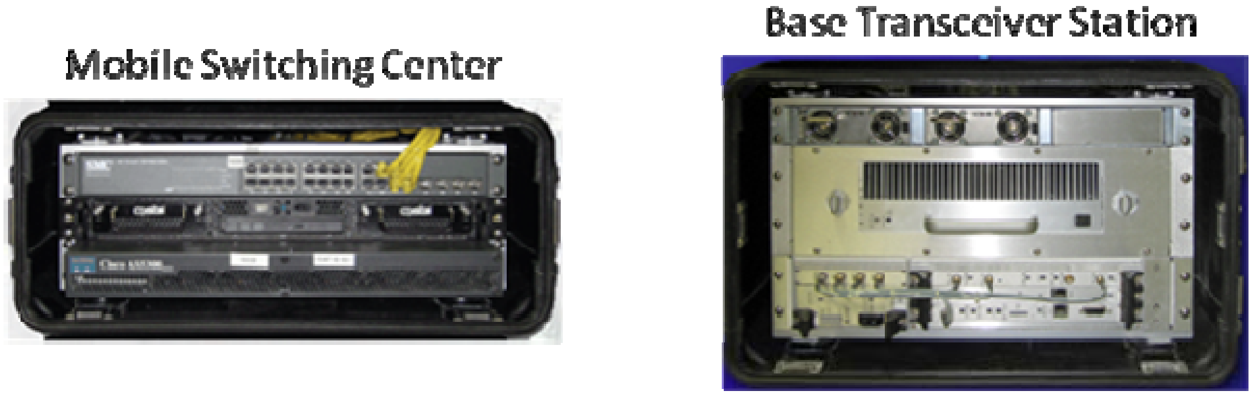


Figure 15. Equipment for CERDEC’s Joint Cell Phone Project
(Army CERDEC, 2009)

2. Open-Source Software Version Base Station

As an alternative to the proprietary solutions discussed above, the OpenBTS project attempts to provide a GSM-variant, open-source base-station software for a fraction of the cost. The goal of the project is to provide a cellular network that is capable of being installed and operated for a faction of the cost of traditional cellular technologies (Burgess, 2009). OpenBTS is a Unix application that leverages the Universal Software Radio Peripheral (USRP) (software-defined radio) as the GSM air interface and the Asterisk PBX software as the interconnecting call manager. This type of open-source (10,000 lines of code) technology is extremely desirable for the more widely distributed implementations. The applications connect GSM handsets to either other handsets or VoIP clients, without the need for the traditional BSC, MSC, or Home Location Register (HLR). However, since the leveraged air interface is GSM, the vulnerabilities common to traditional technology still exist.

3. MIL-SPEC Communication Devices

The program currently charged with leading the military in communications is The Joint Program Executive Office (JPEO), Joint Tactical Radio Systems (JTRSs). Over the years they have refined and developed a SCA and Application Programming Interfaces (APIs) standards for facilitating interoperability between communication assets (JPEO JTRS, 2005). These concepts are essential in order to bring new innovative technology to our troops. Additionally, their intent is to maintain Government Purpose Rights (GPR) on all designed software and leverage the Software Defined Radio (SDR) characteristic for future radios. One of their waveforms relevant to this research is the Mobile User Objective System (MUOS) Common Air Interface (CAI), which provides military satellite communications (MILSATCOM). The waveform was designed from the Wideband Code Division Multiple Access (WCDMA) protocol (Department of the Navy Research, Development & Acquisition, n.d.). The relevance is not only the leveraged cellular waveform, but also the fact that any tactical radio capable of hosting this capability must contain two transceivers for the full-duplex waveform. This functionality minimizes the hardware changes needed to support cellular waveforms internal to military tactical radios.

4. Peer-to-Peer

The ultimate advantage to military tactical communications (comms) is the ability to establish secure voice and data connectivity between any two handheld nodes. Modern day military tactical comms allow multiple handhelds to peer together on the same network without requiring tree architectures. Traditionally, this capability has not existed in the commercial cellular industry. However, today a few commercial vendors are advertising this type of technology within a cellular handset. For example, a Swedish company, TerraNet, claims to have developed and conducted a demo (i.e., as of July 2009) of their patented technology. However, as of the last six months it seems the company has not made any additional news statements (TerraNet, 2010). The main point, however, is that the meshing technology (peer-to-peer) within the cellular world is extremely valuable for military applications.

III. Concept

As highlighted in Chapter II, current communication assets of company level Marine units are extremely limited in providing on-the-move data capabilities, in contrast to smart phones that are specifically designed for transmitting and receiving data in high-mobility environments. However, the standard commercial smart phone was not designed to military specifications or requirements. In an attempt to leverage the benefits of smart phones and methodically integrate the technologies, while also ensuring a level of security suitable for military applications, this chapter comprehensively evaluates each feasible integration approach. This chapter is organized along two abstract approaches: wired and wireless. The wired approach is referred to as the tethered concept in this thesis. The wireless approach is broken into two subsections: indirect bridging, and direct interfacing (i.e., the handset and tactical radio connecting via a common wireless signal). Each of these concepts has valuable and unique advantages along with some disadvantages.

To motivate the different approaches, the chapter first discusses the advantages and disadvantages of, (i) centralized versus decentralized architectures and (ii) not integrating the technology and instead supplementing the preexisting infrastructure. The author discusses these concepts first to highlight the dichotomy that surrounds the concepts.

A. Centralized versus Decentralized

As mentioned in Chapter II, the traditional cellular architecture is designed to maximize user capacity while minimizing cost. Instead of all cellular services being available at the cell towers, the providers condense the redundant equipment in close proximity to one node (e.g., a base station controller, radio network controller, mobile switching center, etc.). This enables one node to control many nodes (i.e., base transceiver stations), which facilitates simple operational management and reduces overall labor/equipment cost. This tree architecture is extremely cost-efficient for the commercial sector because one command center can control the entire network, essentially permitting a scalable network, while maximizing return. However, the entire system is dependent on reliable connections because services cannot be delivered if they don't reach the server. In military wireless-communication architectures, this might not be feasible due to our highly mobile ad-hoc networks (MANETs). Marine Corps nodes are primarily connected via an intermittent wireless connection, as opposed to the commercial sector's reliable Gigabit links. This centralized approach could cause serious consequences if the backhaul links were down for any extended period of time. Therefore, for military MANET applications, a decentralized approach with critical services local to the immediate access points is crucial. Infantry units need the ability to internally conduct operations or exercises without higher or adjacent dependencies. In an effort to maintain cost efficiency and reduce the footprint of communication equipment, a limit needs to be placed on the capability that one node can provide. As listed in Chapter II, many commercial all-in-one solutions exist, with one node providing thousands of channels (i.e., many cell-phone connections per access point). These high capacity solutions incur a cost of size and weight. Such concerns can be mitigated by limiting the capabilities to those attainable via software upgrades only (e.g., a 10-channel capacity per node).

B. Without Integration, Completely Commercial

Before discussing the various concepts of integrating the technologies, the thesis addresses the idea of completely leveraging the commercial infrastructure. Most countries have a preexisting cellular infrastructure. During occupation missions, instead of completely destroying the communication network, perhaps the invading military could seize the existing network. This would facilitate uninterrupted communications, while enabling the invaders to monitor all traffic as needed, which could be considered advantageous. In the event the country does not possess massive infrastructure, the existing network would be used as a beginning and therefore cost less money than completely building a new network from scratch. Today's revolutionary technology provides wireless throughput ranges well beyond the data rates of our tactical radios. Therefore, the concept of hosting local 4G cellular networks without the need for a military network seems extremely valuable. However, even with these highly capable networks, the well-known vulnerabilities are still present regardless of who controls the network. Since these assets would be considered a public good and highly used by the adversaries the potential for public destruction or sabotage seems unlikely. Additionally, if the sole source for communication is the cellular network, it seems unlikely the community would destroy this resource. In fact, it seems useless for adversaries to monitor and detect locations, because the demographics of the users would likely be significantly diverse between locals and non-locals—the outsiders would blend in with the populous; as opposed to a military network in which the users are strictly service members and it is therefore easier to detect non-military devices or people. As an additional precaution, security protocols can be added above the physical layer—no organization would want an unauthorized intruder to listen in on conversations or pretend to be an authorized user. Most of today’s cellular phones are capable of adding encryption software without adding significant cost. There are three problems with this approach, (i) the occupying terrain must be conducive for easy and efficient cellular infrastructure development (i.e., not an austere environment), (ii) the amount of time required to develop a feasible infrastructure might be unacceptable for expeditious operations, and (iii) the resources procured and installed most likely would remain behind once the mission completed.

C. Wired

1. Tethered Concept

This idea is similar to the D-DACT system. The D-DACT can operate independent of any other device. However, to send or receive data, the device needs to tether via a data cable to a SINCGARS radio (Operator's and Organizational Maintenance Manual—Dismounted Data Automated Communications Terminal, 2006). The tethering concept is valuable because the emission security concerns are no longer a factor. If the handheld device only transmits data via a tethered cable, then the wireless interfaces could be disabled to prevent unnecessary emissions. If the mission's main priority is intelligence gathering with an environment conducive to limited mobility, then the concept seems feasible. A method to reduce the cost from the highly expensive D-DACT would be to leverage COTS equipment that is suitable for austere military environments with modern data capabilities. In review of three commercial cellular handsets, HTC's Dream with Android OS, Apple's iPhone, and RIM's Blackberry, the hardware does contain characteristics (Universal Serial Bus (USB) On The Go (OTG)), which enables the handset to function as a tethered device with minor driver modifications (Google Inc., 2009; Apple Inc., 2009). However, the tethering concept limits mobility and reduces flexibility by requiring a wired connection between the data-collection device and the data-disseminating device. As an immediate solution, this might be the best option until the military makes a decision about the amount of risk it is willing to take in order to leverage the cellular technology.

D. Indirect Bridging

This concept brings in additional hardware; however, it eliminates the tethered cable or the sophisticated software-equivalent mobile base stations. Essentially, every IP-capable tactical radio could act as a gateway for a mobile base station (our discussion of mobile base stations is in Chapter II). The mobile base stations would host the local cellular networks and leverage the interconnecting tactical radios for backhaul communications. Depending on the flexibility and complexity of the mobile base station and the connecting tactical radio, minimal—if any—software adjustments would be required. Because each tactical radio and mobile base station provides different throughput characteristics, the communications architectures would need to account for these disparities. Therefore, a mobile base station with more than 2,000 channels should be used for FOB deployments. The limited 8-channel plus devices are more appropriate within company-level communication architectures. The biggest concern of this configuration is the security limitations of mobile base stations (i.e., the emissions and Medium Access Control (MAC) layer vulnerabilities). This concept is suitable for missions without the LPI/LPD requirements. Since the majority of today's cellular handsets are capable of encrypting data (through software) up to a secret level[6], this concept seems feasible for those environments. It is not feasible for the environments with conditions that require strict emissions control or security. Even though some of the commercial protocols unintentionally provide limited emission security by implementing spread spectrum functionality and power control, these devices would still require significant modifications to create an LPD/LPI signal.

E. Direct Interfacing

This concept suggests separating the air interface resident onboard the handsets from the remaining cellular protocols. Because ultimately the objective is to adopt an LPD and LPI signal while maintaining the cost-efficient and highly innovative characteristics within the cellular handsets, this concept stresses two areas: hardware modularity and software portability to support device interoperability. The modifications to the cellular handset are only required in environments that requires that level of confidence. To directly connect a cellular handset via a wireless interface to the current military tactical radios we suggest three approaches: (i) add a MIL-SPEC signal to the cellular handset, (ii) modify the tactical radio to include a COTS cellular protocol, or (iii) modify a COTS cellular protocol to operate on both the military radio and commercial handset.

1. MIL-SPEC Signal

The first method under the direct concept consists of adjusting the cell-phone firmware and hardware, while leaving the tactical radio unchanged. To fully integrate the cell phone without adjusting the tactical radio, three changes are needed to the handset: (i) a firmware upgrade to add military waveforms for interoperability, (ii) a

[6] Although only limited handsets are approved for transferring classified information, the majority of cell phones contain characteristics required to run the encryption algorithms categorized by NSA as Suite B (NSA, 2009; Cellcrypt, 2009).

hardware modification since the military waveforms operate on the lower band frequencies (e.g., the radio frequency (RF) front end hardware would need to be replaced with a lower band transceiver), and (iii) a hardware addition to include the crypto fill and Type 1 security capability. However, for the tactical radios with inherent wideband frequency ranges and Suite B encryption algorithms, the second and third concerns might be negligible. The first problem with this direct concept is cost. The main reason for leveraging the cellular technology is the low-priced, highly capable handsets. If these changes were implemented on a cell phone, then the results would be similar to the previously mentioned D-DACT. The D-DACT was built based on the technology of the Personal Digital Assistant (PDA); however, as the military requirements increased, the price per unit increased. According to the CNET Reviews website, the top five commercial PDAs range from $429 to $599 (Cha, 2009); however, a single D-DACT costs about $10,000, or $15,000 with accessories (Stanley Associates, 2009). This direct method becomes impracticable if it requires major hardware changes, but it might be feasible if made through software updates.

2. Commercial Off-the-Shelf (COTS) Cellular Onboard Military Radios

The second method consists of adjusting the firmware or hardware on the military tactical radios. This method does not necessitate any changes to cell phones. Therefore, the tactical radios would require an additional chipset to include the desired cellular protocol. Instead of adding hardware, one alternative would be to modify the firmware to include the desired cellular protocols, ranging from the physical and link layer associations to the application-layer services. These modifications would create a method for military troops to leverage cellular technology without bringing additional equipment, other than the handsets, to the battlefield. Since the vulnerabilities in the commercial cellular technology would now be present in military tactical radios, either additional modifications (i.e., emission controls, data encryption, etc.) are required or a specific understanding of the associated risk would be required when operating in those modes. At the application layer, there exist applications to partially mitigate security vulnerability by encrypting the data. A known solution for a secure (content protection) phone is General Dynamics' Sectera Edge, a Secure Mobile Environment Portable Electronic Device (SME PED). However, this device operates on the traditional cellular waveforms, which are not completely LPD, LPI, LPE, and anti-jam signals. Therefore, this device is still vulnerable to the associated attacks. However, perhaps in some situations this would not be a factor.

3. Modified Wireless Interface

As mentioned above, a completely OTS cellular protocol is not desirable in environments requiring high levels of emission control. However, to mitigate high cost and leverage the capabilities within a cellular handset the following concepts modify various components of the cellular protocols to integrate the technologies.

a. Modify Uplink/Downlink Signal

The motivation for modifying the cellular device's physical signals is the emission security vulnerabilities. This concept involves modifying a GSM, CDMA, WiMAX, or LTE signal to create an LPI/LPD variant. This will require chipset and protocol stack modifications. The cellular protocols were chosen vice a military waveform, because the cellular handsets already have the radio frequency (RF) front-end to support the ranges. For example, the above mentioned commercial protocols use transceivers, which operate in the frequency bands of 850/900/1800/1900 MHz and above. Any changes to the hardware (i.e., RF front-end) would require large manufacturing volumes to offset the high production costs.

b. Decouple the Signal from Remaining Protocol

The purpose of modifying the cellular protocols includes increasing flexibility and eliminating dependency on the centralized architecture. Therefore, this concept consists of eliminating the required cellular switching and control methods for the traditional cellular protocols. For example, in GSM, each BTS is dependent on a BSC, MSC, and HLR to complete the GSM network. This concept would leverage the BTS functionality by using the above-mentioned modified cellular signal to connect the handsets, but it would replace the remaining switching functionality with a VoIP infrastructure. This concept is similar to the OpenBTS project mentioned in the previous chapter and future 4G technology. However, this concept can apply to any cellular protocol. The idea is to decouple the wireless interface from the remainder of the networking protocol, which would facilitate future enhancements to wireless interfaces by creating a modular system. Therefore, when new technology arises a fully redesigned handset is not required—the wireless interface could simply be swapped out for an upgrade. If the commercial industry discovers a new method at the air interface level (physical layer) to significantly increase data rates, the technology could easily be adopted without significant modification to the overall protocol.

c. Adding MIL-SPEC Content Protection Measures

As mentioned in Chapter II, the traditional commercial cellular infrastructure is more susceptible to security threats than are military tactical networks. The content protection threats can be mitigated by including end-to-end and link-encryption protocols. Virtually all newer cell phones are equipped with the hardware requirements for this type of capability. The market for this capability exists because of the threat of compromises to the industry's intellectual property. Most businesses require some level of protection, which can be accomplished on a cellular handset at the applications layer with a combination of cryptography and hashing algorithms: Advanced Encryption Standard (AES), Elliptic curve Diffie-Hellman (ECDH), and the Secure Hash Algorithm (SHA) (Cellcrypt, 2009). As highlighted in the Suite B specification, this combination can provide security for information up to the secret level (NSA, 2009). Alternatively, the process of encrypting the data could occur at a lower level.

d. Tactical Radio Modifications

Traditional military radios only operate one waveform at a time, as opposed to modern cellular handsets that operate multiple interfaces simultaneously (i.e., a Personal Area Network (PAN), a Local Area Network (LAN), and Wide Area Network (WAN)). By design, the military's traditional wireless communication devices are half-duplex, single-channel radios with only one transceiver. This limitation can cause problems when integrating a technology (cellular handsets) designed to operate multiple interfaces simultaneously. Therefore, this concept suggests two modifications: (i) modify the tactical radio's hardware and firmware by adding additional transceivers to allow full duplex cellular protocols or (ii) modify the cellular protocol to account for the single transceiver, and daisy chain an additional radio to support the additional transceiver for the backhaul link. An advantage to adding additional transceivers is that doing so reduces the hardware footprint by eliminating the need for extra radios. However, it takes time and money to produce a completely new model of radios. An advantage to modifying the cellular protocol is that doing so eliminates the need for re-manufacturing, re-certifying, and re-approving the new model. However, the modifications to the cellular protocol could introduce complex and sophisticated changes, rendering the method infeasible. As previously mentioned, any MUOS capable radio would provide the perfect radio host for supporting a modern commercial cellular signal. As suggested by their CDMA characteristics, these radios provide support for multiple transceivers in the frequency range needed for commercial cellular interoperability.

e. Spectrum Modification

A recurring issue that exists in both the military and commercial worlds is limited-spectrum resources. The DoD owns a wide range of frequencies in the lower bands. However, the cellular bands are mostly allocated to commercial service providers, which become a problem when the DoD wishes to use one of these high frequency bands. The options are to either purchase a lease from a provider or leverage the DoD-allocated spectrum. The problem with leveraging the DoD spectrum is that commercial cellular handsets are not configured for these ranges. Therefore, modifications to the handset would be required, to leverage additional spectrum outside of normal cellular service provider's allocations. Additionally, these modifications would support frequency flexibility for operating outside US boarders in uncertain environments.

