2016-06

A feasibility assessment of 6LoWPAN for secure communications in the U.S. Army

Stephens, Alan L.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A FEASIBILITY ASSESSMENT OF 6LOWPAN FOR SECURE COMMUNICATIONS IN THE U.S. ARMY

by

Alan L. Stephens

June 2016

Thesis Advisor: Gregory Miller
Co-Advisor: Preetha Thulasiraman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE A FEASIBILITY ASSESSMENT OF 6LOWPAN FOR SECURE COMMUNICATIONS IN THE U.S. ARMY			**5. FUNDING NUMBERS**
6. AUTHOR(S) Alan L. Stephens			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis uses systems engineering techniques to assess the feasibility for the United States Army to use IPv6 securely over an IEEE standard 802.15.4 (6LoWPAN) network in both an operational and a support role. The methods used include assessing the limitations and security mechanisms of 6LoWPAN, assessing wireless security concerns, small battery capacity and duration, and the remaining potential for use in both environments. The same model could apply to other protocols or capabilities given operational requirements. Expected operational situations aid in identification of requirements. The two operational scenarios examined in this thesis indicate 6LoWPAN could provide value and meet technical requirements in a support environment such as a combat hospital, but analysis of a tactical situation such as replacing an AN/PRC-154A radio for Nett Warrior backhaul indicates its implementation would be problematic. Specifically, in the generalized tactical role, 6LoWPAN devices with a standard AAA rechargeable battery exhibit a lifetime of 11.7 hours or 15.3 hours with a standard AA rechargeable battery and 2.45-inch device length transmitting at -2 dBm. The required encryption standards and layered protocol stack headers result in message payload limits, the worst-case being 45 bytes of data. Reliable voice communications are not feasible over 6LoWPAN's limited bandwidth.

14. SUBJECT TERMS LoWPAN, 6LoWPAN, 802.15.4, energy, security, feasibility, wireless, networks, range, duration, wireless security, BFT, systems engineering, requirements, Army			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A FEASIBILITY ASSESSMENT OF 6LOWPAN FOR SECURE COMMUNICATIONS IN THE U.S. ARMY

Alan L. Stephens
Major, United States Army
B.S., University of Alabama, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2016

Approved by: Gregory Miller
Thesis Advisor

Preetha Thulasiraman
Co-Advisor

Ronald Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis uses systems engineering techniques to assess the feasibility for the United States Army to use IPv6 securely over an IEEE standard 802.15.4 (6LoWPAN) network in both an operational and a support role. The methods used include assessing the limitations and security mechanisms of 6LoWPAN, assessing wireless security concerns, small battery capacity and duration, and the remaining potential for use in both environments. The same model could apply to other protocols or capabilities given operational requirements. Expected operational situations aid in identification of requirements. The two operational scenarios examined in this thesis indicate 6LoWPAN could provide value and meet technical requirements in a support environment such as a combat hospital, but analysis of a tactical situation such as replacing an AN/PRC-154A radio for Nett Warrior backhaul indicates its implementation would be problematic. Specifically, in the generalized tactical role, 6LoWPAN devices with a standard AAA rechargeable battery exhibit a lifetime of 11.7 hours or 15.3 hours with a standard AA rechargeable battery and 2.45-inch device length transmitting at -2 dBm. The required encryption standards and layered protocol stack headers result in message payload limits, the worst-case being 45 bytes of data. Reliable voice communications are not feasible over 6LoWPAN's limited bandwidth.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

6LoWPAN	Internet protocol version 6 over LoWPAN
ACK	acknowledgement message
AES	advanced encryption scheme
AH	authentication header
ARP	address resolution protocol
AT&L	Acquisition, Technology, and Logistics
BFT	Blue Force Tracking
bps/kbps	bits per second/ kilobits per second
BPSK	binary phase-shift keying
CAP	contention access protocol
CAS	close air support
CBC-MAC	cyber block chaining messaging authentication code
CCM	CBC-MAC
CCP	casualty collection point
CIO	Chief Information Office
CSH	combat support hospital
CSMA-CA	carrier sense multiple access with collision avoidance
codec	compressor-decompressor
COTS	commercial-off-the-shelf
dB	decibels
dBW	decibel watt
dBm	decibel milliwatt
DAGR	defense advanced GPS receiver
DHCP	dynamic host configuration protocol
DIACAP	DOD Information Assurance Certification & Accreditation Process
DLL	data link layer
DOD	Department of Defense
FFD	full function device
GPS	global positioning system
GTS	guaranteed time slot
HVT	high-value target

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet engineering task force
IP	Internet protocol
IPSec	Internet protocol security
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IRAD	internal research and development
JBC	joint battle command
KEYMAT	keying material
LCC	life-cycle costs
LoWPAN	low-power wireless personal area network
mW	milliwatt
MAC	medium access control
MAC	message authentication code
MANET	mobile ad-hoc network
MGRS	military grid reference system
MTU	maximum transmission unit
O-QPSK	offset quadrature pulse-shift keying
OSD	Office of the Secretary of Defense
PAN	personal area network
PL	platoon leader
PSG	platoon sergeant
QoS	quality of service
RFC	request for comment
RFD	restricted function device
RFID	radio frequency identification
RTLS	real-time location system
TCP	transfer control protocol
UAV	unmanned aerial vehicle
UDP	user datagram protocol
W	watt
WPAN	wireless personal area network

EXECUTIVE SUMMARY

This thesis uses systems engineering techniques to assess the feasibility of the United States (U.S.) Army securely using IPv6 over an IEEE standard 802.15.4 (6LoWPAN) network. The Internet of Things (IoT) offers connectivity to previously isolated devices needing to pass only small amounts of information. Current trends to maximize transmission speeds and data throughput pay little concern to energy. This thesis presents a model that assesses 6LoWPAN in both a potential operational role as a Blue Force Tracker (BFT) backhaul and a potential support role as connecting a combat support hospital (CSH) as a smart building. Examination of the two scenarios indicate 6LoWPAN could provide value and meet technical requirements in a support environment, but analysis of a tactical situation such as replacing a AN/PRC-154A radio for BFT backhaul within the Nett Warrior system indicates its implementation would be problematic. Specifically, in the tactical role, 6LoWPAN devices with one standard AA rechargeable NiMH AA battery, a small dipole antenna only 0.45 inches longer than the battery, and processing capability draining power at 5 nJ/bit send team member position updates every 10 seconds at spacing intervals up to 300 meters apart to the team leader. Under this specific requirement, each team member device lasts over 15.3 hours. The limitation of battery device size and NSA type I encryption standards result in messages limited to 45 bytes of data. The range limitations of 6LoWPAN and narrow messaging capability get exchanged for extremely low SWAP amounts.

The thesis initially examines the IoT as well as the genesis of the study and background. The Army user community, as any entity, arguably gravitates toward high bandwidth, high-powered devices to accomplish tasks in an increasingly complex network environment. In contrast, the Soldier on the battlefield prefers the lightest weight solution meeting the requirements. The IoT concept embraces network connectivity of every day, isolated electronic objects for two-way data communications using extremely low power with the intent of extending duration. This thesis first analyzes feasibility leveraging the benefits of IPv6 functionality over a lower size, weight, and power (SWAP) solution to still meet current user requirements.

This thesis then explores the capabilities and options available by using 6LoWPAN. Decrements made at each protocol stack layer translate to headers required to achieve user requirements and remaining payload space. Standards for each protocol stack layer define required header contents and allow a capability assessment of each option. Each selected option determines remaining packet size in octets that defines application layer payload minimum and maximum limits. First, the physical layer offers topology options and node identification protocols. The data link layer offers security alternatives of 6LoWPAN. Each option yields varying message security levels to meet U.S. Army requirements. The network layer determines routing protocols in lieu of a full 40-byte IPv6 header that would diminish remaining payload space. The transport layer determines how the messages move through the network and whether or not two-way communications require receipt acknowledgments. Finally, any remaining payload can carry data traffic. The most streamlined scenario leaves 87 octets for application layer use while even the most robust leaves 45 octets for application layer use.