F. Peer to Peer (P2P)

A true P2P architecture is desirable if cellular handset technology is going to reach its full potential as a supplement military communications. Currently, the most valuable characteristic in military communications is the P2P architecture. The minimum equipment required for a two-person conversation is two military radios. This is a true distributed architecture for which no access point is required. However, not all military waveforms (wireless protocols) or commercial cellular handsets operate this way. For this distributed architecture, each cell phone would essentially act as a sender, receiver, and relay node (i.e., the cell phone acts as the access point).

IV. Experiments

A. USRP/OPENBTS

To begin understanding the difficulty of the integration problem a simple exploration study was completed. The goal of the research was to evaluate the complexity of building a complete software version, including the functionality of a BTS, but not requiring the traditional BSC, MSC, PTSN, and other inherent services of the traditional cellular infrastructure. The setup involved installing a Linux OS (Ubuntu 9.04), Asterisk (Private Branch Exchange (PBX)), OpenBTS (open source GSM base station software), GNURadio (signal processing package) and a VoIP client on a standard Dell OmniPlex 620 desktop.

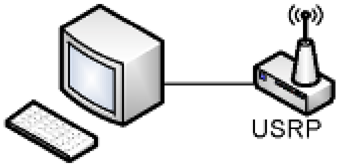


Figure 16. OpenBTS Hardware Architecture[7]

The hardware used to transmit and receive the cellular signals was the Universal Software Radio Peripheral (USRP). This device was equipped with two RFX900 daughter boards as transceivers. The assembly of hardware and software installation took a few weeks due to the author’s limited knowledge of the technology. However, after configuring the various software packages and provisioning the first phone it became very easy to manipulate. Even though the software is based on older technology (i.e., 2.5 Generation), the experiment proved the potential of an integrated solution with a limited capacity. For a significant proportion of the world, 2.5G is still a popular technology for cellular communications

[7] Figure 16 was designed by the author.

(Ergen, 2009). For a military application, the combined software/hardware suite could be used if the limitations inherent to the GSM technology were mitigated through additional coding. The standard computer can be replaced with any software-defined radio capable of running the listed or compatible software on board the device. Due to the limitations of the USRP, the SDR is not capable of running on board software. However, the more sophisticated equipment (i.e., Field Programmable Gate Arrays (FPGAs), with Digital Signal Processors (DSPs), and an internal microprocessor) similar to the current military radios might be capable of running these on board services in a limited capacity. The concept surrounding the software proved to be extremely valuable since (i) it is open source code which can be manipulated to military specifications, (ii) it eliminates traditional tree like network infrastructures and thus provides flexibility for ad hoc networks, and (iii) an IP based backbone increases the interoperability with other systems (i.e., VoIP, ubiquitous computing, etc.). However, given this capability, are military tactical radios even capable of transmitting this type of traffic at the desired speed of common modern day smart phones? What level of capacity do military radios provide? To explore such questions another study was conducted.

B. Tactical Network Topology (TNT) Capabilities Based Experimentation (CBE) 10-1 participation (w/ LGS TACBSR)

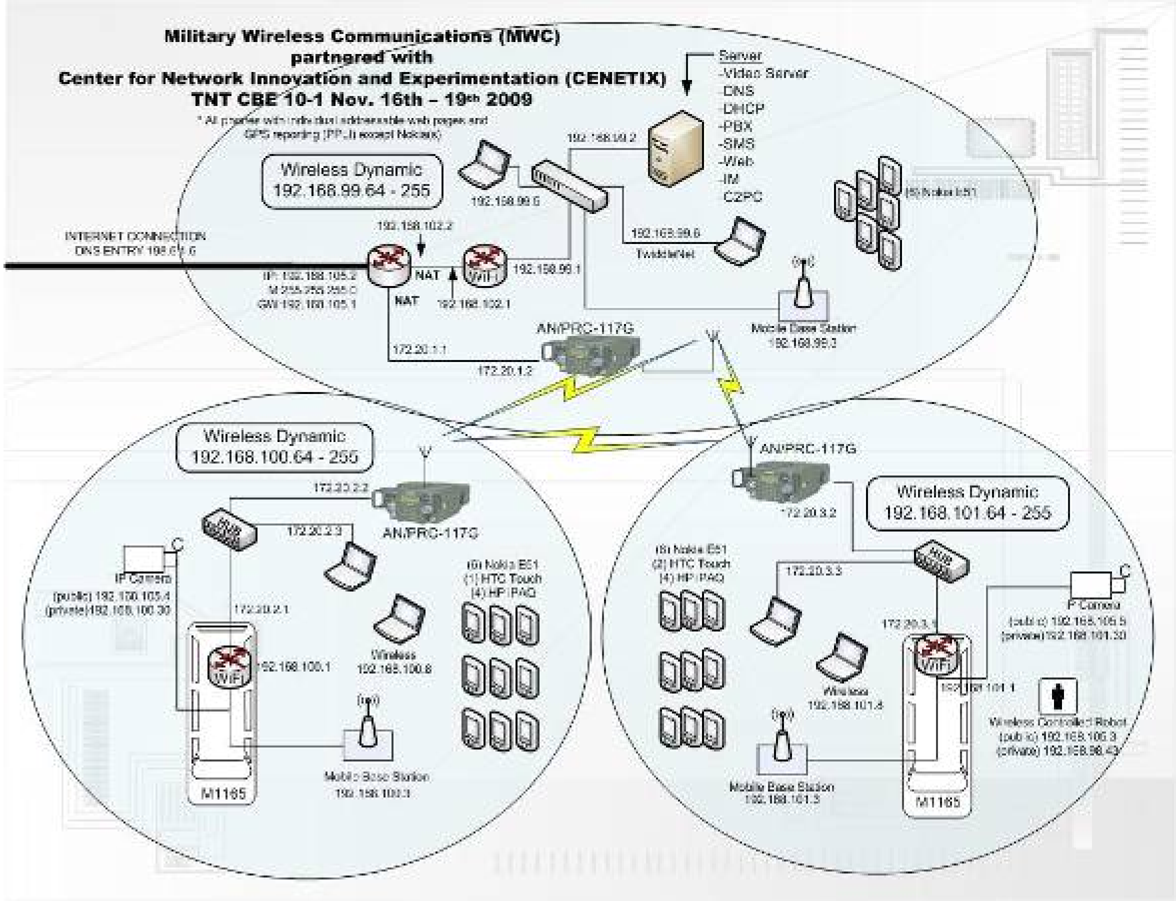


Figure 17. TNT CBE 10-1 Architecture[8]

This exploration was designed to evaluate the feasibility of integrating cellular handsets with military wireless communications. The hardware leveraged for this experiment was three Lucent and Alcatel Government Solutions (LGS) Innovations Tactical Base Stations, three Harris RF Communications AN/PRC-117G, and three Cisco Ruggedized WiFi routers. Again, this experiment was not designed for an end solution, but as a proof of concept beyond the OpenBTS exploration. The exercise

[8] Figure 17 was designed by the author.

leveraged a contrived design (Figure 17) created to explore the capabilities inherent in the tactical radios (AN/PRC-117G).

As mentioned in Chapter II, the PRC-117Gs are single channel half-duplex radios. The experiment interconnected three cellular edge networks (LGS Innovations, TacBSRs) via our tactical radios (AN/PRC-117G with 50W amplifiers mounted within the vehicles). Each cellular network provided six available channels to configure as data or voice. After four days of setting up, configuring, reconfiguring, and testing various scenarios, the author bridged multiple single channel tactical radios by three full-duplex base stations (TacBSRs) each containing six simultaneous voice / data channels. Essentially, three spatially separated GSM networks were interconnected via the tactical radios. Voice conferencing was established to test multiple cellular handset connections, and live video streams were established to pass video from one network to another. The video capturing devices ranged from HMMWV mounted IP cameras to mobile wireless cellular handsets. At first, live video was successfully routed via the 2.5G cellular mobile base stations (i.e., from a cellular handset in one network to another cellular handset in a different network). However, given the limited throughput, a WiFi access point was leveraged to evaluate the capacity of the tactical radios. As expected, the throughput was drastically increased by using the WiFi access point. After a few throughput tests the interconnecting tactical radios demonstrated a capacity above the commercial 2.5G cellular limitations. This evaluation identified future potential for easily connecting cellular base stations at a fraction of the cost—about $26,000 per device. However, the throughput limitation identified additional concerns about providing a technology (i.e., 2.5G), that is already out of date by more than a decade.

C. TNT CBE 10-2 Participation (W/ Ericsson QuicLINKS)

During the TNT 10-1 explorations, the author conducted most tests in an effort to evaluate various commercial equipment and determine feasibility assessments for integration. As a result of some equipment failures and configuration errors the study ended without an in depth exploration of the technology. This new round of testing conducted during the TNT 10-2 event was intended to extend the prior studies and answer the previously developed questions. The main objective was to quantify throughput variations and emission significance.

Between February 21–26, a group consisting of a Naval Postgraduate School (NPS) student and researcher (John H. Gibson), Ericsson Federal Engineers, and a Harris RF Communications Engineer deployed to Camp Roberts, CA, to further evaluate commercial cellular integration with military wireless communications.

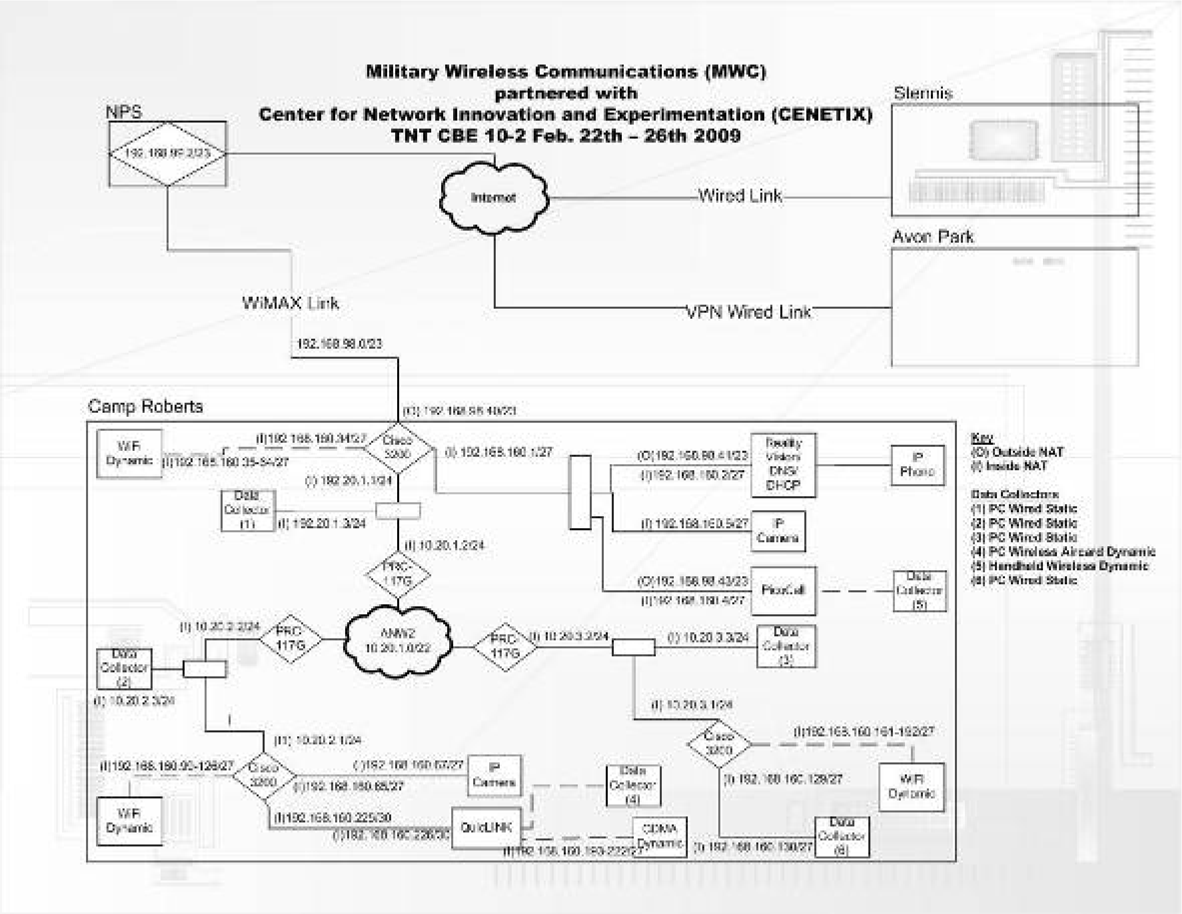


Figure 18. TNT CBE 10-2 Architecture[9]

[9] Figure 18 was designed by the author.

Figure 18 details the complexity of the topology leveraged for the duration of the week. Although not specifically mentioned in the experiment, a VoIP network was established with a PBX server to create an interoperable voice network with the varying cellular technologies. This capability proves valuable when connecting the various voice communications. However, this capability only provides voice connectivity. The purpose of the topology complexity was to evaluate what the maximum potential for the direct concept (i.e., the idea of hosting mobile base stations aboard FOB installations and leveraging smaller variations for convoy or foot mobile support).

1. Throughput Testing

When developing a solution for using cell phones at the edge of a network the remaining architecture is extremely important in regards to supplying a reliable transport infrastructure. Therefore, the following throughput testing was conducted to evaluate military radio data capacity. The author organized the throughput test results in increasing order starting with the simplest topology, two radios wirelessly connected, in an effort to eliminate uncontrolled variables as the complexity of the experiment increased. For each test, two protocols are presented to illustrate the consistency of the results regardless of the leveraged transport layer. This will help highlight the significance of the test results and eliminate any doubt of unconsidered variables.

The Harris RF Communications' AN/PRC-117G tactical radio was leveraged primarily, because the previous model is an existing platform used in military operations and this is the expected replacement model. Additionally, its achievable data throughput rates are advertised as and seem representative of leading the market in capacity. For the throughput testing the following equipment was used: Ericsson QuicLINKs Moible Base Station with WCDMA, Harris AN/PRC-117G Tactical Radio with ANW2, HP Netbook and Panasonic Toughbook clients, Cisco Ruggedized 3200 Series Routers with 10/100 Router, Switch, and 802.11b/g interfaces, and Harris RF-3184-AT320 225-450 MHz and RF-3186-AT320 500-2000

MHz) UHF antennas. The software used for measurements and data collection were as follows: BMExtreme (for real-time throughput monitoring through Simple Network Management Protocol (SNMP)), iperf/jperf (for traffic injection and end-to-end statistics), and Wireshark (for packet captures). All statistics were correlated and verified with the output results received from iperf and Wireshark captures.

a. Test 1

The purpose of the first test was to set a base line for observed throughput with only two tactical radios directly attached. Figure 19 illustrates the topology used to measure the capacity of the tactical radios. Both radios were configured to operate with a 2-node max configuration, a frequency center of 305 MHz, the Advance Networking Wideband Waveform (ANW2), 50 Watt amplifiers, 4 kilometer Line-of-sight (LOS) of separation across the wireless link, and UHF vehicular dipole antennas (rated for 225 to 450 MHz).