Systems engineering approaches develop user requirements for an operational BFT scenario and a less volatile equipment-tracking scenario in an Army CSH. User requirements for throughput, frequency of position update, maximization of device duration, and minimization of device size define feasibility space of an assessment or design space for development. Subsequently, each user requirement gets measured against 6LoWPAN capabilities and constraints. Various device sizes and associated dipole antenna lengths, throughput constraints, multiple transmission powers, specified receiver sensitivity, encryption, and resiliency all translate into measures of success. A holistic view of the set of measures determines 6LoWPAN's feasibility for secure Army use.

As a result, the Army and other services should investigate use of 6LoWPAN in environments with limited energy and low throughput requirements. Specific areas for future research and application of the study to similar areas for analysis include defining logical interfaces with existing or necessary capability, measuring sufficiency of performance from a user perspective, material enhancements to increase SWAP savings, and application of this model to additional use cases.

I. INTRODUCTION

A. BACKGROUND

The Internet of Things (IoT) embraces network connectivity of everyday, non-computer objects for two-way data communications. The IoT concept offers potential to extend connectivity to devices and mobile nodes at the tactical edge of the battlefield at low cost. Size, weight, and power (SWAP) provide strong metrics for measuring consumer cost. The individual Soldier positioned at the last tactical mile places a premium on minimizing SWAP. Likewise, asset location tools enable leaders to assess quickly and reallocate personnel and resources to the right place and time. Internet Protocol version 6 (IPv6) over a low-power wireless personal area network (LoWPAN), defined by the Institute of Electrical and Electronic Engineers (IEEE) as 802.15.4, is often referred to as 6LoWPAN. The IEEE 802.15.4 standard specifies physical layer and media access control layer (MAC) for LoWPANs, focusing on low-cost, low-speed, and low-power communication. IPv6 adds the upper layer protocols enabling the network and transport protocols. 6LoWPAN commonly encapsulates the combination of IPv6 over an 802.15.4 network. Shadowed by ever-increasing bandwidth and range capable devices, this often-overlooked protocol offers a relatively small SWAP footprint position location capability to the United States Army.

The leaders of today's Soldiers risk sensory overload from informational displays while simultaneously deciphering friend or foe in an often-asymmetric environment. The information presented to the Soldiers may require fusion or processing before becoming actionable, or even useful, intelligence. One tool requiring little to no individual processing, quickly locating friendly forces on the battlefield, is blue-force tracking (BFT). While maintaining locational awareness of friendly forces in a dismounted operation often occurs through line of sight (LOS) or verbal passing of information within a small fire-team or squad sub-section, supporting elements or higher echelons may be left only approximating individual Soldier locations. The U.S. Army's dismounted BFT system, Nett Warrior, named after WWII Medal of Honor recipient, Colonel Robert B. Nett, allows users to see their own location, location of other users,

and locations of the enemy on a moving map (Lopez 2010). The Nett Warrior system being fielded today currently offers the location of the system users (Dawson 2015). Additionally, current initiatives aim to reduce the weight burden, often surpassing 100 pounds, on Soldiers while maintaining or enhancing current operating capabilities (Friedl and Santee 2011). Using 6LoWPAN is a potential solution to increasing awareness of individual Soldier positions while incurring negligible weight increase to the Soldier's payload.

IEEE 802.15.4 networks operate on different frequency ranges depending on modulation schemes and location. Additionally, some of the frequencies are reserved for industrial, scientific, and medical (ISM) uses and authorization for use hinges upon accepting interference from licensed users and not interfering with those licensed users. (Federal Communications Commission 2016). Regulatory bodies in China, Japan, Europe and the United States set allowed frequency ranges and channel allocations (IEEE 2011). Current commercial uses of 802.15.4 physical networks include interior lighting control, audio and video control, thermostat control, interactive toys, smart badges, or multiple home monitoring systems. Industry also finds utility in 802.15.4 networks for remote sensor and actuator control in monitoring or automation processes (Toscano and Bello 2012). Even location detection of critical equipment by means other than radio-frequency identification (RFID) is possible, though not ideal, for 802.15.4 networks. These networks require augmenting upper layer protocol to perform self-computed range detection (Wheeler 2007).

IPv6 also accelerates router processing using an improved option mechanism and configures addresses dynamically, if necessary. Addressing with IPv6 protocol increases flexibility by increasing the number of address layers. Specifically, IPv6 is built to multi-cast messages (i.e., sending messages to a specifically tailored audience), without current limitations currently seen in IPv4. IPv6's additional fields even allow users to tailor parts of a packet for special handling (Stallings 2014). IP Security (IPSec) also increases with IPv6, inherently offering embedded features preventing many, though not all, attacks common to wireless sensor networks (WSNs).

This thesis studies 6LoWPAN as an available capability, rather than a tangible material solution, to fit currently unspecified requirements. Within the defense industry, many specific solutions exist in search of requirements to the benefit of the contractor that funds such projects with internal research and development (IRAD) dollars. 6LoWPAN, however, is a concept apart from specific hardware, and this thesis assesses the feasibility of further research upon evaluating the security and operability against presumed requirements derived through systems engineering techniques.

B. POTENTIAL BENEFITS

The IoT concept comprises the future of all machines, all appliances, and all digital "things" being assigned an IP address. Possessing an IP address allows the potential for communication capability with the rest of the World Wide Web. Existing routing and security protocols allow tremendous potential for military application. Potential uses of assigning IP addresses to "things" include secure two-way communications capable of securing sensor-specific information. Two-way traffic allows sensors to receive secure keying material (KEYMAT) or even data input should the node possess onboard storage capacity.

LoWPANs offer a less costly, more energy efficient, scalable alterative to mesh networking in applications not demanding high-throughput or high-definition video. Energy efficiency translates directly to lessened weight on the Soldier and less platform or facility waste. Furthermore, properly allocating communication periodicity extends battery life and increases overall system value. Before the Internet Engineering Task Force (IETF) released standards on 6LoWPAN, an alliance of companies seeing a need for a LoWPAN routing protocol formed the Zigbee Alliance that built upon the IEEE defined 802.15.4 standard. Today, the Zigbee Alliance standard, specifically designed for 802.15.4 networks, accomplishes similar functions of IPv6 though the two standards are incompatible. Still other standards have been and can be developed to route traffic over the IEEE 802.15.4 standard. IPv6 offers the most widely known and community-supported standard allowing more rapid implementation within a modularized acquisition or system integration.

C. GOALS AND OBJECTIVES

This thesis uses systems engineering techniques to explore the security and feasibility of using 6LoWPAN in an operational as well as a support setting. Applications of 6LoWPAN include, but are not limited to, those previously mentioned.

Research questions to help determine the feasibility of 6LoWPAN for Army usage include:

1. How might the Army employ 6LoWPAN?
    a. Why would the Army want 6LoWPAN?
    b. What are the limitations of 6LoWPAN?
    c. Where would 6LoWPAN interface current capabilities?
2. How secure is 6LoWPAN for operational or support use?
    a. What security options are available to 6LoWPAN?
    b. What security mechanisms are most important to the Army?
    c. How well can 6LoWPAN defend against common attacks?
3. How well can 6LoWPAN support required operations? What is the maximum expected performance in terms of range, duration, and throughput?
4. What would 6LoWPAN cost the Army, in terms of SWAP, to employ 6LoWPAN?
5. Is further exploration of 6LoWPAN for Army use worthwhile?