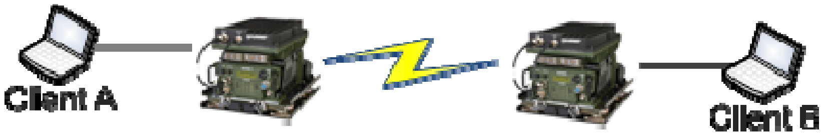


Figure 19. Throughput Test 1 Topology[10]
(Harris Corporation, 2009)

For this configuration, two protocols (Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)) were tested to evaluate the maximum throughput capacity respectively. For TCP, traffic was injected by iperf software with one computer configured to initiate the client for pulling and pushing continual 1470 byte sized packets, across 28 flows (14 uploading and 14 downloading), with TCP window size of 8 Kbytes, and for duration of 300 seconds (5 minutes). As, displayed on the graph in Figure 20, the remaining 150 seconds did not finish due to a radio

[10] Harris radio picture taken from reference, however the overall figure was created by author.

problem. This issue is a known problem with the leveraged firmware version and according to a Harris representative is fixed in the current release.

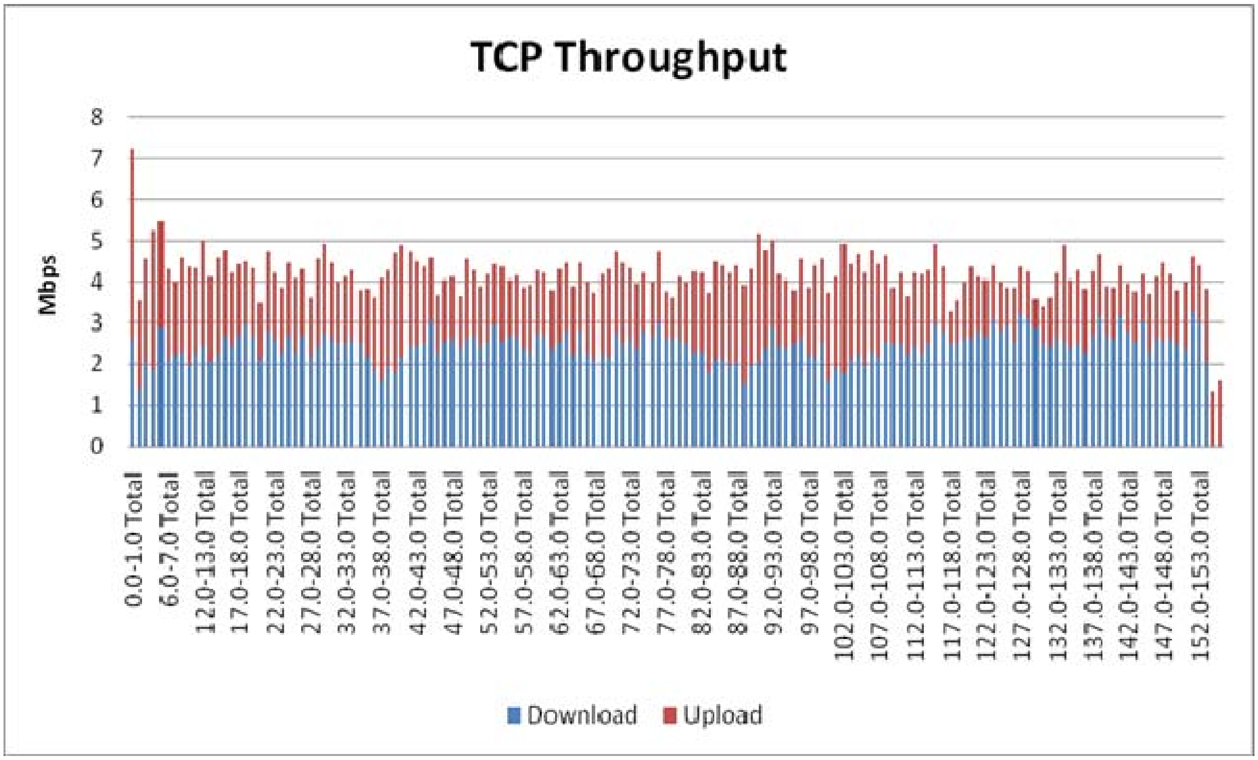


Figure 20. PRC-117G TCP Throughput (Test 1)

Even though the test failed to complete, Figure 20 illustrates the results received from the iperf output. Additionally, to prevent faulty data from a single data collection source, the results were verified during the test from near-real-time SNMP returns and after the test through correlated Wireshark captures. These results indicate that the radios are capable of supporting traffic rates around 3.5 Mbps—however, without further testing the patched firmware these results are inconclusive. The blue section represents the traffic rate of the downloading flows from the server to the client and the red represents the traffic rate of the uploading flows in reverse. This data is not indicative of a sustained or average rate. It only points out the fact that the radios did reach this rate before a crash occurred.

Given the results from Figure 20, our group ran a UDP test with a client sending 1 flow along with the server sending 2 flows at a rate of 1 Mbps per flow. The UDP test used the same topology as the TCP test. However, the first test failed at 40 seconds and the next at 100 seconds. Each time the number of concurrent flows was reduced. The crashes this time were different than those in the TCP test. This time the radio network recovered directly and automatically after the traffic was removed. The network seemed to crash after the average round trip times (RTTs) reached on average above 1 second. The only logical conclusion is that the radio's buffer is filling up and limiting the ability to forward incoming packets. After reducing the configuration to one client and one server continually pushing 1470-byte datagrams with a total of 3 flows (1 uploading and 2 downloading), leveraging a UDP buffer size of 8 Kbytes, the test lasted a total duration of 540 seconds (9 Minutes) until it successfully terminated without crashing. Figure 21 illustrates the results from the test. The flows are displayed separately to show the symmetry between each flow.

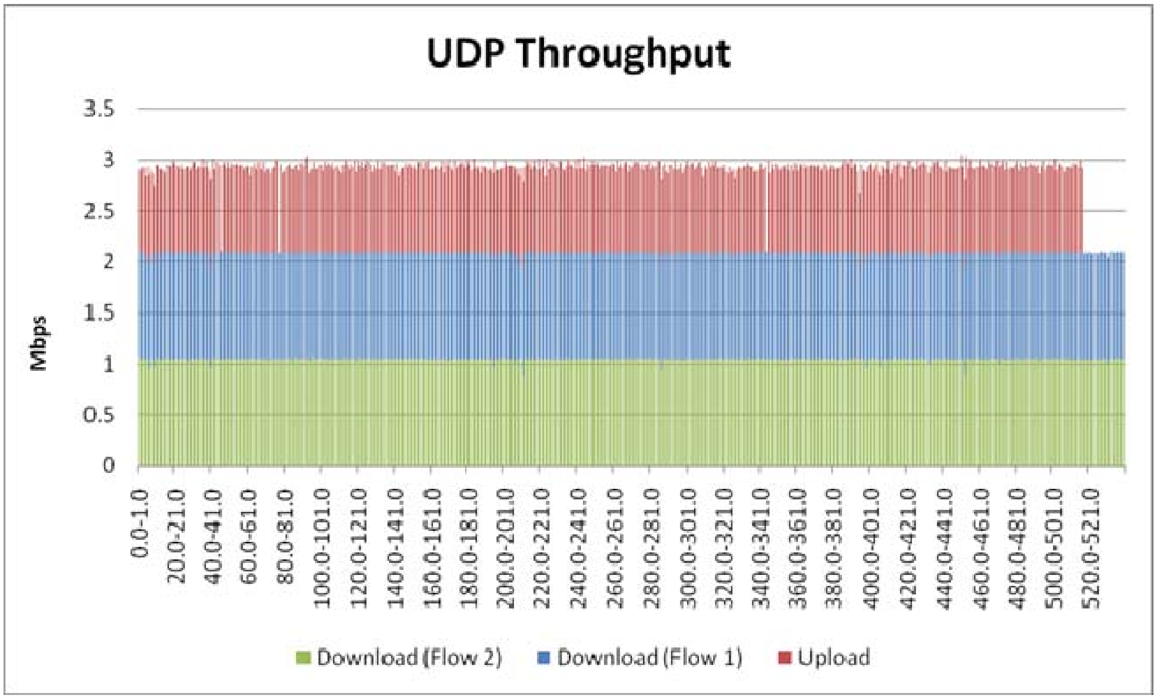


Figure 21. PRC-117G UDP Throughput (Test 1)

Figure 21 provides evidence for a 9 minute UDP sustained throughput rate of just below 3 Mbps. Given the test thus far, it seems the radios, as advertised, are bandwidth restricted to sustainable rates under 3 Mbps. Figure 21 differs slightly from Figure 20 in that the plots are illustrated per second vice per every ten seconds. Every second was plotted in an effort to show the steady flow for the UDP traffic. These results are a significant improvement for traditionally tactical radios. Normally the data rates for older models are in the low kilobits. The results suggest our modern day military tactical radios are capable of supporting megabits per second of data across military company/platoon-sizes radios.

b. Test 2

The second test added additional layer 3 devices to the topology. The purpose of this test was to identify if adding routers outside of the core radio network would cause significant delays. For this test, two clients each directly attached via Ethernet cable to a Cisco 3200 Ruggedized router, and they were interconnected by the previously configured 117G Radios with the same 2-node max configurations as test 1. As in the earlier test, the radios were operating at the 305 MHz frequency, with ANW2, Waveform Identification (WID) 7, 50W amplifiers, 4 km LOS separation, and UHF vehicular dipole antennas (225 to 450 MHz).

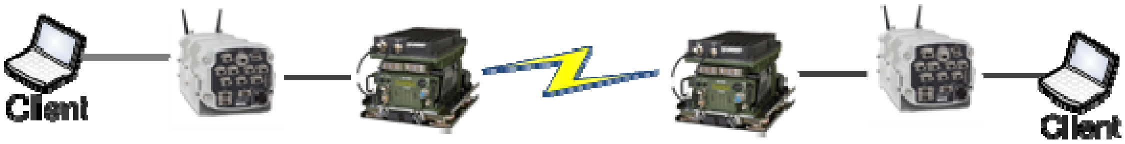


Figure 22. Throughput Test 2 Topology[11]
(Cisco, n.d.; Harris Corporation, 2009)

[11] Harris radio and Cisco router picture taken from reference, however the author created the overall figure.

For this test, the same software and methods from the previous test were used. The first test consisted of exchanging continual 1470 byte sized packets, a TCP window size of 8 Kbytes, 10 bidirectional flows (5 upload and 5 download), and a duration of 300 seconds (5 minutes). We ran this test a few times, including a run with more flows, each time resulting in the observance of significant round trip time delays followed by network connectivity loss. In some instances the packet captures presented results suggesting an intermediate node was sending TCP FIN (i.e., TCP finished with protocol and now gracefully shutdown flow) packets before the application (iperf) was successfully complete. For example, this could be the case if the buffers of the radios were overflowed.   A common fix to this problem could be cutting off the tail of the buffer. However, if the device was too overwhelmed, the tail cutting method might keep dropping the newest packets, thus never servicing new packets. Therefore, this test was limited to the 10 flows.

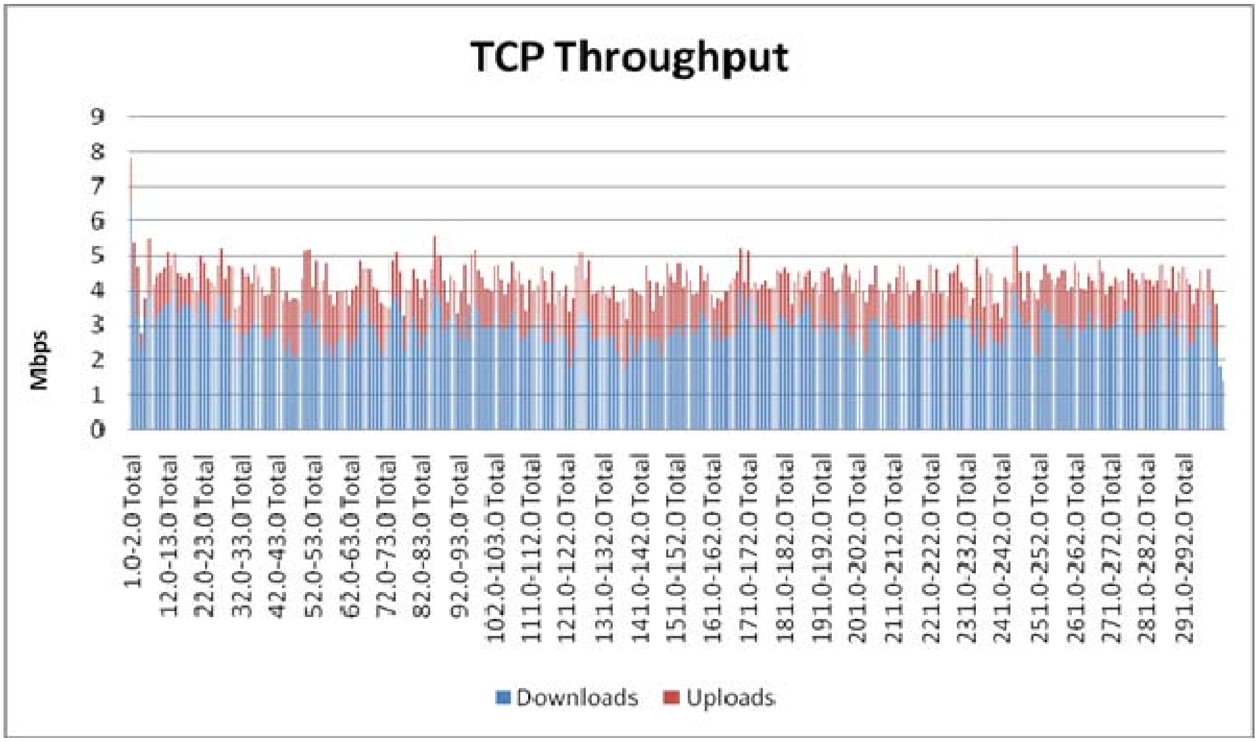


Figure 23. End-to-end TCP throughput (Test 2)

The results from this topology seem fairly similar for link data rates, but the per flow rates drastically differ. As depicted, the combined upload flows occupy about 25% of the capacity for the overall data. Figure 20 illustrates this type of activity, but does not indicate that it is as prevalent (i.e., sometimes the upload flow would win the conflict and share the channel capacity). This type of behavior seems consistent with data starvation where the downloading flows are competing with the upload flows for throughput.

The setup configuration for the following UDP test was identical to that of test 1. The UDP results for this test were very similar as well. UDP traffic injected by iperf software with one computer configured to initiate one client for pulling and pushing continual 1470 byte datagrams across 3 flows (1 uploading and 2 downloading), with UDP buffer size of 8 Kbytes for a duration of 300 seconds (5 minutes).