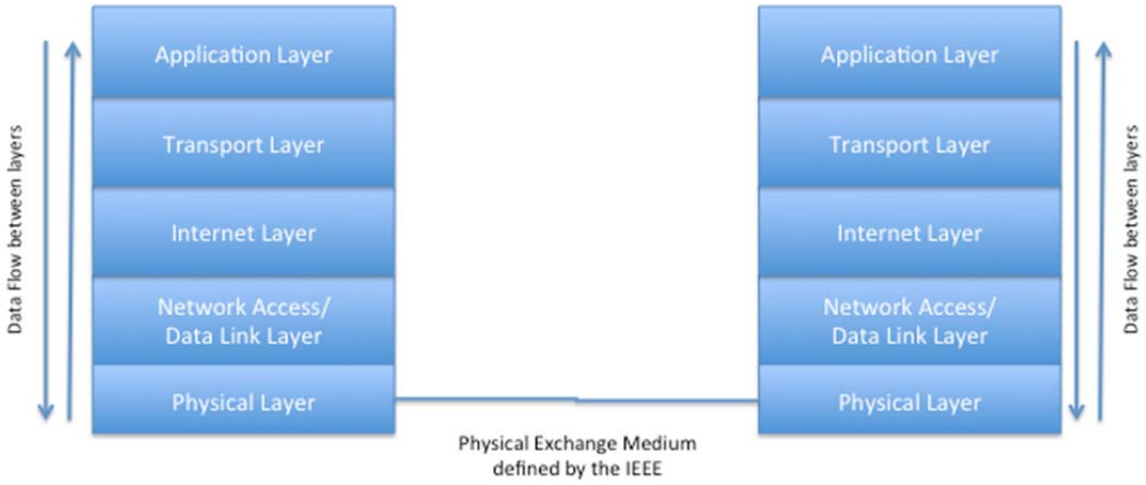
D. METHODOLOGY

Methodology for this thesis will use systems engineering techniques to determine the feasibility of 6LoWPAN for two generic Army use cases. An exploration of the problem space through user perspectives, potential threats, and operational concepts culminating in an operational scenario help shape the operational requirements. Combined with defined system boundaries and functional analysis, a complete list of requirements develops the framework with which to measure feasibility. Lastly, analysis of expected system performance against defined requirements determines feasibility.

II. 6LOWPAN OVERVIEW

A. INTERNET PROTOCOL VERSION 6

Transmitting data over an IEEE 802.15.4 network requires protocol standards above the data link layer (DLL). This thesis specifically analyzes use of IPv6 due to the widespread adoption and accepted standards worldwide. IEEE only specifies the standards at and below the DLL due to the variety of networking options able to sit atop the physical layers. The IETF, initiators of IPv6, exists to make the Internet work better and to improve Internet-based communications through standardization (Alvestrand 2004). Other entities, perhaps lesser known or specifically designed for a sub-network, specify alternative protocols usable at any level peer-to-peer communications occur. Organizations similar to the IETF may also develop routing protocols that sit atop the Data Link Layer (DLL) as depicted in Figure 1.



Large collections of protocols used by the Internet Activities Board (IAB) define the TCP/IP Protocol Suites. Standardized protocol allows peer-to-peer communication.

Figure 1. TCP/IP Protocol Suite. Source: Stallings (2014).

The Zigbee Alliance, almost synonymous with 6LoWPAN, claims to provide the only open, global wireless standard that provides foundation to the Internet of Things. The Zigbee Alliance consists of approximately 450 member companies, purportedly non-

profit, specifically developing products complying to an agreed-upon standard established prior to the release of the 6LoWPAN working group's first requests for comment (RFC), 4919 and 4944, both released in 2007 (Montenegro et al. 2007; Kushalnagar, Montenegro, and Schumacher 2007). The two protocols, 6LoWPAN and Zigbee, accomplish practically identical tasks but 6LoWPAN offers versatility of readily running on other physical layer mediums. Bridging a gap between non-Zigbee and Zigbee compliant devices requires a more complex gateway application than 6LoWPAN (Sarto 2016). This thesis does not explore the nuanced advantages or disadvantages between Zigbee and 6LoWPAN but uses 6LoWPAN as the study case due to proclivity of information and interoperability on mediums beyond IEEE 802.15.4 networks.

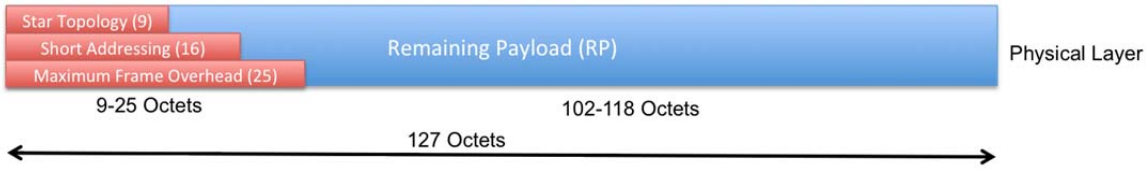
B. PACKET ARCHITECTURE

IEEE 802.15.4 networks have a single packet maximum transmission unit (MTU) constraint of 127 octets, or bytes (Montenegro et al. 2007). Constraints dictate design space, thus, the 127-octet limit of a single packet forces fragmentation of messages exceeding the single frame payload size (Montenegro et al. 2007). 6LoWPAN networks, although capable of multi-frame transmissions, expect one-frame, or packet, transmissions that minimize excessive headers required to fragment and reassemble the original message (Kushalnagar, Montenegro, and Schumacher 2007). Additionally, because IPv6 requires assembly of packets below the network layer, multiple frame packets could prove too much for devices with little memory or processing capacity to reassemble (Kushalnagar, Montenegro, and Schumacher 2007). However, depending on the selected application of 6LoWPAN, dropped packets may be inconsequential assuming most packets arrive at the intended destination. Specific operational requirements must dictate the quality of service (QoS) that is technically required. Within the TCP/IP Protocol Suite, each protocol layer further restricts the amount of payload available to the next higher layer.

1. Physical Layer

The 127 bytes in the IEEE 802.15.4 packet includes a 25-byte header in addition to the payload. The 25-byte header includes information such as a preamble and delimiter

that enable receiving nodes to synchronize with the bit stream, frame control sequence number, frame length, source and destination MAC addresses, and others. NXP Laboratories demonstrated short addressing in a mesh network by reducing the physical layer header to 16 bytes and reducing a network in a star topolgy to only nine bytes as shown in Figure 2 (NXP Laboratories 2013). The compression of this field, or any other, is not the direct focus of this work but demonstrates parameters allowable for analysis.



The physical layer header compression options can leave as much as 118 octets for remaining payload space.

Figure 2. Physical Layer Compression Options.

2. Data Link Layer

Encryption lies within the upper sub-level of the DLL, the logical link control sub-layer (LLC), that sits atop the medium access control (MAC) sub-layer. The Advanced Encryption Standard (AES) demonstrates a viable security layer in an 802.15.4 network and is specified in the RFC 4919 (Kushalnagar, Montenegro, and Schumacher 2007). The 128-bit advanced encryption standard, AES-128, exists in IPSec by default. A common augmentation of AES includes cipher block chaining message authentication code (CBC-MAC). Incorporating an additional counter to the CBC-MAC (CCM) ensures uniqueness of every MAC. Networks commonly use AES-CCM with various bit block sizes ranging from 32 to 256. The keying material, KEYMAT, request for each AES-CCM-128 requires 21 octets as specified by RFC 4944 (Montenegro, Kushalnagar, Nandakishore, Hui, and Culler 2007). RFCs pertaining to 6LoWPAN do not specify octet requirements for 256-bit encryption. AES-CCM creates randomly generated initialization vectors, IV, at the sources, unique to each transmission preventing replay attacks (Hersent, Boswarthick, and Elloumi 2012; Housley 2005). Encryption, regardless of selected size, requires four bytes for frame counting and one byte for key counting. This

increases the header by five bytes, or octets (Sastry and Wagner 2004). The RFC 4944 indicates that dividing the encryption bit key size by eight and adding five administrative bytes, equates to a theoretical header demand of 37 octets for AES-CCM-256 bit key encryption, 29 octets for AES-CCM-192, and 21 octets for AES-CCM-128. Figure 3 demonstrates the header required for each level of encryption and the corresponding remaining payload and results in answering the research question of what security options are available to 6LoWPAN.

The military requires use of AES-CCM-256, a NSA Type I encryption standard, for transmitting traffic up to top secret (National Security Agency 2015). However, the National Institute of Standards and Technology (NIST) further clarifies AES-CCM-128 acceptable to transmit sensitive but unclassified government information (Barker and Roginsky 2015). A requirement to pass top secret information leaves only 65 bytes of the 102 bytes on an 802.15.4 network available for upper layer usage. The most current 6LoWPAN RFC detailing AES specifies only as high as AES-CCM-128 encryption. The operational security requirements using 6LoWPAN will be discussed later in this chapter but the brief exploration of requirements addresses security mechanisms most important to the Army.