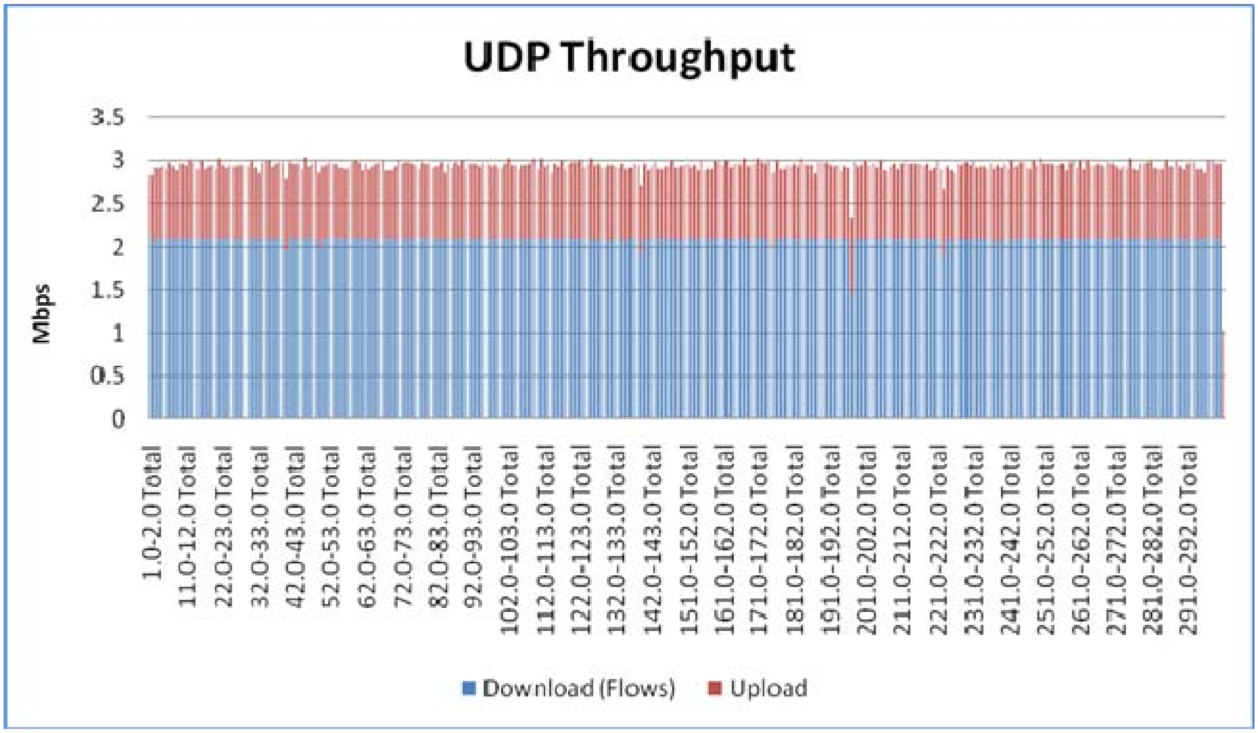


Figure 24. End-to-end UDP Throughput (Test 2)

The takeaway from these graphs is that the results are similar to test 1, suggesting that the added routers do not add significant delays to the network. This makes sense, given that the Cisco routers were configured to operate their interfaces at 100 Mbps. In retrospect, it would make more sense to throttle the links at the Cisco routers in an effort to prevent congestion at the radios. This might have prevented the observed buffer overflows. Without knowing the actual buffer size on the radios the process becomes trial and error. These results gave a good base line for evaluating the tactical radios' integration capability with cellular technology and vice versus.

c. Test 3

The third test (topology illustrated by Figure 25) consisted of evaluating the Ericsson QuicLINK base station for a base line before integrating the two networks. For this test, one wireless client was provisioned via a 3G WCDMA air-card and the QuicLINKs base station ran independent of any other wireless provisioned devices. In an effort to measure capacity between the QuicLINKs and clients, the other client was connected directly to the LAN interface side. If clients are connected via air-cards, then the bottleneck between the two clients would be the weakest link capacity (i.e., the uplink for each device, since the power output and antenna gain of the base station is significantly different than that of the wireless devices). The power output for the QuicLINKs is statically assigned at 10W. The antenna used for these tests was the Harris (RF-3186-AT320 500 MHz - 2 GHz UHF) antenna.

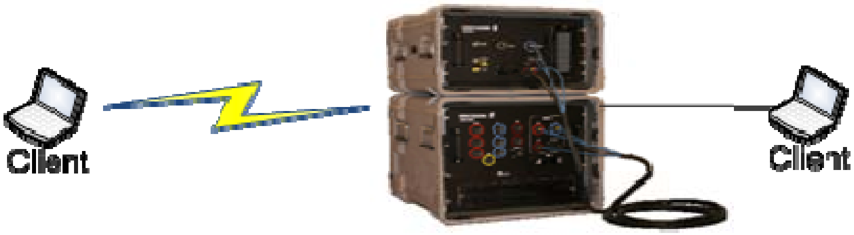


Figure 25. Throughput Test 3 Topology[12]
(Ericsson, 2009)

The TCP traffic was injected by iperf software with one computer configured to initiate one client for pulling and pushing continual 1470 byte sized packets. Iperf transmitted across 20 flows (10 uploading and 10 downloading), with a TCP window size of 8 Kbytes for duration of 300 seconds (5 minutes). Upon completion, the iperf output resulted in an average of 1.5 Mbps uplink and 1.5 Mbps downlink, giving a total of 3 Mbps link capacity. In anticipation of a faster downlink, the test was run again with 6 UDP flows dedicated to the downlink and zero uploading flows. The result was a link capacity of about 5.8 Mbps. The same test was completed for the uplink and the result was a capacity of about 1.6 Mbps.

d. Test 4

A fourth test, based on Figure 26 topology, was conducted in an anticipation of the future employment architectures leveraging similar devices for primarily connecting with other internal users.

[12] The Ericsson QuicLINK picture was taken from the reference, however the author created the overall figure.

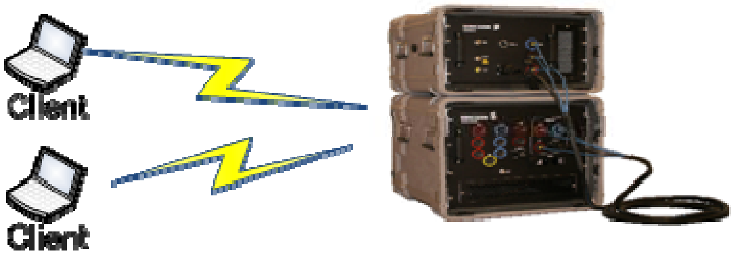


Figure 26. Throughput Test 4 Topology[13]
(Ericsson, 2009)

As with the previous test, the TCP and UDP protocols were used to evaluate the base station data capacity using the iperf software. Multiple flows were initiated to identify how the device would handle each one. Figure 27 shows the results from a TCP test having identical characteristics (i.e., same window, packet size, and duration) as previous 10-flow (5 uploading and 5 downloading) TCP test. In the next couple of graphs, the results are combined into ten second periods and only display the average for that timeframe.

[13] The Ericsson QuicLINK picture taken from reference, however the author created the overall figure.

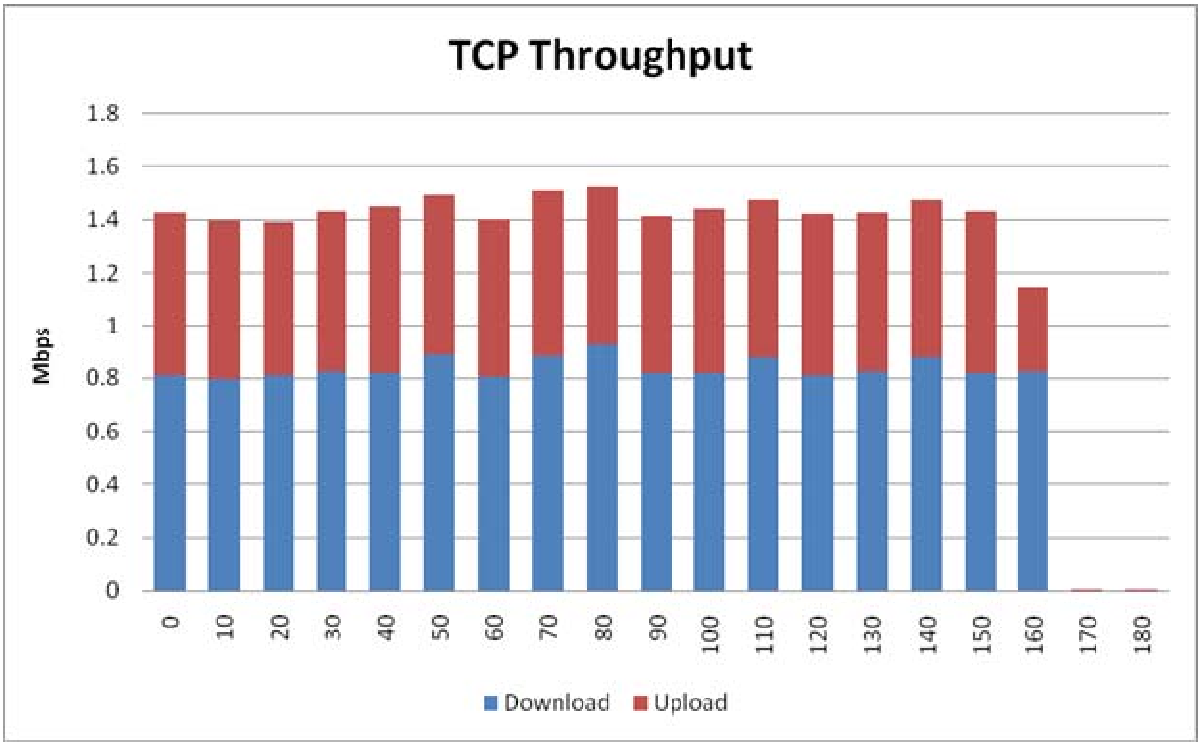


Figure 27. QuicLINK TCP Throughput (Test 4)

Notice Figure 27 shows a lower rate of throughput compared to previous UDP test. This difference could be attributed to the maximum uplink capacities. These results are consistent with the rates observed during test 3. This suggests that adding any additional wireless clients should not affect the rate per client.

Given the same topology (air-card client via QuicLINKs to air-card server) the group ran two UDP test with the same parameters as before. The purpose of these tests was to establish comparable results and evaluate possible shortfalls in the previous tests. This test ran (Figure 28) to completion at 300 seconds and did not identify any inconsistencies with the previous data.

The most observable results illustrated by these figures for test 4 and the previous results from test 3 are the throttled data rate on TCP at 1.4 Mbps and the shortened upload flow for the UDP test. These observations suggest an average link capacity of approximately 1.5 Mbps regardless of the transport protocol used.

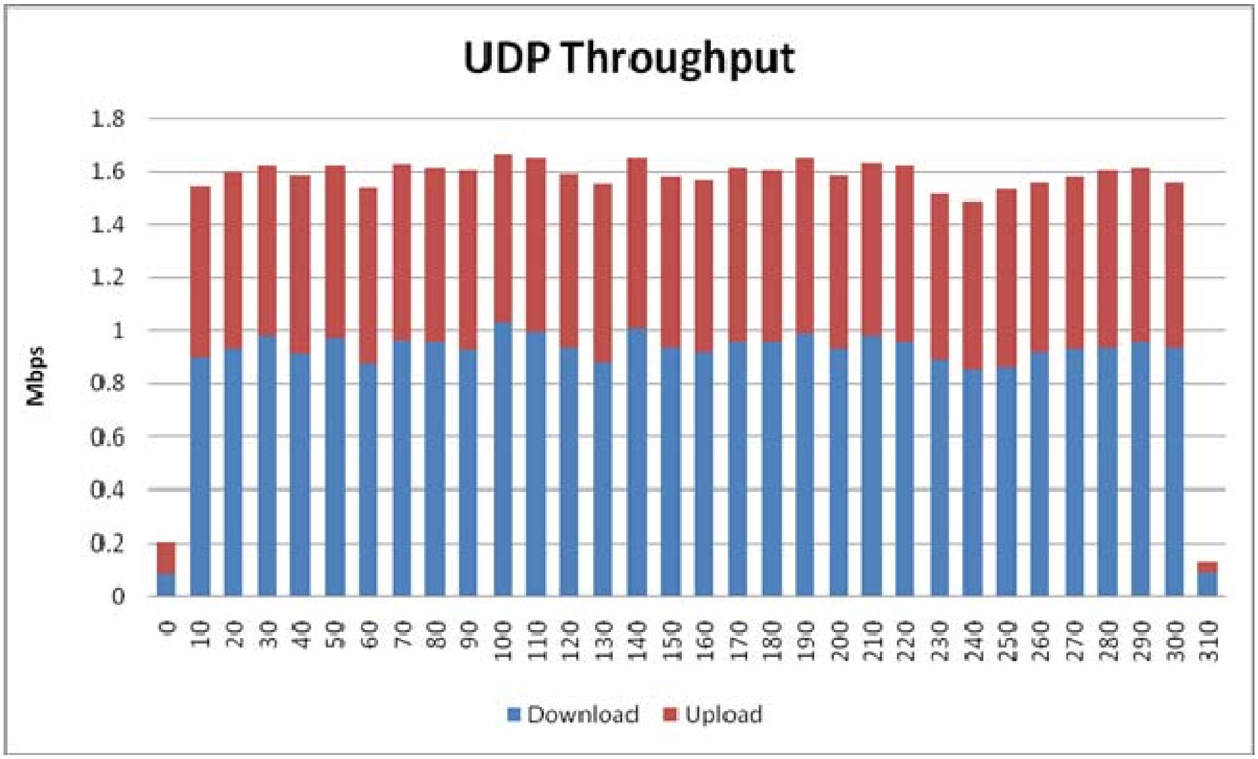


Figure 28. QuicLINK UDP Throughput (Test 4)

The observed data rates are identical to the rates of the UDP test 3. The only observable difference from the previous test is the packets being fragmented. It is not possible for TCP packets to be fragmented given the protocol behavior, but UDP packets can be fragmented when the source Maximum Transmission Unit (MTU) is different than the destination MTU. The result of fragmenting the packets can cause time delays if extreme enough. For this test, every packet was fragmented with the largest frame size of 1512 bytes. However, the largest packet was measured at 1444 bytes. This suggests a header and tail size of 68 bytes. The average packet was captured at 1396 bytes with an additional 14 bytes in the frame header. Therefore, this suggests the QuicLINKs is adding additional bytes for error correction and fragmenting, because their MTU is smaller than normal. This difference could be attributed to the additional error correction bytes. The additional error correction bits are not a major concern for the integration concepts; however, the fragmentation issue is a problem—over time this could cause significant capacity degradation.

Therefore, when designing a deployable network, one solution to this problem is to fix the frame size (MTU) at 1400 bytes (i.e., anticipating transport mediums like Ethernet, which have a default frame size of 1500 bytes).

e. Test 5

For the final test (illustrated by Figure 29), all tested devices were now combined to explore the concept of bridging the cellular network with the tactical one as discussed in the last chapter. The end-to-end architecture contains one client attached to the network via 3G QuicLINK provisioned air-card and the QuicLINKs base station attached via a dedicated Virtual Local Area Network (VLAN) on the Cisco router. On the other side, a client was attached to a switch with other computers connected.

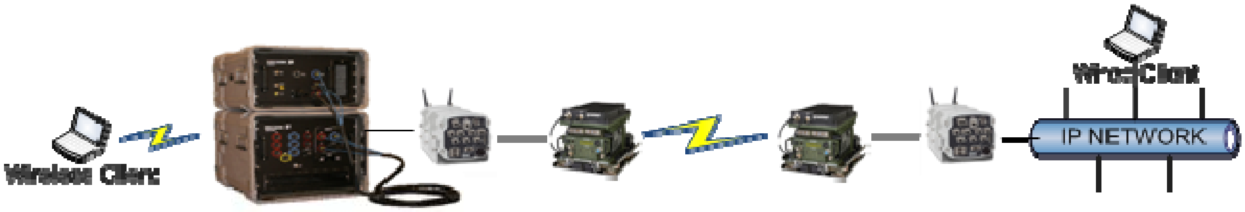


Figure 29. Topology Test 5 (End-to-end)[14]
(Ericsson, 2009; Cisco, n.d.; Harris Corporation, 2009)

During half of the test we adjusted the 117G radios to operate with the two previously configured 2 node max configuration and operate at the 305 MHz frequency, with ANW2, WID 7, 50W amplifiers with 4 km LOS separation, UHF vehicular dipole antennas (225 to 450 MHz). Additionally, we ran a further test to evaluate the higher frequency mode with ANW2. During that part of the test, the radios were configured for 1785 MHz, with UHF vehicular dipole antennas (500 MHz to 2 GHz). In this mode the radios were not capable of leveraging the 50W

[14] The graphics were taken from references, however, overall all figure was created by author.

amplifiers; therefore the power output resides around 5Ws average with peaks up to 20 Watts.

This first part of the test was limited to 10 TCP flows, as the previous test validated the radios capacity around this rate. The radios were configured for the 305 MHz mission plan.

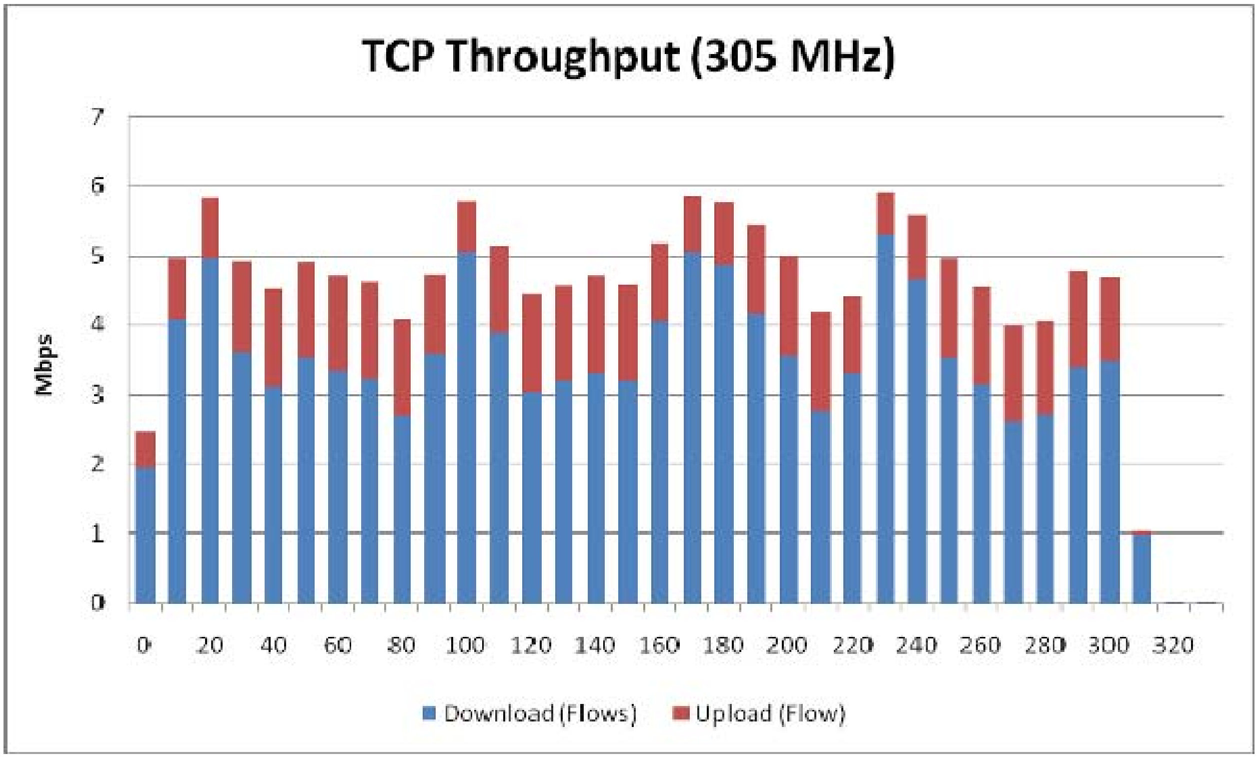


Figure 30. End-to-end Fully Integrated TCP Throughput (Test 5)

The data in Figure 30 is consistent with the previous data as the uploading data rate (constricted by the uplink rate on the QuicLINKs), on average returned a 1 Mbps capacity. Since the downlink from the QuicLINK to the air card has a much larger capacity, the protocol compensated for the difference and allocated more bandwidth. Because we've restricted the transport protocol, the link capacity averaged just above 3.3 Mbps. These results are very promising for a topology, which leverages QuicLINK and PRC-117G type devices. The military is no longer in the kbps throughput ranges, with which service members are more familiar.

The same test above was run again with the 1785 Mhz mission plan for the 117Gs. The distance stayed the same at 4 km LOS. Our first test failed after 80 seconds and therefore we ran an additional test with only 6 flows (3 uploading and 3 downloading). The observed WID originally started at 5 and then increased to 7 before and during the beginning of the test. The figure below is color coded by individual flow (the number signifies the port number) and illustrates the throughput rate per flow as a function of time.

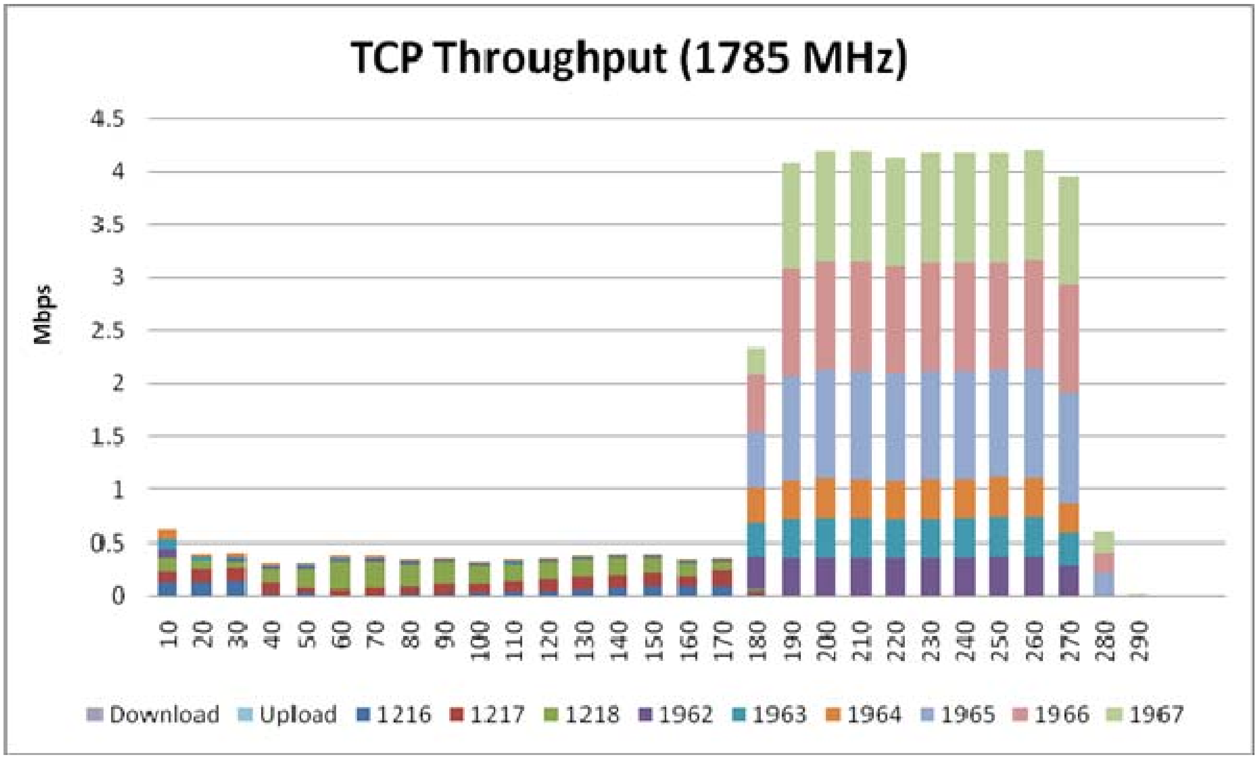


Figure 31.   End-to-end TCP 1785 MHz Throughput (Test 5)

As Figure 31 illustrates, during the first 170 seconds of this test we observed WID 5 and 6, at about the 170 mark the radio transitioned into WID 7. Therefore, with the additional bandwidth (in MHz) the radios allocated more capacity. It appears that iperf was monitoring the link capacity indicated by the packet capture data identifying three TCP FIN packets received at 170 seconds followed by multiple reset packets. As we have seen in all the previous TCP figures, iperf pushes a larger amount of packets in the beginning to test the link capacity (monitoring packet loss).

The result of the radio's increasing capacity facilitated iperf canceling three flows and initiating three other flows. The significance of this data highlights the capability of the entire network and shows the ability of the network to recover autonomously from harsh environments. However, at about 280 seconds, the PRC-117G radios faulted without recovery. This is the same issue identified in earlier tests (confirmed by a Harris representative). The fault requires the recycling of the radio. However, this is a known issue and a Harris representative reported it will be fixed in the next firmware release.

For the next part of the test, referencing Figure 32, we reset the PRC-117G radios to the 305 MHz mission plan, iperf injected UDP traffic with constant 1470 byte datagrams across 3 flows (1 uploading and 2 downloading), and used a UDP buffer size of 8 Kbytes for a duration of 300 seconds (5 minutes). After only about 100 seconds of run time, the network crashed (stopped forwarding traffic). Some packets were fragmented, but the majority of the frames were transmitted at 1512 bytes without fragmentation. After we terminated the iperf software the network recovered without recycling any of the equipment.

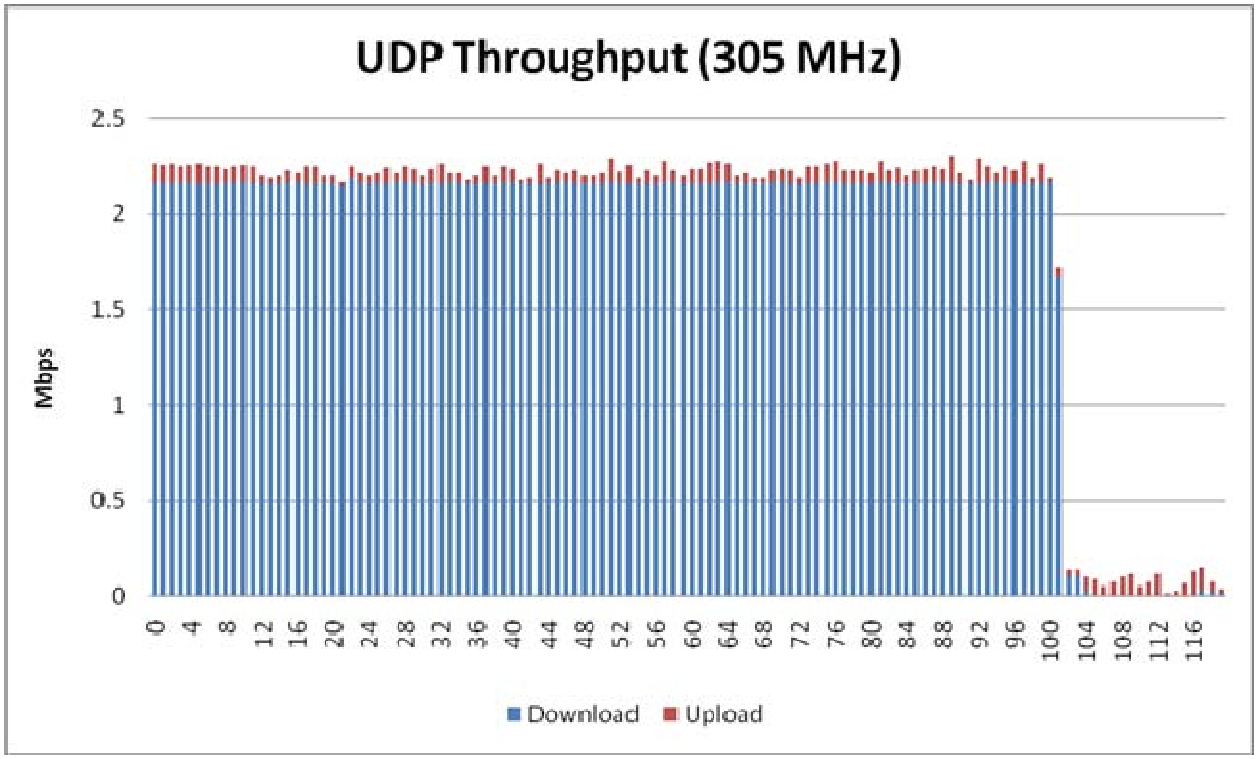


Figure 32. End-to-end UDP 305 MHz Throughput (Test 5)

Two things are worth noting from this test: (i) the uplink traffic (cellular client to LAN client) was completely lost or dropped and (ii) the test failed even when the flows were restricted to 1 Mbps. When we look at the iperf results and wireshark captures, it appears that the majority of the uploading flow packets were dropped or lost. The only fragments for this run were the uplink frames initiated from the aircard client. It appears the QuicLINKs was fragmenting the traffic on the uplink side, but not on the downlink. When the fragmented packets arrived at the LAN client, the UDP layer seems to have been removed.

On the next test, we used the same iperf configuration as the previous test. The only variation of this test included changing the mission set on the PRC-117G to operate at 1785 MHz frequency. Just as before, the 1785 MHz frequency band is not capable of using the amplifier (i.e., no frequency above the 500 MHz range is capable of leveraging the amplifier). Therefore, we ran this test at an average of 5 watts of power output and 4 kilometers of separation. As with the previous test, fragmentation occurred again. This time, however, every packet was fragmented and therefore it would seem that every time the frames are fragmented, the throughput of the link was abnormally affected. The following graph (Figure 33) displays the rates received at the 1785 MHz frequency and ran to completion.

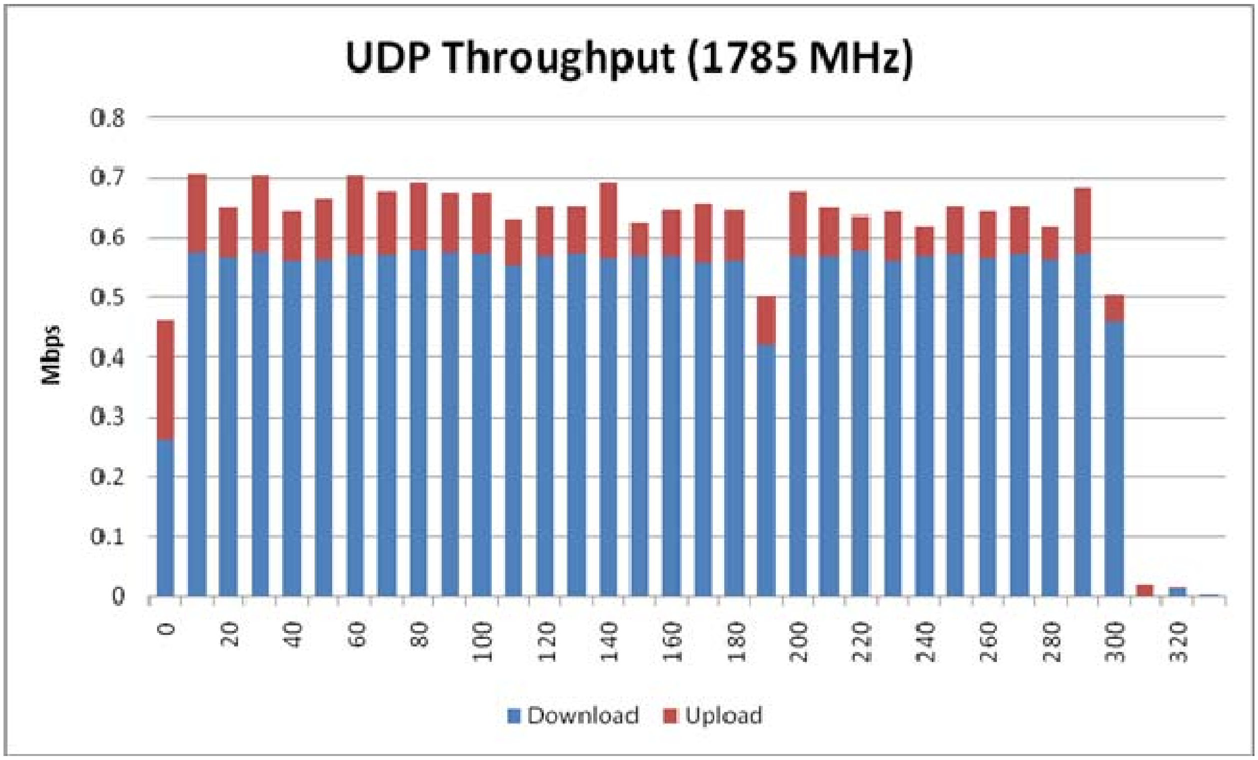


Figure 33. End-to-end UDP 1785 MHz Throughput (Test 5)

Notice the limited throughput again suggesting the fragmentation is causing a large reduction in data rates. We conducted the throughput testing to highlight the potential of the overall integration. The results are not comprehensive and should only be viewed as a rough estimate.

2. Emission Testing

For the second half of the exercise, we tested the individual communication devices and evaluated for emission detection. The test leveraged the Hewlett Packard 8562A Spectrum Analyzer with an estimated cost of $5000 according to eBay bids and other auction sites. The device was connected to a computer and an external omnidirectional 10db antenna without an additional amplifier. The device is capable of monitoring a range of 9 kHz to 22 GHz with a sensitivity of -110 dBm (Hewlett Packard).

The following screen capture (Figure 34) illustrates the emissions environment for the test. The screen capture shows the frequency between 30 MHz to 2.5 GHz. The resolution bandwidth is set at 2.0 MHz for this frequency span and therefore any signal within 2 MHz proximity of each other will appear as one signal. Some of the frequencies display emissions at high power levels. This result is most likely attributed to the environment being located outside of a satellite installation and military airfield. The indicated points on the screen capture highlight our equipment emissions within close proximity of the transceivers and our spectrum analyzer's receiver. The green line represents the average signal return as a function over time. The purple line represents the maximum return achieved within the measured time. The left side of the screen capture details total time measured incremented sequentially (MAX HOLD and VID AVG). A few things should be noted: (i) the top of the screen capture starts at -10 dBm and each horizontal grid line represents another 10 dBm; (ii) the tactical radios are easily masked by the noise floor at this resolution; however, the screen capture measures the local 117G with 50W amplifier attached, the local one was turned off after this capture); (iii) the TacBSR is not detected at this resolution most likely because of the distance and the power output of only 350 mW; (iv) the cell phones were detected, because they were within close proximity (30ft) of the spectrum analyzers receiving antenna and 4 km from the base station; (v) with these parameters the machine noise floor is about -74 dBm and therefore some of these signals will be more prevalent when the span and resolution are narrowed.