The DLL could have increasing bit counts to enhance protection. AES-CCMs-192 and 256 are not specified by any standard for 6LoWPAN. If implementing AES-CCM-192 or 256, payload space begins to lessen for higher-level protocols.

Figure 3. Data Link Layer Security Options.

3. Network Layer

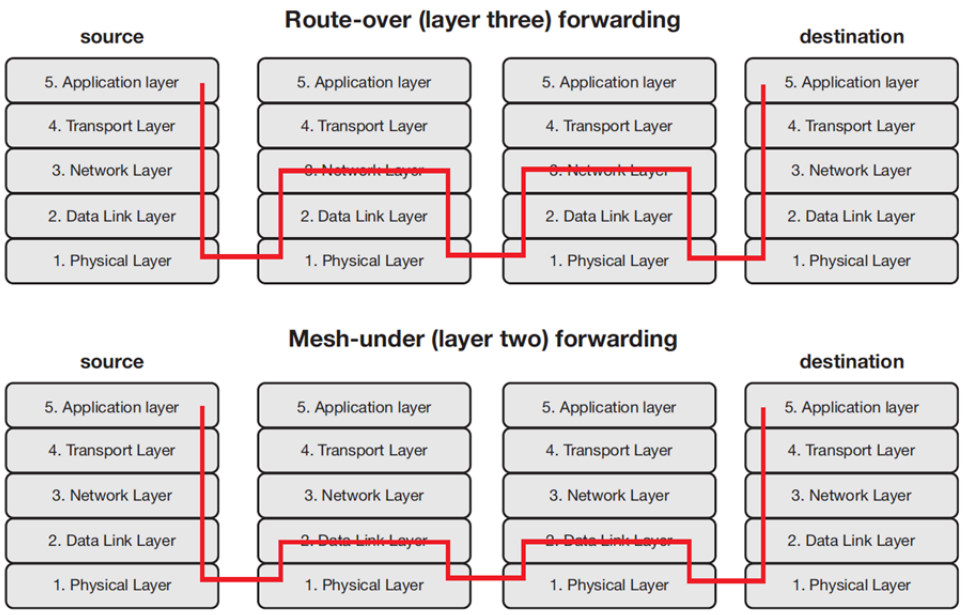
Above the DLL lies the network layer, specifically IPv6 in 6LoWPANs. In a general sense, IPv6 standardization of packet header size to 40 bytes eases the burden on inter-routing processing as compared to IPv4 header sizes that vary between 20 and 40 bytes, depending on options. Additionally, IPv6 limits the size of a single packet per transmission, or MTU, to 1280 octets (Kushalnagar, Montenegro, and Schumacher 2007). However, a MTU of 1280 octets assumes no lower layer constraints. The IEEE 802.15.4 MTU constraint of 127 octets presents a notable problem of not leaving much room for payload unless compressed. Therefore, an adaptation layer specific to 6LoWPANs manages compression as well as fragmentation and reassembly, if necessary, and resides just above the DLL and manages interaction with the IPv6 networking layer. An IPv6 header used over an 802.15.4 network can compress from 40 octets to as low as two octets if link-local (link-local presumes no need of full IP addressing due to remaining under a common router), as depicted in Table 1, or twelve octets if the network implements hopping (Hui and Thubert 2011). Compression of the IPv6 header eliminates unnecessary information for a network under specific assumptions. For instance, assuming the entire network communicates using IPv6 and if the traffic class and flow label fields are zeroed out, then the 32 bits that would be required to present this information is reduced to one bit. This is shown in the first three rows of Table 1. The same table also shows the payload length derived from the message authentication code (MAC) eliminates 16 additional bits. Most significantly, the source and destination addresses reduce from 128 bits each to two bits each assuming the network is link-local. A message expected to take multiple IP hops requires an additional five bytes. Table 1 compares the differences in an uncompressed IPv6 header and a fully compressed IPv6 header set for link-local communications (Ee, Ng, Nordin, and Borhanuddin 2010).

Table 1. IPv6 Header Compression Characteristics. Source: Ee et al. (2010).

Header Field	IPv6 header length	6LoWPAN HC1 length	Explanation
Version	4 bits	--	Assuming communicating with IPv6
Traffic class	8 bits	1 bit	0 = Not compressed. The field is in full size 1 = Compressed. The traffic class and flow label are both zero.
Flow label	20 bits		
Payload length	16 bits	--	Can be derived from MAC frame length or adaptation layer datagram size (6LoWPAN fragmentation header).
Next header	8 bits	2 bits	Compressed whenever the packet uses UDP, TCP or Internet Control Message Protocol version 6 (ICMPv6).
Hop limit	8 bits	8 bits	The only field that never compresses.
Source address	128 bits	2 bits	If both source and destination IPv6 addresses are in link local, their 64-bit network prefixes are compressed into a single bit each with a value of one. Another single bit is set to one to indicate that 64-bit interface identifier are elided if the destination can derive them from the corresponding link-layer address in the link-layer frame or mesh addressing header when routing in a mesh.
Destination address	128 bits	2 bits	
HC2 encoding	--	1 bit	Another compression scheme follows a HC1 header.
Total	40 bytes	2 bytes	Fully compressed, the HC1 encoding reduces the IPv6 header to two bytes.

The IPv6 header can be significantly reduced under the above assumptions.

The Network Layer specifically directs the datagram, or packet, to the right place in time. Figure 4 depicts two methodologies for traffic forwarding in 6LoWPAN. Mesh-under forwarding refers to link-local communications, requiring only two total bytes of IPv6 header, and Route-over forwarding refers to communications passing over a router. The latter methodology requires 12 bytes of IPv6 header (Ee et al. 2010; Olsson 2014).



Traffic over a 6LoWPAN can capitalize on interoperability with mediums beyond the 802.15.4 radios by routing via IP addresses, costing 7 bytes of Network layer header, or remain within a network by not passing through a router, costing only 2 bytes of network layer header.

Figure 4. Routing Options of 6LoWPAN. Source: Olsson (2014).

6LoWPAN messages remaining uncompressed require 40 bytes of network layer header. This is impractical size necessitates compression for a 6LoWPAN network. Figure 5 illustrates the compression options and header lengths required for each traffic-forwarding option. However, fragmentation provides an option for larger messages but increases security risks and likelihood of incomplete message traffic. Additionally, fragmenting requires an additional four bytes for the initial fragment and five bytes for additional fragments of a message (Ee et al. 2010). The network layer payload and header nominally become encapsulated within the DLL's encryption unless otherwise specified.

Link-local communications need only 2 bytes of network layer header; those requiring IP hops over routers require a 12-byte header. An uncompressed header requires 40 bytes and is, therefore, never used for 6LoWPAN.

Figure 5. Network Layer Options.