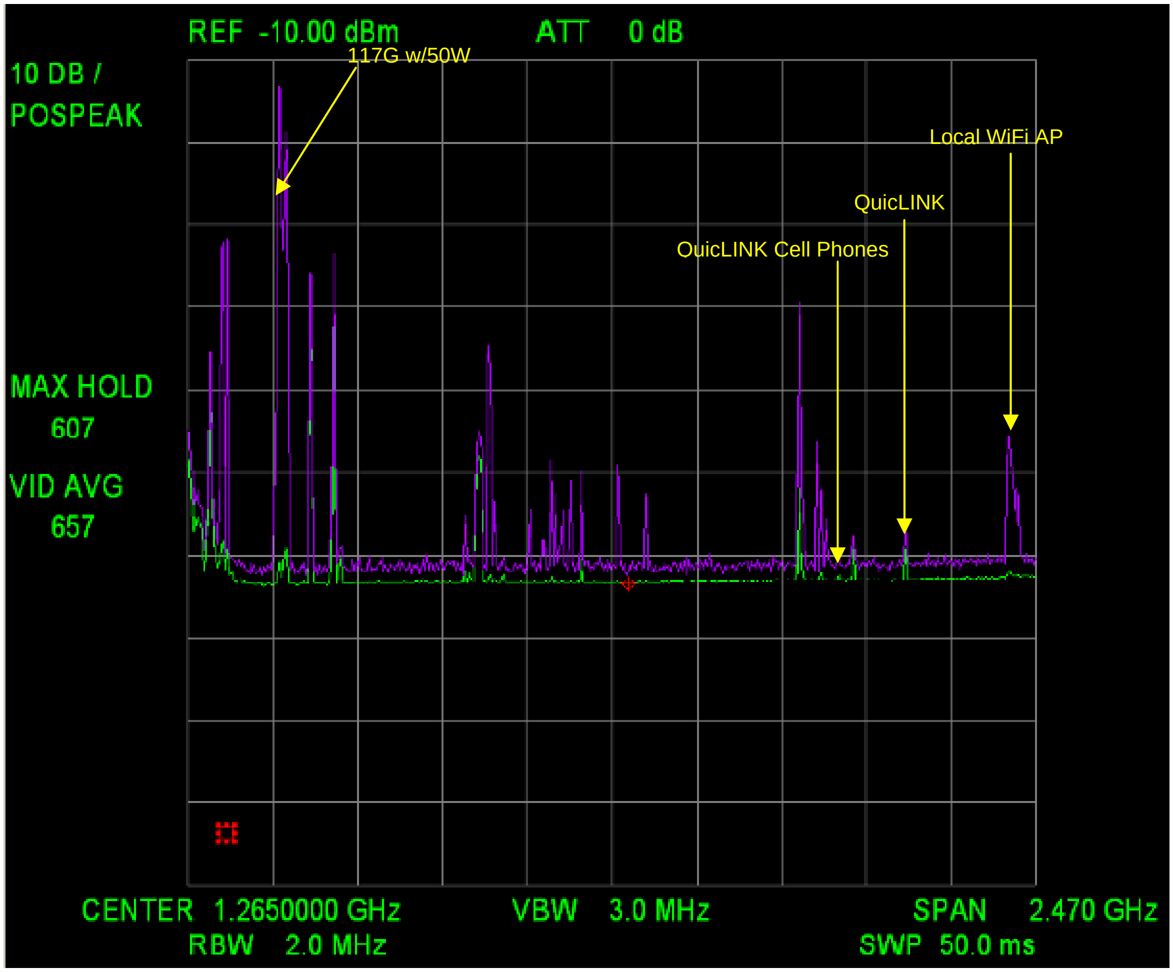


Figure 34. 30 Mhz to 2.5 GHz Spectrum (Test 6)

Figure 35 illustrates the Harris 117G radio emission signature operating ANW2 with 50W amplifiers at the 305 MHz center frequency with 5 MHz bandwidth. Figure 36 illustrates the same radio, waveform and bandwidth in Hertz; however it is operating at a less power (5W average), and a greater distance (4 km separation). The screen captures depict an average and max hold over time. Normally, in real-time you would see the signal hopping; however, since this is a still capture, the figure depicts a snapshot of the results at a specific instant in time. The max hold number on the left side of the capture depicts how long the sample has been compiling returns. For Figures 35-38, in order to maintain a controlled experiment, (since every tactical radio shares the frequency band) only the monitored radio was active during each emission test (i.e., no other radios were associated or even turned on). As you continue through the following figures remember the radios were not associated and therefore should not be detectable unless they are transmitting.

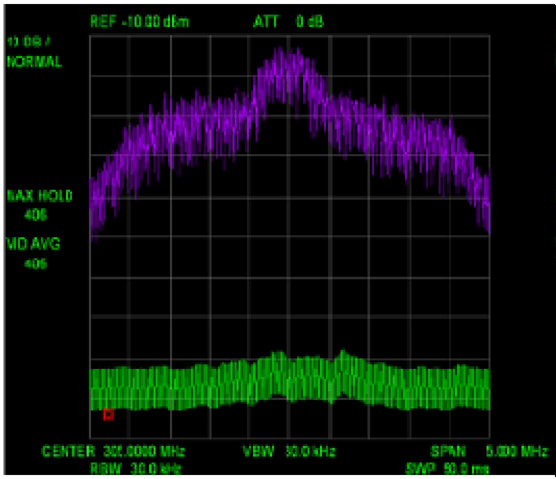


Figure 35. . PRC-117G, 305 MHz Center at 50 W, 5 MHz bandwidth, with 65ft Separation

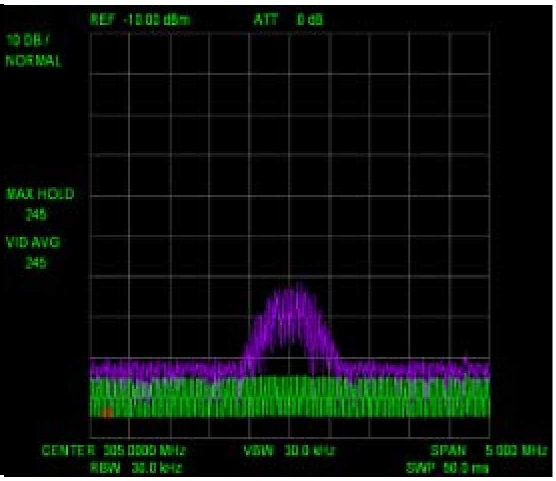


Figure 36. PRC-117G, 305 MHz Center at 50W, 5 MHz Bandwidth, with 4 km Separation

Figure 37 illustrates that the radio emits -15 dBm of power at the center frequency. This is mostly due to the limited distance (i.e., 40ft LOS) between the receiving spectrum analyzer and transmitting radio. Figure 38 illustrates the exact same radio's emissions with the same configuration, but with a separation of 4 kilometers. Notice at this distance the signal is obviously detectable; however, possibly not very easy to intercept. The video average emission (green line) is slightly affected and therefore can increase the likelihood of detection. The second thing to note is that the power output of this signal is not evenly distributed across the span. The center frequency is given more power and less around the edges. Perhaps, the power is limited at the edge to provide a guard band for neighboring channels. The increase of power in the center can give other identically configured radios an advantage; however, as Figure 36 illustrates, this advantage could be considered a vulnerability that an adversary might leverage to detect the emissions. It should be mentioned that the machines threshold of the noise level for these captures are on average -100 dBm. However, the actual noise level is a little lower. The actual noise level for each of these captures can be calculated using the power spectral density for thermal noise equation ($N_o = kT$). The average temperature for this test was about 25 degrees Celsius (i.e., 298.15 Kelvin). Therefore, using Boltzmann's constant of $1.5x10^{-23}$, the average noise spectral density for all the emission testing was about $4.47x10^{-21}$ W/Hz. Using this number we can easily convert the units into watts by multiplying the RBW by the noise spectral density. The product results in an actual floor for figure 35 and 36 of about -128.73 dBm. This means the spectrum analyzer is unable to view about -30 dBm more of power at this frequency. Therefore, with more sophisticated resources the signal becomes more visible.

The next two figures (Figure 37 and 38), are identical to the previous figures except the frequency on the radio was altered to 1785 MHz for a center. At this frequency, a different antenna was leveraged (RF-3186-AT320 500MHz – 2GHz) and the vehicle amplifier adapter (VAA) was not capable of amplifing the signal. Therefore, at the 65ft reading, the emission was detected at -45 dBm vice the previous -15 dBm.

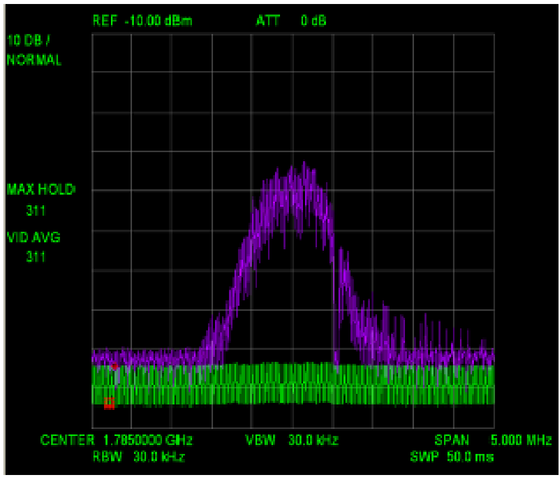


Figure 37. PRC-117G, 305 MHz Center at 5W, 5 MHz Bandwidth, with 65ft Separation

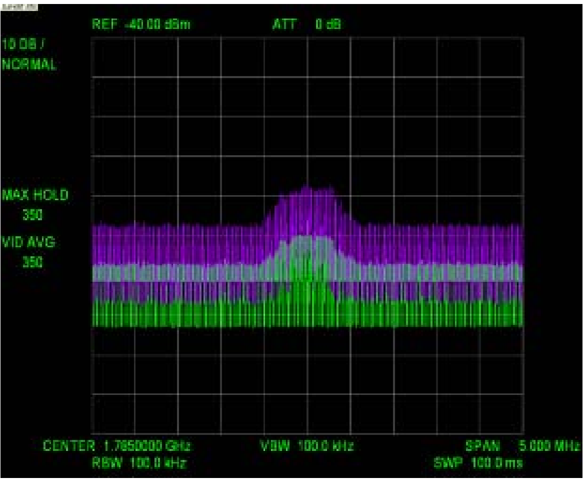


Figure 38. PRC-117G, 1785 MHz Center at 5W, 5 MHz Bandwidth, with 4 km Separation

It is evident that Figure 37 is significantly different than the previous emission signature (Figure 35). This is most likely due to the radio operating at a different output power. As confirmed by a Harris engineer, even though the radio was configured to use 5 MHz of bandwidth, it automatically determines the span based on the quality of the environment. This figure appears to be consistent with Harris's proprietary labeling of waveform identification (WID) 6. As before, Figure 38 shows the same setup, but at a separation distance of 4 km. Figure 38, is illustrated at just about the noise floor of the machine. Therefore, given the RBW of 100 kHz, the calculated noise floor is about -123.50 dBm. This represents about -13 dBm of power remaining visible. With this little power the radios will most likely not operate at a maximum capacity, but should still operate as the previous throughput testing found.

The next figures illustrate a different tactical radio's signal (Trellisware Cheetah) with attached amplifier (Wildcat, 10W power output), which performs frequency hopping. The figures show a capture in time with more than 400 samples of the 1785 MHz frequency center with 20 MHz of bandwidth. Notice the previous radio emissions signatures (Figure 35-38) are spread across the spectrum with more power in the center as opposed to the following figures, which illustrate a more evenly distributed signature.

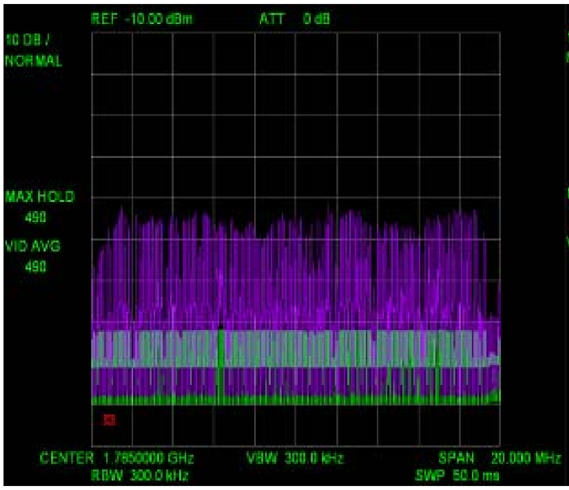


Figure 39. Trellisware Cheetah Radio, 1785 MHz Center at 10W, 20 MHz Bandwidth, with 40-ft Separation

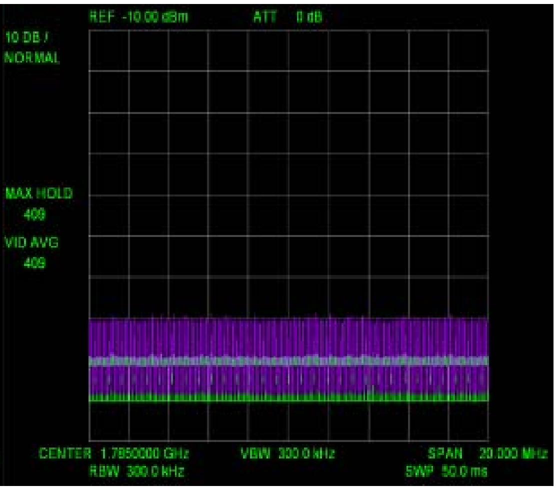


Figure 40. Trellisware Cheetah Radio, 1785 MHz Center at 10W, 20 MHz Bandwidth, with 4 Kmm Separation

Figures 39 and 40 both represent Cheetah’s emission signature without any other radios attached to the network (i.e., only one device emitting at 40 ft and 4 km respectively). Figure 39 shows that the maximum hold has not clearly defined an apparent solid horizontal line at 490 seconds. We expected this, because the previous PRC-117G (Figures 4 and 36) utilized a more narrow frequency span and this radio is using 20 MHz. Assuming that the radios use the same speed hopping pattern, this should take 4 times (20:5 MHz ratio) as long to create that clearly separated max hold line. However, based solely on visual observation during the time of capture, it appears the hopping pattern is faster on the Cheetah radio. This could make it harder to intercept and exploit. Figure 39 presents another valuable observation in regards to the varied line weight. Notice, some of the measured power returns a value of around -75 dBm, but over time the values increased randomly across the span at -55 dBm and -65 dBm. This varied signal power could be an indicator of power control. Since no other radios were attached to the network, the radio could be sending out a hello message to locate other unidentified nodes. Notice Figure 40 is virtually invisible above the spectrum analyzer’s noise threshold. Since the signal is spread evenly, it appears as noise. The calculated noise floor for this capture is -118.74 dBm. Therefore, the capture does not illustrate -20dBm of power per frequency.

The reason for presenting the tactical radio emission signatures in the beginning was to identify characteristics that make their signatures different than the commercial non-LPD/LPI equivalents. The next figures highlight Ericsson’s QuicLINK base station uplink spectrum. One major difference to note is the following signals are full duplex. Therefore, each side of the link is transmitting and receiving on separate frequencies. All of the previous radios were half-duplex and, therefore share one frequency for transmitting and receiving. The following figures represent the uplink (cell phone transmitting to the base stations), which is allocated for cell phones to transmit and the base stations to receive.

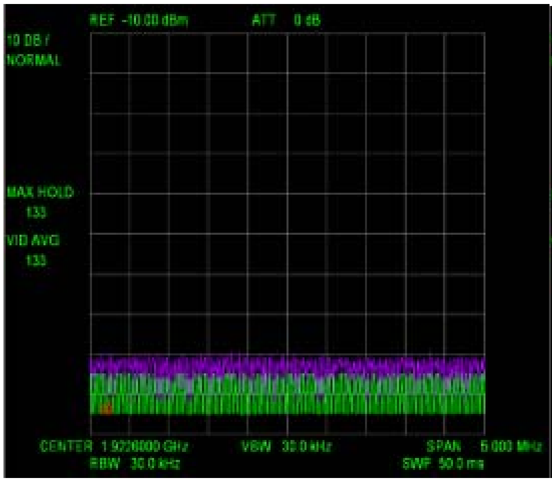


Figure 41. Ericsson QuicLINK Uplink, 1922.6 MHz, 5 MHz Bandwidth, Base Station 40-ft Separation, with Cell Phone at 30 ft from Spectrum Analyzer Receiver

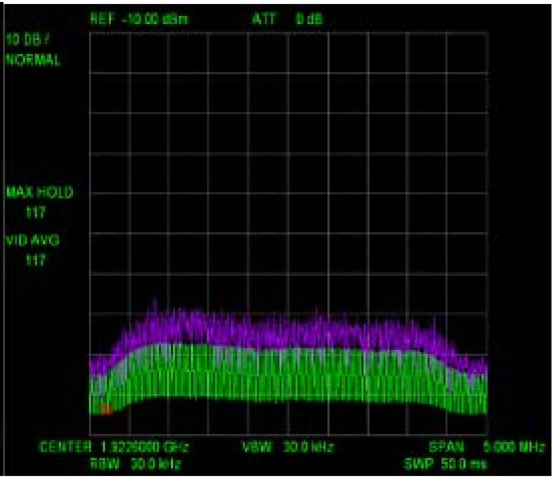
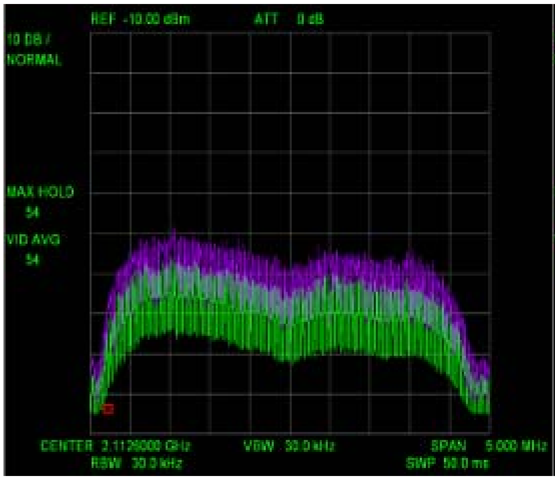


Figure 42. Ericsson QuicLINK Uplink, 1922.6 MHz, 5 MHz Bandwidth, Base Station 4 km Separation with Cell Phone at 30 ft from Spectrum Analyzer Receiver

Figure 41 appears to be noise, likely resulting from the close proximity of the base station to the cell phone (30 feet separation). Figure 42 is the result of the frequency when the base station was driven out 4 km from the provisioned local cell phone. It seems reasonable to assume that the phone increased its power output to compensate for the long distance between devices. This suggests the phone is using a power control method to limit and increase the transmit power as required. Therefore, if an adversary is leveraging similar equipment, they could detect the emissions when the provisioned cell phone and associated base stations are at a considerable distance apart. Even with the noticeable signal at this resolution, it would be much harder to identify the emissions if the actual frequency band was unknown. However, given the power reading of the local phone (-80 dBm), the signal detection would be much harder if at all possible beyond a greater distance (i.e., considering this reading was measured at 30 ft of separation between the cell phone and spectrum analyzer receiving antenna). The most significant difference between the following cellular signatures and the previous tactical radios is the video average (i.e., the green line). In the previous figures (Figures 35-39), the green line had very little if any movement; however in the above Figures 41 and 42, the average measured signal is similar to the maximum hold pattern. This is most likely a result of the previous signals masking their emissions by hopping across various frequencies and therefore, the majority of the time each frequency was not used. For example, if the span is broken into 20 smaller size channels over a period of 400 seconds, each channel (if evenly distributed) would contain power 5% of the time. Since the green line is depicting the average, the 95% would over shadow the 5%, and the line appears flat. Therefore, no single frequency is occupied long enough to affect the average (i.e., a LPD/LPI signal). However, Figure 42 illustrates a different picture—each frequency contains power. This suggests power control capable handset are harder to identify when in close proximity to their provisioned base station.

The next figures highlight the QuicLINK base station downlink (i.e., the base station transmitting to the cell phone) spectrum. The link is reserved for the base station's transmissions. As you will notice from the first figure on the left, the signal is easily identifiable in close proximity. However, at the longer distance the base station's signal looks extremely similar to the uplink (cell phone transmitter) frequency. Without knowing the actual uplink and downlink frequency spans, an advisory could easily mistake one for the other. This makes it easier for blue forces to blend in with the local commercial providers.



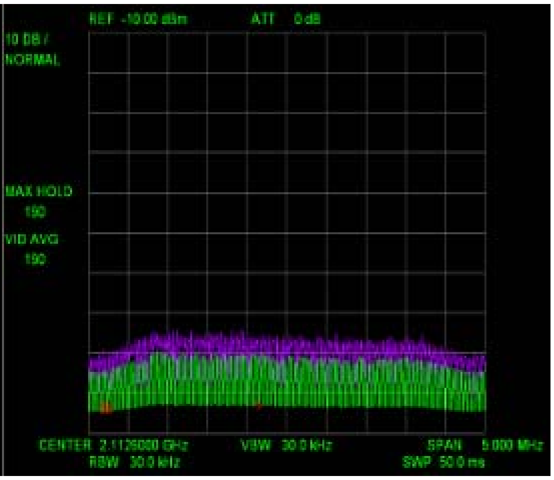


Figure 43. Ericsson 3G QuicLINK Downlink, (Base Station Transmit), 2112.6 MHz at 10W, 5 MHz Bandwidth, and 40ft Separation

Figure 44. Ericsson 3G QuicLINK Downlink, (Base Station Transmit), 2112.6 MHz at 10W, 5 MHz Bandwidth, and 4 km Separation

Figure 43 (QuicLINK base station) shows that at close proximity the spectrum analyzer illustrates receiving similar power (-60 dBm) as Figure 39 shows (Trellisware Cheetah). This similarity is directly related to the fact that both devices were emitting 10W of power and leveraging the same antenna, but obviously at different times. However, the video average is significantly different, which suggest a constant emission signature. Therefore, the power control is only occurring on the cell phone and not at the base station.

The next figures represent similar radios—a cellular base station and a cell phone. However, the protocol we used is drastically different. Figure 45 and 46 represent the signal emissions received from an LGS Innovations TacBSR GSM base station (pico cell). The purpose of these captures is to illustrate the significance between the two technologies (CDMA and GSM). We conducted the captures in a lab environment with 70 db of attenuation to simulate the 25 meters of distance and extracted them from an Agilent E4405B spectrum analyzer. These captures are not meant to be representative of a field environment as the previous figures, but at least they give a good depiction of the signal's characteristics. Figure 45 illustrates the cell phone emissions captured when the device was provisioned with the base station; however, no continuous conversation or data was transmitting. The yellow video average line is not similar to the max hold line, only because a constant transmission is not present. Figure 46 represents the base stations transmission frequency. Notice the video average line is similar to the max hold line. This is evident most likely because the base station is constantly transmitting to allow listening cell phones an opportunity to request provisioning handshake information.

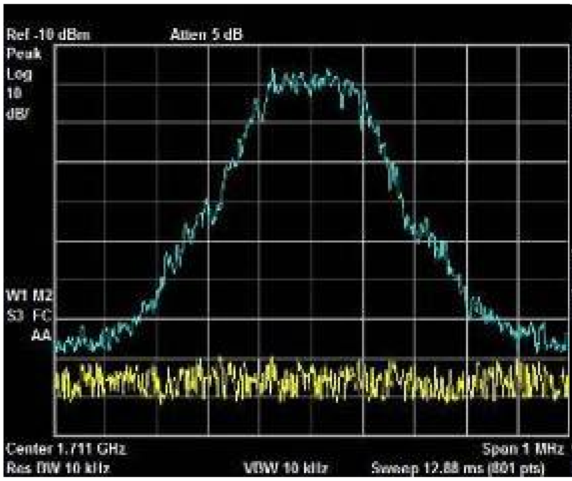


Figure 45. LGS Innovations TacBSR Uplink, (Cell Phone Transmit), 1711.0 MHz mW, 1 MHz Bandwidth, and 20 ft Separation

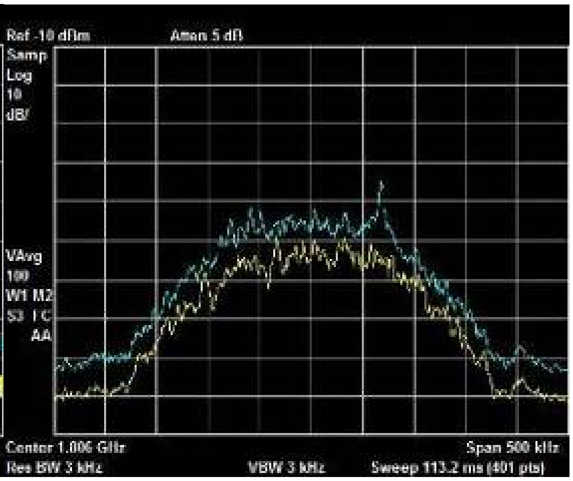


Figure 46. LGS Innovations TacBSR Downlink, (Base Station Transmit), 1806.0 MHz at 350 mW, 500 KHz Bandwidth, and 25 Meters Separation

The largest takeaway from the cell phone emissions channel is that neither the max hold nor the video average lines were detecting any signals above the noise level until a cell phone actually attempted to place a call or send data. This mean a normal (GSM) phone will most likely not be detected unless it initiates a call, receives a call, or sends data traffic.

This device occupies a channel size of 200 kHz and that channel is broken into 25 kHz smaller sized channels. Notice the 200 kHz channel occupies only about the top 5 dBm from center. Figure 47 illustrates the actual channel size with additional space on either side. The figure was captured during a constant transmission, represented by the yellow line.

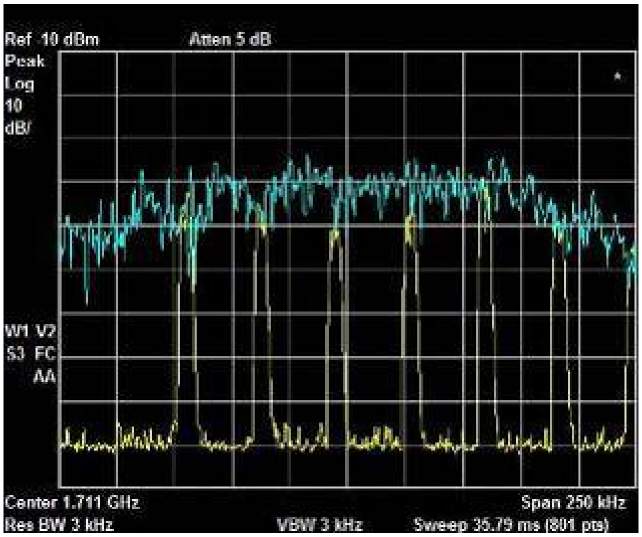


Figure 47. LGS Innovations TacBSR Uplink, (Cell Phone Transmit), 1711.0 MHz mw, 250 kHz Bandwidth

The most significant take away from this chapter is that military tactical radios have matured enough to support 3G cellular traffic. The traditional military radio with the limited throughput rates is a thing of the past—the larger the available bandwidth the higher throughput potential. The second take away, is that cellular handsets have potential for minimizing emission signatures. For the power control capable handsets and when the base station was in close proximity, the resulting emissions signature suggested a less detectable profile than common military LPD/LPI tactical radios. The final take away, as evident by the radio resets, buffer overloading, and the fragmented packet issues, both the cellular base station (QuicLINK) and the tactical radio (PRC-117G) had problems with an unmanaged network. This data suggest an additional service (e.g., IntServ) is required to prevent future networks from being overwhelmed.

V. Conclusion

A. Potential Solutions

Based on the analysis of Chapter III and the experimental results of Chapter IV, the idea of extending our tactical network's edge by integrating commercial handsets seems feasible. However, the magnitude of desired integration significantly depends on the level of acceptable risk. Given the susceptibility of current commercial cellular technology, if the military desires the cellular handset capability down to the lowest level, a tiered approach is suggested as follows.

- For Phase I—procure (i) commercial standard equipment to supplement preexisting infrastructure (completely commercial concept), (ii) handheld devices suitable for the commercial standards along with the ability to process the encryption algorithms for secure communications, and (iii) mobile base stations (i.e., pico, micro, and macro versions) for environments not developed enough to support the required infrastructure (indirect concept). The cellular handset should possess the capability to directly transmit traffic and participate in a WAN via a cable (tethered concept) for environments with high emission control requirements.

- In Phase II—eliminate the devices and technology that weaken security and prove to be most costly. For example, the indirect concept can become extremely costly (i.e., higher throughput base stations cost significantly more than a typical vehicle mounted tactical radio). On one hand, one may purchase base stations with a limited number of channels, but now are limited in data rates and user capacity. On the other hand, one may purchase high capacity base stations, and end up wasting capacity due to a high channel to user ratio (i.e., a convoy using a costly mobile base station for edge communications, 20 service members to 1 base station capable of a 1200 channel capacity costing $250,000). Additionally, new procurements could be required to replace older cellular handsets, which prove vulnerable to various attacks.

- For Phase III—implement the suggested COAs within the direct method: increase emission security for commercial cellular handsets, reduce the commercial infrastructure footprint, develop a software implementation of the tactical cellular base stations as an additional waveform on the tactical radios, and design security layers to increase software portability and mitigate malicious code vulnerabilities. By converting the cellular protocols to a software implementation, this facilitates hardware independency, which is imperative to reduce the overall costs. Essentially, choose which radios already contain the hardware requirements, and then design the wireless protocol to host the network. On the acquisition side, instead of procuring 1000 radios with this capability, the military acquires 1000 licenses to install the protocol (waveform) on their inherent radios. This approach assumes most defense contractors (i.e., radio manufacturers) would need to develop compatible firmware for the capable radios, given that this expense is exponentially cheaper than the alternative of designing new hardware models for this capability.

In technical aspects, the major takeaways from this thesis are three-fold. First, modern day military tactical radios have the potential capacity to support 3G edge cellular networks without significant degradation of services. Throughout the experiment chapter, multiple tests proved link capacity above megabit data rates on both the tactical radio and 3G cellular base station. These results demonstrate that modern day tactical radios have the capacity to host 3G cellular services.

Second, the level of LPD/LPI classifications can vary significantly based on tactical radios (i.e., not all Type-1 level tactical radios carry the same level of emission security). The emissions testing in chapter IV suggests even LPD classified radio signals are detectable within a certain range and power level. Therefore, what is the level of LPD/LPI a cellular protocol would need to obtain to be considered acceptable? Is it really critical that the signal not be detectable or just not exploited? Even though the cellular signals do not contain the same level of emission security as the tactical radios, they were harder to detect on the cellular handsets (and in some cases not detectable).

Third, flow level traffic prioritization and policing is essential and not normally found in 3G and below cellular base stations. During the throughput testing, the network consistently observed buffer overflows. This was mostly attributed to the LAN traffic flooding the wireless router level devices. In military autonomous, wireless, and ad hoc networks, the flows should be monitored to prevent one application from essentially crashing the link. In most cases the links were not restored until the traffic was reset, suggesting some type of FIFO buffer with the tail end being cut during overflows. How sophisticated should our radios be? Should layer 3 (i.e., within the ISO model) type services be required in military tactical radios? The greater number of services the military requires, the more potential exist for significant delays; however, in some cases the added functionality might be worth the delays (e.g., IntServ to prevent link capacity degradation).

B. Use Cases

If it were possible to establish secure and reliable local cellular networks from our tactical radios, what would be the applied use cases? What new capabilities would this technology bring the Warfighter? This thesis research helps to formulate the following use cases.

Every Marine a Radio

Every Marine, from a combat arms Military Occupational Specialty to a non combat arms, could be issued a cell phone capable of working in garrison and while deployed.

Automated Vehicle Maintenance

All vehicles can be equipped with monitoring equipment. These automated vehicle status reports could be delivered to select personnel via a vehicle maintenance mobile application. This would enable warnings and high priority issues to be highlighted prior to major accidents.

Handheld Intel Collection

Military Intel collection teams currently use pencil and paper or heavy laptop computers. The complex collection process and refinements can be consolidated instantaneously to prevent overlap or inefficient collecting.

Situation Awareness

Ground troops can receive live video feeds from multiple contributing sources (i.e., commanders and small unit leaders can view live footage from a bird's eye view).

Logistic Coordination	Logisticians can coordinate embarking or debarking details with real-time updates.
DDACT Replacement	All cell phones with data services can leverage either an internal or external (client-server scenario) type map data. Marines could replace the current Blue Force tracking system (hardware) with a software download to any phone. Obviously, interoperable software would need to be leveraged on the cellular handset to incorporate the technology.
Coalition Force Intra Communications	These cellular networks could be suitable for coalition force traffic. Therefore, when allies are collocated with US troops we could issue cellular handsets in an effort to maintain critical communication lines.
Sharing of PPLI information	All modern day cellular handsets are equipped with an internal GPS capability (911 mandate). Therefore, if integrated with tactical networks, a command operations center could visually see the physical location of any Marine.

C. Future Work

1. Tethering Concept

This concept was not explored, although it should be evaluated to determine if the idea of directly tethering a cellular handset is feasible after all things are considered. After trial and error testing, the cellular handsets did seem capable of being configured as the host USB device. However, without further testing and developing a proof of concept, this idea still seems open for speculations.

2. Commercial Standard Cellular Networks (4G)

Based on the research conducted in this thesis, modern military tactical radios are capable of hosting cellular (i.e., 3G and below) edge devices without causing degradation of services when users leverage the tactical network for interconnectivity or backhaul communications. Therefore, the 4G technologies should be evaluated in order to identify additional capabilities, capacity, and interoperability.