4. Transport Layer

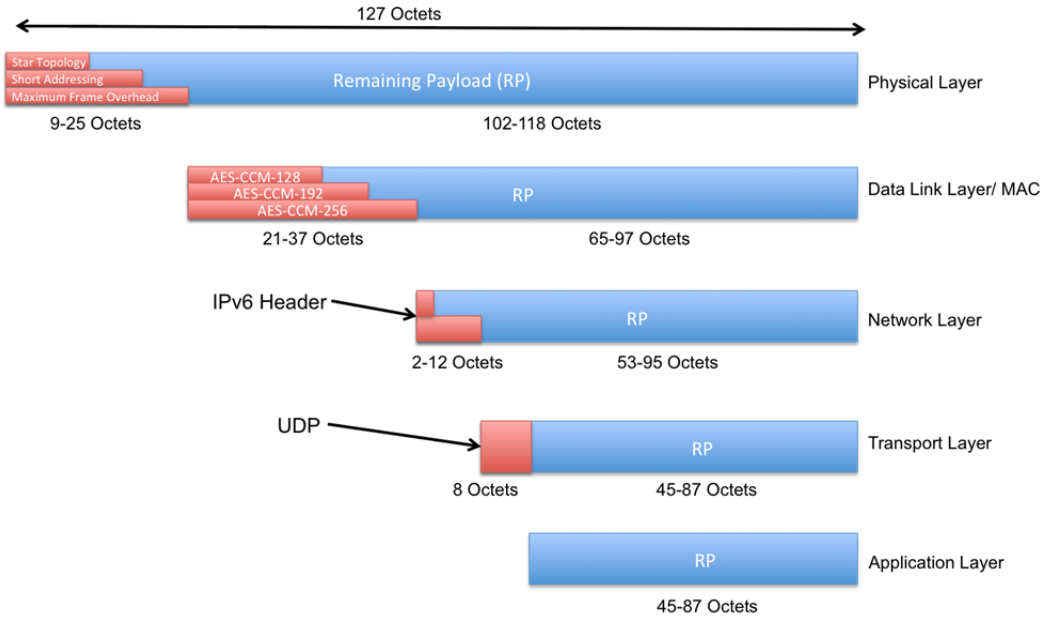
The transport layer rides atop the networking layer and controls the handling of the datagram message. User datagram protocol (UDP) is a connection-less link between source and destination requiring no confirmation of receipt. Conversely, transmission control protocol (TCP) is a connection-oriented link that controls and confirms packet delivery. A network running TCP experiences heightened traffic demands due to control messages transiting the network back-and-forth between source and destination. This behavior opens networks, specifically wireless networks, to denial of service attacks due to packets requiring extensive exchanges before sending any traffic. Networks running UDP, however, behave more like a fire-and-forget method, reducing the transport layer header length but never receiving message receipt acknowledgement. Accordingly, UDP's lessened header length requirement makes it the prescribed transport layer protocol for 6LoWPANs. Figure 6 depicts the UDP header requirement and the remaining payload space.

UDP requires less header length but cannot provide receipt confirmation as TCP may. TCP requires a 20-byte header and significantly increases utilization sometimes associated with line congestion. Therefore, UDP is the prescribed protocol for 6LoWPAN.

Figure 6. Transport Layer Options.

5. Application Layer

Application layer data remains flexible as a user-specific demand requirement. This work focuses on the feasible amount of space remaining for user-specific application data with best guess estimates of constantly changing application requirements. Simply stated, a mesh-under network using a star topology using AES-CCM-128 physical security and UDP transport protocol leaves as much as 87 octets per transmission for application use. Conversely, a more robust route-over network using a mesh topology, AES-CCM-256 physical security and UDP transport protocol leaves only 45 octets per transmission for application use. Figure 7 illustrates the full range of viable options.



The most streamlined scenario leaves 87 octets for application layer use while even the most robust leaves 45 octets for application layer use. Note that all overhead shows as headers but may also include any associated trailers.

Figure 7. Range of Layered Options and Resultant Remaining Payload (RP).

C. PHYSICAL PERFORMANCE CHARACTERISTICS

Networks, specifically wireless networks such as 6LoWPAN, inextricably link range, throughput, power, and security. Range depends on the amount of power transmitted across the system among many other factors. The power requirements depend on the amount of transmissions, amount of processing, length of transmissions, and internal loss factors. Throughput, or network utilization, depends on the frequency selection, the range of each transmission, the bit error rate (BER) and required header length. As stated above, each protocol option of the TCP/IP stack drives the header length required for each transmission, driving the payload throughput, and power requirements. The following section explains the derivation of 6LoWPAN's system limitations.

1. Range

IEEE 802.15.4 radios, at the physical layer, largely determine range of 6LoWPANs, unless multi-hopping. Without multi-hopping, 802.15.4 radios normally range only tens of meters due to range decreasing in free space according to Friis free space equation, Equation 2.1 (Rappaport 2002).

$$d_{\max} = \sqrt{\frac{P_{Tx} G_t G_r \lambda^2}{(4\pi)^2 (P_{Rx}) NF}} \tag{2.1}$$

Antenna gain in the transmitting antenna, G_t, and the receiving antenna, G_r, the wavelength in meters, λ, the minimum power a receiver antenna must receive, P_{Rx}, and the system loss factor, NF, all contribute to the maximum allowable separation distance, d_{max}, for successful communications. Additionally, this estimation neglects interfering signals or atmospheric attenuation due to the relatively short distances achievable by this IEEE standardized radio system. The IEEE 802.15.4 specification provides conditions for receiver sensitivity in Table 2.

Table 2. Receiver Sensitivity Conditions. Source: IEEE (2011).

Term	Definition of term	Conditions
Packet Error Rate (PER)	Average fraction of transmitted packets that are not correctly received.	Average measured over random physical service data unit (PSDU)
Receiver sensitivity	Lowest input power for which the PER conditions are met.	1) PSDU length of 20 octets 2) PER < 1% 3) Power measured at antenna terminals 4) Interference not present

The PER and bit error rate (BER) are assumed synonymous for the purposes of this analysis.

IEEE 802.15.4 radios, as defined by IEEE standard, operate in various modulation schemes at each allocated frequency. The throughput, measured in bits per second (bps) depends on the modulation scheme selected. While there are multiple modulation options, the higher end of the throughput, the 2.4 GHz range, requires offset-quadrature phase shift keying (O-QPSK) allowing throughput of 250 kbps while lower frequency O-QPSK options afford only 100 kbps. Frequency bands around 915 MHz or 868 MHz, offer throughputs of only 40 kbps or 20 kbps, respectively, by using binary phase-shift keying (BPSK). The same frequency bands may also use O-QPSK, resulting in theoretical throughputs up to 100 kbps. Additionally, lower frequencies using BPSK require more stringent channel accuracy and higher receiver sensitivity as shown in Table 3.

Table 3. Frequency Allocations of Most Common Modulation Schemes and Associated Throughput. Adapted from IEEE (2011).

Frequency Range (MHz)	Modula-tion	Throughput (kbps)	Channels		Trans-mitted Power	Receiver Sensitivity	Authorized Region
779 - 787	O-QPSK MPSK	250 250	7		-3 dBm<	-85 dBm	China
868–868.6	BPSK ASK O-QPSK	20 250 100	1		-3 dBm<	-92 dBm -85 dBm	Europe
902–928	BPSK ASK	40 250	10			-92 dBm	North America
950–956	GFSK BPSK	100 20	21	0-7 BPSK	1 dBm <	-92 dBm	Japan
				8-9 BPSK	10 dBm <		
				10-21 GFSK			
2400–2483.5	O-QPSK	250	16		-3 dBm <	-85 dBm	Worldwide

IEEE 802.15.4 radio transmission power capability must exceed -3 dBm but frequency allocation requirements may further limit maximum power output (IEEE 2011). Though the IEEE standard assumes a negligible antenna gain, or a unity value, actual radio construction will result in a realized gain. Assuming a dipole antenna construction, as an example, derived equations that roughly approximate dipole antenna gain to an easily calculable value (Equation 2.2) such that d is the full length of the receiving antenna, assumed to be the device diameter for extremely small 802.15.4 radios as an assumption and λ is the signal wavelength (Harney 2004). This relationship allows analysis of differing device sizes.

$$Gain(Dipole) = \frac{\left(\left(\frac{2\pi}{\lambda}\right)d\right)^4}{32} \tag{2.2}$$

Using, for example, 2.45 GHz (wavelength of 122.45mm), and device maximum length of one inch, or 25.4 mm, the antenna gain equates to only 0.09 while a device maximum length of even two inches increases the factor to 1.44. More effective

antennae, such as fractal antennas could boost antenna gain but is not explored in this work.

IEEE 802.15.4 systems commonly advertise transmission ranges of 10-30 meters (Gutierrez et al. 2006). As previously seen in Equation 2.1, parameters that increase range include higher antenna gain, more transmitted power, lower transmitting frequencies, or lower receiving antenna sensitivity.

Finally, attenuation through structural materials reduces transmitted power at a determined rate (Equation 2.3) and commonly relies on empirical results (Jenn and Sumagaysay 2004). The relationship is a logarithmic value associated with a ratio of power transmitted through the surface, $P_{transmitted}$, compared to power emitted from the source, $P_{incident}$. Studies indicate approximately 10 dB loss through a 10-inch concrete wall (Jenn and Sumagaysay 2004).

$$\text{Loss, dB} = 10 \log_{10} \left(\frac{P_{transmitted}}{P_{incident}} \right) \tag{2.3}$$

2. Throughput

Frequency, range, topology, and network size determine throughput across a 6LoWPAN radio link. Frequency allocations derive from country authorization or, if in a hostile environment, allocations from internal de-conflictions and threat analysis. Lower frequencies often travel longer distances and are generally more persistent while higher frequency ranges allow higher throughput but competition with other devices increases. Bluetooth technology and microwave ovens also operate in the 2.4 GHz range, though Bluetooth is similarly unlicensed, and microwaves operate in a Faraday cage. Investigations into interference levels of Bluetooth and microwave ovens find no significant influence to 802.15.4 networks at ranges nearing one meter (Sikora and Groza 2005).

Range, as described above, establishes a threshold distance at which a desired throughput can be achieved, as a function of frequency. Additionally, increasing nodal count on a common access point progressively detracts from the maximum throughput

amount. Small networks with periodic traffic will likely not notice degradation in throughput but as a networks scale larger, latency will occur in a network with decreasing access periods.

IEEE 802.15.4 networks use carrier sense multiple access with collision avoidance (CSMA-CA) or ALOHA channel access (IEEE 2011). Whether or not a personal area network (PAN) coordinator desires slotted or unslotted CSMA-CA access. CSMA-CA essentially requires a node test the target node, or nodes, for a ready to receive or not ready to receive status. If the target node, or nodes, appears ready to receive, the sending node transmits the message. If the target node, or nodes, does not appear ready to receive, the sending node waits a variable amount of time before attempting to re-send. The pre-determined CSMA-CA protocol determines the amount of time before attempting the retransmission. CSMA-CA options include slotted or non-slotted and persistent or non-persistent. Using a slotted CSMA-CA ensures all assigned nodes to a network get guaranteed time slots (GTS) in which to request access. Using non-persistent CSMA-CA protocol allows scalability since only transmitting members of the network compete for time slots. Additionally, the amount of throughput of CSMA-CA depends heavily on the expected time of propagation. Nodes separated by greater distances decrease the normalized throughput. Nodes separated by approximately 300 meters experience a throughput reduction by a factor of approximately 0.86 and separations of 30 meters experience a throughput reduction by a factor of approximately 0.96 (Agrawal and Zeng 2014).

Voice communications require significant amounts of throughput with most estimates requiring a minimum of 64 kbps. Additionally, any packet header detracts from the amount of payload on which voice communications can travel. If only 45 bytes remain out of 127, only 35.4% of the throughput is available for payload traffic in the worst case. In the best case, 78 remaining bytes allow for approximately 61% of throughput available for payload traffic. In addition, the CSMA-CA protocol requires acknowledgements and timers resulting in packets not being sent continuously (Hersent, Boswarthick, and Elloumi 2012). Node separation's heavy influence on slotted non-persistent CSMA-CA reduces the realized throughput by the factors discussed in the

preceding paragraph. Therefore, at 300 meters, the realized throughput to expect lies between 0.30 and 0.53 of the channel throughput.

A recent expert on the IoT estimates that of the 250 kbps bandwidth, only 50 kbps (or 20%) is usable for applications and only if no other devices compete for network access (Hersent, Boswarthick, and Elloumi 2012). Applying the above factor of 0.86, only 76 to 132 kbps remain for any given node in the network for application use assuming only a point-to-point link. This estimate is very close to other estimates of 50 kbps in light of expected header lengths and CSMA-CA protocols (Hersent, Boswarthick, and Elloumi 2012).

3. Power and Energy

IEEE 802.15.4 standard writers assumed power for devices would come from batteries intended to remain in service long periods of time but also capable of using mains, or grid-derived, power (IEEE 2011). Power consumption depends not only on the level of power transmitted, but also on the periodicity at which the component transmits, processes, and receives data. 6LoWPAN physical operating constraints dictate a floor output capability of -3 dBm while only local frequency regulations dictate transmission power ceiling levels. ISM bands limit transmission power to a maximum of 1 mW (Hersent, Boswarthick, and Elloumi 2012).

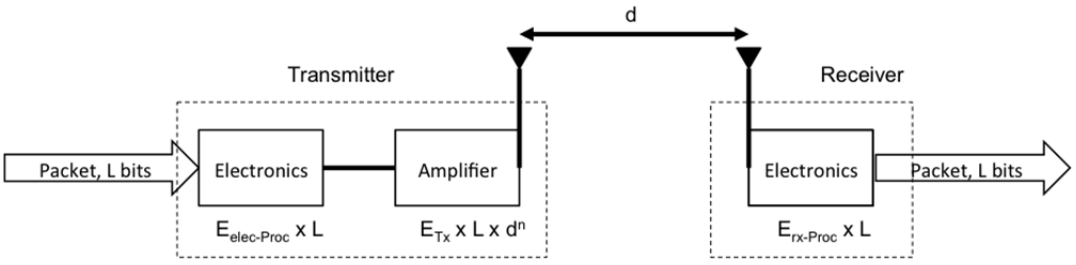
Joules (J) represents the International System of Units (SI) measure of energy. Batteries drain at differing rates depending on discharge current, in milliamps (mA), of direct current (DC). Voltage multiplied by amperage totals power and multiplying by time, in seconds, results in total energy. As an example, a typical 1.5-volt (V) AA alkaline battery containing 1700 mAh of current capacity contains 9180 Joules. Considering, then, that 6LoWPAN devices emit at the milliwatt level, nor at a constant level, the anticipated duration of a network and its associated devices should span long periods even with a much smaller initial voltage amount. Additional energy source parameters, assuming a device receives power from battery, include capacity, in joules, and efficiency. Slower power drain increases efficiency (Pedram and Wu 1999). Given the low power draw of 802.15.4 radios, this paper assumes a nominal value of 90%. For

the purposes of this paper, node size drives battery size and weight limitations. Ideally, commonly sized batteries ease logistical burden in usage cases. This thesis explores the expected lifetime of an expected node given expected usage parameters. Duracell batteries, a very common brand name battery in North America, designs battery metrics in accordance with the International Electrotechnical Commission (IEC). The density of batteries varies by chemical composition but, for comparison, Duracell's 1700 mAh NiMH rechargeable AA battery weighs 28 grams at a length of two inches and nominally discharges at 1.2 volts (Duracell 2016). Duracell's 1000mAh NiMH rechargeable AAA battery weighs 12.8 grams at a length of one and three-quarters inches and nominally discharges at 1.2 volts as well (Duracell 2016). Therefore, a typical AA rechargeable battery nominally contains 7344 Joules and a typical AAA rechargeable battery nominally contains 4320 Joules.

The transmission power, as a function of distance, contributes most significantly to the power drain on a device. An additional drain, assumed a constant value in this work, includes data aggregation, E_{DA}. E_{DA}'s assumed value in this work is 5 nJ/bit in keeping with estimates of similar work on microsensors such that Equation 2.4 holds true (Heinzelman, Chandrakasan, and Balakrishnan 2002). Multiplying by the message length in bits, L, determines the overall E_{DA} as a function of message length.

$$E_{DA}(L) = \frac{5nJ(L)}{bit} \tag{2.4}$$

The same study presented a method of determining energy dissipation per bit of data using binary values for distance, near or far, and varying message size (Heinzelman, Chandrakasan, and Balakrishnan 2002). The study also used fixed distances assuming polynomial free-space loss at a rate of distance squared, d^2, within a designated distance before assuming a multi-hop transmission (Heinzelman, Chandrakasan, and Balakrishnan 2002). The study's multi-hop transmission exhibits a quadratic energy loss at a rate of d^4, to account for multipath fading (Heinzelman, Chandrakasan, and Balakrishnan 2002). Figure 8 illustrates the exchange of energy as a compilation of E_{Tx} and E_{DA} per bit.



Heinzelman's model depends on range, processing, and packet size, though transmission power and processing power hold constant with only binary input to distance (near or far). The electronic drain should be confirmed by actual product testing. The referenced source provides parameters based on similar testing.

Figure 8. Energy Transfer Model. Source: Heinzelman et al. (2002).