3. Self-Contained SDR

The research has successfully implemented a COTS cellular protocol (i.e., GSM modified with a PBX backhaul created by OpenBTS) running onboard a desktop computer tethered to a SDR as the RF front-end for broadcasting the signal. The next step is to implement a 3G or higher protocol onboard an independent SDR (i.e., no tethered PC dependency). As with the OpenBTS implementation, an effort to eliminate external dependencies (i.e., BSC, MSC, and HLR type services) should be made to enhance interoperability. The Marine Corps should make an effort to leverage the SDRs similar to the models contained within modern military tactical radios in order to ensure future compatibility.

4. Cellular Protocol Onboard Military Tactical Radio

This concept modifies a cellular protocol (i.e., in software form) and implements the code onboard a modern day relevant military tactical radio. The radio of choice should be a radio already procured by a military service in an effort to prevent unnecessary future acquisition cost and facilitate the reuse of current technology. Since some military radios already contain waveforms developed from cellular protocols (i.e., MUOS), these devices should be evaluated prior to modifying various hardware components required for full integration.

5. Adopt LPD/LPI Characteristics

This research should evaluate adapting current commercial cellular protocols to inherit LPD/LPI characteristics. This will allow cellular handsets and base stations the ability to mask or limit the susceptibility of their emissions. However, this modification could be unrealistic in regards to cost and time. What is the level of skill set required to obtain these qualities? What is the cost of converting the protocol? How long would it take to bring this technology to production?

6. Military APIs

The idea is to research and develop military APIs (cell phone virtual machine and OS libraries), in an effort to prevent vulnerable security calls from either the OS or application (by increasing information assurance characteristics), and to facilitate a portable software architecture. This approach incorporates the evaluation of current security protocols required of military communication devices, the design of a virtual machine capable of hosting, and restricting cellular OSs according to the security policies, and the integration of high priority libraries, whose applications would be required to make OS calls.

7. Handset Frequency Modification

Since the military routinely engages in overseas conflicts, which require specific frequency allocations, cellular handsets should be explored to determine complexity for modifying or adding additional frequency bands. This would enable out-of-band communication for countries without available space within the cellular range. For example, stateside all the frequency allocations are dedicated to commercial providers. When military allied forces operate within our boarders (e.g., coalition training exercises), the US allocates specific military frequencies (i.e., non-commercial bands) for their use. Perhaps, other allied countries have similar scenarios, which require communications to be independent of any specific frequency band. In addition to increasing frequency flexibility, this technology would assist in masking the protocol essentially decreasing the likelihood of being detected (i.e., our adversaries might not look for cellular profiles outside of standards).

8. Software Encryption

The thesis work covered in the previous chapters was unable to evaluate a handheld capable of encrypting the communication at any level. The next step should be to evaluate the commercial industry's handheld security software; specifically, the algorithms, which are categorized under the Suite B classification. Some questions of concern are: (i) what level of security is possible on a generic modern day handheld; (ii) what hardware requirements are required to meet each level of security; (iii) what level of delay is added to the end-to-end communication; (iv) is it possible to encrypt both the circuit switch as well as the packet calls; (v) can the data be encrypted at rest and while transmitting across the network; and (vi) what is the best topology for an encryption scheme (i.e., link, end-to-end, or both).

9. Cost Analysis

All concepts discussed thus far are theoretically possible. However, some might prove infeasible due to high acquisition cost or long development timelines. Therefore, a cost evaluation should be conducted for each concept in order to increase feasibility. The military’s current acquisition cycle requires specific procedures for various reasons. This requirement can increase procurement time and, in some cases, cause project cancellations. Therefore, a timeline and roadmap should be developed with suggestions of multiple courses of action based on technology-feasible assessments.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

Adamy, D. (2001). *EW101: A course in electronic warfare.* Norwood, MA: Artech House.

Apple, Inc. (2009, December). *USB device interface guide.* Retrieved December, 2009, from http://developer.apple.com/mac/library/documentation/DeviceDrivers/Conceptual/USBBook/USBIntro/USBIntro.html

Army CERDEC. (2009, October). *Joint Cell Phone (JCP) project.* Unpublished Powerpoint presentation. Given at Headquarters Marine Corps, Command, Control, Communications, and Computers

Burgess, D. (2009, December). *OpenBTS wifi*. Retrieved December 2009, from http://gnuradio.org/trac/wiki/OpenBTS

Cellcrypt. (2009). *Cellcrypt mobile*. Unpublished Powerpoint presentation. Palo Alto, CA.

Cha, B. (2009, May). *CNET reviews*. Retrieved December, 2009, from http://reviews.cnet.com/best-pdas/

Cisco. (n.d.). *Wireless network router - Cisco systems*. Retrieved March 2010, from http://www.cisco.com

CNSS Glossary Working Group. (2006). *National Information Assurance (IA) Glossary.* (CNSS Instruction No. 4009). Fort Meade, MD: National Security Agency.

Command, M. C. (2010). *Total Force Structure Management System (TFSMS).* Retrieved November 2009, from https://tfsms.mccdc.usmc.mil

Couch, L.W., II. (1990). *Digital and analog communication systems* (3rd ed.). New York, NY: Macmillan Publishing Company.

CTIA - The Wireless Association. (2010, January). *CTIA semi-annual wireless industry survey.* Retrieved (2010, January) from http://www.ctia.org/

Davie, B., & Peterson, L. (2003). *Computer networks: A system approach* (3rd ed.). San Francisco, CA: Morgan Kaufmann.

Department of Defense (DoD). (2009, August 19). *Dictionary of military and associated terms* (Joint Publication 1-02). Washington, DC: DoD.

Department of the Navy Research, Development & Acquisition. (n.d.). *MUOS Mobile User Objective System.* Retrieved January 2010, from https://acquisition.navy.mil/rda/home/programs/information_communications/muos

Ergen, M. (2009). *Mobile broadband: Including WiMAX and LTE.* New York: Springer.

Ericsson. (2009, Febuary). System description QuicLINK R2.1. Unpublished document. (Doc. #221 02-FGC 101 0295 Rev C).

Executive Agent for Theater Joint Tactical Networks (EA-TJTN). (2009). *Joint User Interoperablity Communications Exercise (JUICE) 2009.* Army.

General Dynamics. (2009, December). *General dynamics C4 systems*. Retrieved December 2009, from: http://www.gdc4s.com/content/detail.cfm?item=32640fd9-0213-4330-a742-55106fbaff32

General Dynamics. (n.d.). *Sectera edge smartphone.* Retrieved December 2009, from http://www.gdc4s.com/documents/GD-Sectera_Edge-w.pdf

Google, Inc. (n.d.). *Android FAQ.* Retrieved December 2009, from http://android-dls.com/wiki/index.php?title=Android_FAQ

Halenda, G. (2004, August). *Tactical communication: D-DACT vs. HP iPAQ 5555.* Retrieved August2009, from http://www.popsci.com/scitech/article/2004-08/tactical-communication-d-dact-vs-hp-ipaq-5555

Harris Corporation. (2009). *Harris RF communications*. Retrieved December 2009, from www.rfcomm.harris.com

Harris Corporation. (2009, June). *AN/PRC-150(C) advanced tactical HF radio data sheet*. Retrieved September 2009, from www.rfcomm.harris.com

Harris. (2009, September). *Harris AN/PRC-152 type 1 multiband multimission handheld radio data sheet.* Retrieved September 2009, from www.harris.com

Harris, S. (2008). *CISSP all-in-one exam guide* (4th ed.). Emeryville, CA: McGraw-Hill.

Hewlett Packard. (n.d.). Valuetronics. *Signal Analyzers - Spectrum analyzers, high-performance protable - HP 8560A, 8561B, 8562A, 8563*.

IEEE. (2000). *IEEE 100: The authoritative dictionary of IEEE standards terms* (7th ed.). Standards Information Network IEEE Press.

Information Technology Laboratory. (2002). *Federal information processing standards publication.* Gaithersburg ,MA: National Institute of Standards and Technology.

International Telecommunications Union (ITU). (2008). *ITU world telecommunications / ICT indicators database.* Retrieved January 2010, from www.itu.int

Joint Fires Integration and Interoperability Team. (2009). *Tactical cellular limited operational assessment report.* (LOA tr-09-03), Eglin AFB: United States Joint Forces Command.

Joint Program Executive Office (JPEO) Joint Tactical Radio Systems (JTRS). (2005, August). *JPEO JTRS Overview to OMG.* Retrieved January 2010, from http://jpeojtrs.mil

Joint Special Operations Command (JSOC). (2009). *Memorandum for director, joint systems integration center.* Memorandum. MacDill Air Force Base, FL: JSOC.

Joint Systems Integration Center (JSIC). (2009, September 18). *Tactical cellular.* Powerpoint Presentation. Norfolk,VA: JSIC.

Joint Systems Integration Center (JSIC). (2009). *Teamlinc's potential to enhance tacticell.* Whitepaper. Norfolk,VA: JSIC

Kuhn, R. (2009, October). RDN: A paradigm shift in tactical communications. Whitepaper. LGS Innovations.

Kurose, J. (2008). *Computer networking: A top down approach* (4th ed.). (M. Hirsch, Ed.) Boston, MA: Pearson Addison Wesley.

L-3 Communications. (2009, September 9). *L-3 guardian (SME PED).* Retrieved February 2010, from http://www.l-3com.com/cs-east/ia/smeped/ie_ia_smeped.shtml

LGS Innovations. (2007, January). *Tactical base station router.* Retrieved November 2009, from www.lgsinnovations.com

LGS Innovations. (n.d.). *Rapidly deployable network.* Retrieved January 2009, from www.lgsinnovations.com

Lin, Y.B., & Chlamtac, I. (2001). *Wireless and mobile network architectures.* Wiley Computer Publishing.

National Security Agency (NSA). (n.d.). *NSA suite b cryptography*. Retrieved December 2009, from http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

National Security Agency (NSA). (2009). *NSA recommendations for military use of WMAN technology.* NSA Research Directorate.

Nokia. (2009, September). *Nokia connecting people*. Retrieved December 2009, from www.nokiausa.com

NSTISSP. (2003). *Fact sheet: NSTISSP No. 11, revised fact sheet national information assurance acquisition policy.* National Security Agency, Fort Meade, FL: NSTISSP.

Operator's and Organizational Maintenance Manual-Dismounted Data Automated Communications Terminal (DDACT). (2006, September). *U.S. Marine Corps technical manual (TM 11014A-OR)*.

PCWorld. (2009, June). *PCWorld reviews*. Retrieved December 2009, from http://www.pcworld.com/reviews/product/

Poisel, R. (2004). *Modern communicatoins jamming principles and techniques.* Norwood, MA: Artech House Inc.

Qualcomm. (2005, July). *3G deployable CDMA cellular base station supporting secure voice & data presentation.* Unpublished Powerpoint Presentation.

Sierra Nevada Corporation. (2006). *WiZRD smart phone.* Retrieved January 2010, from http://www.sncorp.com/prod/c4n/wizrd.shtml

Stanley Associates. (2009, July). *Requisition and invoice shipping document*. Charleston, SC.

TerraNet. (2010). *TerraNet AB*. Retrieved March 2010, from www.terranet.se

Thales. (2005, September). *MBITR AN/PRC-148(V)(C) Multiband inter/intra team radio data sheet.* Retrieved January 2010, from www.thalescomminc.com

Thales. (2010, January). *Thales – joint tactical radio system*. Retrieved February 2010, from http://www.thalescomminc.com/jtrs.asp

Turner, M.R. (2006). *Software defined radio solutions "Taking JTRS to the field" with curent and future capabilities*. At *SDR 06 Techical Conference and Product Exposition*, 6.

US Census Bureau. (2009, December). *Population estimates.* Retrieved February 2010, from http://www.census.gov/popest/national/national.html

Wolfe, W. (1998). *Introduction to radiometry.* Bellingham, WA: SPIE Optical Engineering Press.

2003 - 2010 Sponsored Research Topics

Acquisition Management

- Acquiring Combat Capability via Public-Private Partnerships (PPPs)
- BCA: Contractor vs. Organic Growth
- Defense Industry Consolidation
- EU-US Defense Industrial Relationships
- Knowledge Value Added (KVA) + Real Options (RO) Applied to Shipyard Planning Processes
- Managing the Services Supply Chain
- MOSA Contracting Implications
- Portfolio Optimization via KVA + RO
- Private Military Sector
- Software Requirements for OA
- Spiral Development
- Strategy for Defense Acquisition Research
- The Software, Hardware Asset Reuse Enterprise (SHARE) repository

Contract Management

- Commodity Sourcing Strategies
- Contracting Government Procurement Functions
- Contractors in 21st-century Combat Zone
- Joint Contingency Contracting
- Model for Optimizing Contingency Contracting, Planning and Execution
- Navy Contract Writing Guide
- Past Performance in Source Selection
- Strategic Contingency Contracting
- Transforming DoD Contract Closeout
- USAF Energy Savings Performance Contracts
- USAF IT Commodity Council
- USMC Contingency Contracting

Financial Management

- Acquisitions via Leasing: MPS case
- Budget Scoring
- Budgeting for Capabilities-based Planning
- Capital Budgeting for the DoD
- Energy Saving Contracts/DoD Mobile Assets
- Financing DoD Budget via PPPs
- Lessons from Private Sector Capital Budgeting for DoD Acquisition Budgeting Reform
- PPPs and Government Financing
- ROI of Information Warfare Systems
- Special Termination Liability in MDAPs
- Strategic Sourcing
- Transaction Cost Economics (TCE) to Improve Cost Estimates

Human Resources

- Indefinite Reenlistment
- Individual Augmentation
- Learning Management Systems
- Moral Conduct Waivers and First-tem Attrition
- Retention
- The Navy’s Selective Reenlistment Bonus (SRB) Management System
- Tuition Assistance

Logistics Management

- Analysis of LAV Depot Maintenance
- Army LOG MOD
- ASDS Product Support Analysis
- Cold-chain Logistics
- Contractors Supporting Military Operations
- Diffusion/Variability on Vendor Performance Evaluation
- Evolutionary Acquisition
- Lean Six Sigma to Reduce Costs and Improve Readiness

- Naval Aviation Maintenance and Process Improvement (2)
- Optimizing CIWS Lifecycle Support (LCS)
- Outsourcing the Pearl Harbor MK-48 Intermediate Maintenance Activity
- Pallet Management System
- PBL (4)
- Privatization-NOSL/NAWCI
- RFID (6)
- Risk Analysis for Performance-based Logistics
- R-TOC AEGIS Microwave Power Tubes
- Sense-and-Respond Logistics Network
- Strategic Sourcing

Program Management

- Building Collaborative Capacity
- Business Process Reengineering (BPR) for LCS Mission Module Acquisition
- Collaborative IT Tools Leveraging Competence
- Contractor vs. Organic Support
- Knowledge, Responsibilities and Decision Rights in MDAPs
- KVA Applied to AEGIS and SSDS
- Managing the Service Supply Chain
- Measuring Uncertainty in Earned Value
- Organizational Modeling and Simulation
- Public-Private Partnership
- Terminating Your Own Program
- Utilizing Collaborative and Three-dimensional Imaging Technology

A complete listing and electronic copies of published research are available on our website: www.acquisitionresearch.org

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944; Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School, Monterey, CA 93943-5100

3. Research Office, Code 09 1
   Naval Postgraduate School, Monterey, CA 93943-5138

4. William R. Gates 1
   Dean, GSBPP
   Naval Postgraduate School, Monterey, CA 93943

5. Stephen Mehay 1
   Associate Dean for Research, GB
   Naval Postgraduate School, Monterey, CA 93943

6. Joshua S. Dixon 1
   Capt., USMC, GB
   Naval Postgraduate School, Monterey, CA 93943

7. Rick Wolf 1
   I MEF Training & Experimentation Group(TEG), Camp Pendleton, CA

8. Zach Loban 1
   MCSC, PG12, Quantico, VA

9. James Robinson 1
   HQMC, C4, Quantico, VA

10. Federico Bermudez 1
    Joint Systems Integration Center, Parkway, Suffolk, VA

11. Geoffrey Xie 1
    Naval Postgraduate School, Monterey, CA 93943

12. Frank Kragh 1
    Naval Postgraduate School, Monterey, CA 93943

13. Donna Miller 1
    Naval Postgraduate School, Monterey, CA 93943

14. John Gibson 1
    Naval Postgraduate School, Monterey, CA 93943

15.	John Armantrout JPEO JTRS, San Diego, CA	1
16.	James Neushul I MEF, G6, Camp Pendleton, CA	1
17.	Lawrence Troffer MCTSSA, Camp Pendleton, CA	1

Copies of the Acquisition Sponsored Research Reports may be printed from our website: www.acquisitionresearch.org

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CALIFORNIA 93943

www.acquisitionresearch.org