However, adjusting distance allows further analysis. Thus, multiplying the transmission power by message length in bits, *L*, and dividing by bit rate, *R*, in bits per second, reveals the transmission energy dissipation rate, E_{Tx}, as a function of message size and range as in Equation 2.5.

$$E(L,d) = \frac{P_{Tx}(L)}{R} \tag{2.5}$$

Therefore, combining Equations 2.4 and 2.5, the energy expended to transmit a message of size, *L*, in bits, over a relatively close distance, *d*, in free space, a radio expends:

$$E_{FS}(L,d) = E_{DA} + E_{Tx} \tag{2.6}$$

4. Topology Options

6LoWPAN offers network topology options of star or meshed. As explained by Figure 2, networks within a single router require less addressing bytes and can operate as either star or meshed. Power consumption at the central node, or full function device (FFD), surpasses power consumption of any individual node. The 802.15.4 specification also refers to outlying nodes as restricted function devices, RFDs (IEEE 2011). Star topologies generally drain individual, or RFD, devices at a rate driven only by distance, message length and periodicity while the centralized FFD device's energy consumption scales at a rate equal to the number of interconnected RFDs. RFDs in mesh networks

generally drain at varying rates driven by proximity to the cluster head, message length and periodicity, and number of network nodes.

D. SECURITY

1. Obstacles

Wireless networks such as 6LoWPAN possess vulnerabilities common to any wireless network but the inclusion of IPv6's embedded security algorithm, IPSec, offers significant protection. Many obstacles limit security implementations to include limited storage, energy restrictions, and MTU (IEEE 2011). Limited storage onboard a sensor limits the ability to process large algorithms or large quantities of even the smallest algorithms. Energy restrictions are user-dependent as the size of the nodal power supply may be quite small if desired on a PAN though perhaps not as restrictive for a less mobile sensor field permanently emplaced. The MTU of 6LoWPAN already limits packet size and increased security, as previously discussed, only further restricts remaining usable payload space.

2. Resistance against Common Wireless Network Attacks

Predicting every type of attack or scenario remains impossible. Measuring resiliency against the most common or most dangerous attacks to a wireless network, however, may highlight a capability's strengths and weaknesses or value in further investigation for military usage. However, implementation considerations must precede any examination of a network's vulnerability. The IETF provides RFC 3756 to present three generic implementation models (Nikander, Kempf, and Nordmark 2004). Each model presents unique challenges to security, the most vulnerable being an ad-hoc network. Therefore, this thesis investigates the resiliency of 6LoWPAN against denial of service (DoS) attacks, router or routing specific attacks such as sinkhole attacks, and non-router or non-routing related attacks such as neighbor discovery (ND) attacks from a best and worst case trust model. This synopsis aims to generalize the wide array of active and passive techniques used against wireless networks. IPSec's authentication headers, AH, in conjunction with AES provides significant security against most malicious attacks. The

research question of 6LoWPAN's resistance to these common attacks is addressed in the following sections.

a. Denial of Service (DoS)

A DoS attack requires that a malicious node exist within transmission range of a threat but does not require co-location of the nodes (Vines 2002). DoS attacks generally occur by a malicious source overtaking the attention of a victim node's receiving antenna and distracting its processor to the point of denying it productive participation in its own friendly network (Nikander, Kempf, and Nordmark 2004). There is little defense any wireless network can provide against physical DoS aside from decreasing the receiving antenna's sensitivity or increasing the transmitting power within a network. By decreasing sensitivity, range quickly diminishes without an increase in transmitted power. Likewise, increasing power drains power resources more quickly and increases the network footprint and vulnerability to other attacks.

b. Router or Routing Attacks

Attacks involving routers or routing take many forms. Sinkhole attacks, sometimes referred to as redirect attacks, cause a node to unknowingly send traffic to what seems to be an ideal path to the intended destination. A malicious last hop router exists as generic IPv6 threat in which a malicious router masquerades as a legitimate last hop router on a network in which an entering node is attempting to discover one (Nikander, Kempf, and Nordmark 2004). Another method involves deleting the actual default router from a node or multiple nodes' routing tables. This attack could follow a DoS attack or even after sending minimal router lifetime over a spoofed router advertisement (Nikander, Kempf, and Nordmark 2004). Additional router-related threats include a good router going bad, spoofed redirect messages, bogus on-link prefix, bogus address configuration prefix, and parameter spoofing (Nikander, Kempf, and Nordmark 2004). Use of statically assigned IP addresses precludes each of these threats (Nikander, Kempf, and Nordmark 2004). With use of dynamic host configuration protocol, DHCP, mitigating the stated threats becomes necessary. Research continues to investigate

methods of mitigating DHCP against such threats (Nikander, Kempf, and Nordmark 2004).

An additional threat specific to CSMA-CA includes a malicious source sending inert packets with a correct preamble equivalent to 802.15.4 protocol. If the malicious source broadcasts messages to the access point, or router, at a rate faster than the other nodes' back-off timers (responsible for avoiding collisions), an access point can be denied service.

c. Non-router or Non-routing Attacks

Attacks taking place beneath the router also come in many forms. Non-router attacks such as neighbor solicitation and advertisement attempt to create unwarranted relationships between MAC Addresses and IP addresses for the purposes of redirection, even underneath the router. Once redirected, a malicious node can redirect, exploit, or even destroy packets. 6LoWPAN provides excellent defense against ND attacks. Turning off performance optimization, a command telling nodes to populate a neighbor cache table, as more links become available, routes all traffic through predetermined routes (Nikander, Kempf, and Nordmark 2004). Star topologies better lend themselves to disabling performance optimization while disabling the function cripples a major advantage of mesh networking. Mesh networks, constantly attempting to optimize traffic routing, more aptly fall victim to this form of redirect denial of service attack (Nikander, Kempf, and Nordmark 2004).

Similarly, a neighbor unreachability detection (NUD) attack happens when a sending node cannot reach the desired destination node after multiple tries. After a requisite number of failures, the sending node flushes the desired destination node's address from the standard address resolution protocol (ARP) table and looks for a valid one. During a NUD attack, a malicious node sends fabricated unavailable messages to the sending node to expedite the dropping of the desired destination node. Preventing the actual process of the desired destination node becoming unreachable or how the sending node behaves in such a situation provides the best defense against a NUD denial of service attack. In a similar manner, preventing hosts from obtaining addresses using

stateless address auto-configuration prevents duplicate address detection (DAD) denial of service attacks (Nikander, Kempf, and Nordmark 2004). Using mesh-under networking alleviates any threat from additional router-level ND attacks outlined in RFC 3756 (Nikander, Kempf, and Nordmark 2004).

E. GEOLOCATION

Without going into the methods 6LoWPAN uses to geo-locate other nodes, research accomplished on the topic reveals some overarching insights. First, implementing a real-time location system (RTLS) requires at least three anchor nodes (Martinez and Lastra 2011). Additionally, a RTLS requires nodes contacting an anchor node receive immediate acknowledgements, something not associated with UDP as the transport layer protocol (Martinez and Lastra 2011). Thus, using 6LoWPAN to geo-locate potentially requires using TCP, requiring a significantly longer header length, and the network to differentiate each node as an anchor node or not (Martinez and Lastra 2011).

F. DESIGN PARAMETERS

Table 4 lists a compilation of the design parameters in which a 6LoWPAN system must operate. Exceptions outside of the parameters are possible but require tradeoffs from other parameters. The table answers the research question of 6LoWPAN limitations by compiling performance parameters.

Table 4. Compilation of Design Parameters. Adapted from IEEE (2011).

Parameter	Minimum	Maximum	Cost –or– Limiting Design Factors
Encryption	AES-CCM-128	AES-CCM-256	Header Length (bits)
Resiliency	Withstand DoS	None	Scalability
Throughput	20 kbps	250 kbps	Energy, Time
Range	10m	200m LOS	Battery Life Antenna Length (Gain)
Transmitted Power	-3 dBm	1 dBW	Battery Life
Receiver Sensitivity	-85 dBm (BPSK) -92 dBm (O-QPSK)	Unlimited Unlimited	Transmitted Power, Interference
Battery Size	Length: None Weight: None	Max length of node Less than 60g (2 AA)	User weight limitations
Topology	Peer-to-Peer, Star	Mesh	Security, Energy Consumption, Scalability
Message Length (Remaining Payload Space)	50 bytes	71 bytes	Security, Routing, Connectivity

III. SYSTEM REQUIREMENTS

In systems engineering, operational concepts or usage scenarios commonly support generated system technical requirements (Buede 2009). The generated system technical requirements must clearly derive from, and easily trace back to, operational requirements. Operational concepts allow defining the anticipated environment, interoperability with other systems, potential threats, and how the users employ the system to more easily highlight specific operational requirements ultimately leading to comprehensive system technical requirements (Buede 2009).

Similarly, Benjamin Blanchard and Wolter Fabrycky (2011) define a generic approach for all system acquisitions and follow-on deployments. Regardless of all factors, systems engineers execute conceptual design, preliminary design, detail design and development, production/construction, operational use and system support, and ultimately, retirement during the lifecycle of a system (Blanchard and Fabrycky 2011). Operational requirements, a concept of support and maintenance, technical performance measures, functional analysis, and allocation of design criteria from the system level to sub-systems, lie within the conceptual design phase and serve to establish system technical requirements (Blanchard and Fabrycky 2011).

The Army's employment of a low-powered, wireless, personal area network in an operational or support setting defines the system within the scope of this thesis. The assessment of 6LoWPAN's employment leverages Blanchard and Fabrycky's approach to construct comprehensive usage scenarios to generate clearly derived system technical requirements.

A. BFT SCENARIO

1. Potential Opportunities

The inception of networking dismounted troops with real-time data began around 1989 as a part of the Land Warrior program, the Army's first attempt at networking individual troops on the battlefield (Gourley 2012). Having occasional name changes, by June 2010, on the Army's 235th birthday, it renamed Ground Soldier System Increment 1

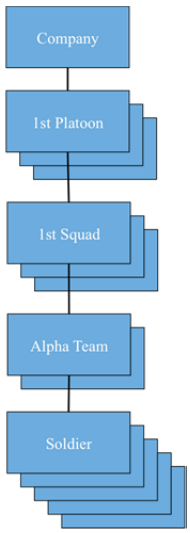
as Nett Warrior, in honor of WWII Medal of Honor winner Robert B. Nett (Gourley 2012). Requirements of Nett Warrior include, but are not limited to, providing command-and-control solutions down to the team leader level (Gourley 2012). The first prototype systems weighed as much as 10 pounds without a backhaul capability, while more recent versions weigh as little as three pounds on top of the Soldier Radio Waveform (SRW) on the Joint Tactical Radio System (JTRS) backhaul link (Gourley 2012). The JTRS SRW link typically occurs over an AN/PRC-154 handheld Rifleman Radio capable of carrying unclassified voice and data traffic, lasting at least 12 hours on a 7.2 Ah Li-Ion battery, ranging over three kilometers, and weighing approximately 1.7 pounds (Thales Defense & Security 2016). The AN/PRC-154A handheld Rifleman Radio, capable of carrying secret and below traffic, generally boasts the same specifications but a shorter range of just two kilometers and lower battery life of over nine hours due to having only a 5.8 Ah Li-Ion rechargeable battery (Thales Defense & Security 2016). For geolocation, the Army currently possesses the defense advanced GPS receiver (DAGR). The DAGR weighs 454 grams, or just less than one pound, including the provided AA batteries, with a continuous lifetime of fourteen hours but does not self-propagate location information beyond the display screen (Rockwell Collins 2016). In total, the dismounted capability available today provides voice and data at the specifications above at a weight of nearly six pounds per user, including the DAGR. The Army's baseline requirement is for a dismounted Soldier to know his own location, the location of friendlies, and the enemy's locations (Leland and Porche 2004). The 6LoWPAN capability may offer comparable performance at a lower SWAP, translating to lower Soldier payload. Lower Soldier payload well answers the research question of why the Army may desire 6LoWPAN.

2. Stakeholder Perspective

A stakeholder's analysis of BFT provides insight to the most important capabilities of an operationally deployed system. The dismounted Soldier on the ground receives position location of other users as well as enemy locations entered by any situationally aware user. The Soldier benefits from BFT through increased protection from fratricide in an increasing complex combined arms fight, but can have an adverse effect if not operating properly. In addition, Soldiers and leaders both aspire to lessen

payload weight demands on Soldiers. Current initiatives aim to reduce the weight burden on Soldiers, often surpassing 100 pounds, while maintaining or enhancing current operating capabilities (Friedl and Santee 2011). Therefore, any additional technology must be as light as possible while maintaining or exceeding current operational effectiveness. For sustained effectiveness, the technology must prove directly beneficial to the user and maintainer of the system. A subjective judgment exists about what a dismounted leader below the squad leader level needs to receive via a network given all typically remain within LOS of each other.

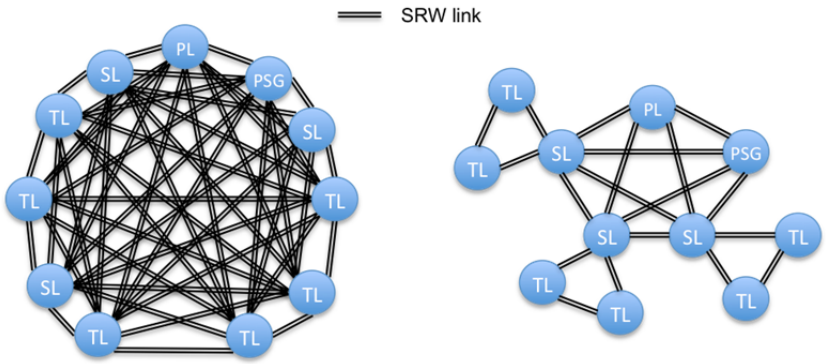
A typical infantry company contains three maneuver platoons, a platoon leader (PL), assisted by a platoon sergeant (PSG) leads each platoon and reports to the company commander. A platoon typically contains three squads, each led by a squad leader (SL) who reports directly to the PL and PSG. Each squad typically contains two teams, led by a team leader (TL) directly reporting to the SL. Lastly, a team typically consists of three to nine Soldiers. Figure 9 shows a generic Army Infantry company hierarchy.



Companies may or may not have combat support and service support elements attached in addition to headquarters elements. The figure is meant to demonstrate to the reader the amount of assets included in any given company, platoon, squad, or team. A company typically contains 2-3 platoons, a platoon typically contains 2-4 squads, a squad typically contains 2-3 teams, and a team typically contains 3-9 Soldiers. This thesis assumes 6 Soldiers plus a team leader comprising one team.

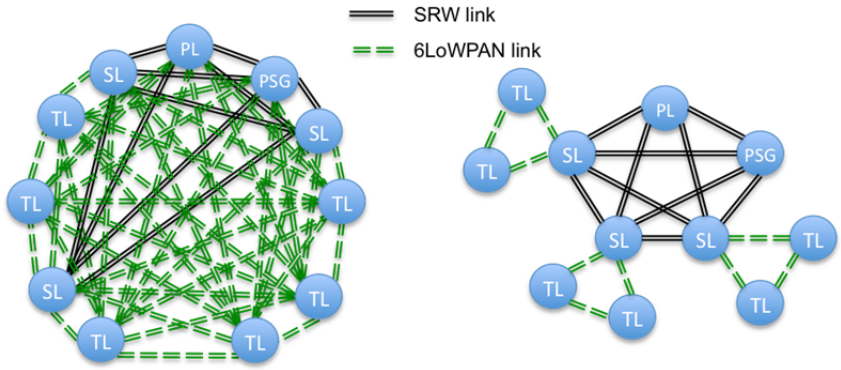
Figure 9. Hierarchical Structure of a Typical Army Infantry Company's Maneuver Elements.

Figure 10 shows two Nett Warrior connectivity implementations linking Soldiers to the network at the TL level. Figure 11 shows an alternative architecture that replaces the SRW backhaul capability from the SL to TL with a lower SWAP, 6LoWPAN capability.



While linkage options can be tailored to need, Nett Warrior capability does not currently reach below the TL level and uses the AN/PRC-154A Handheld Rifleman Radio as a link between nodes. The Rifleman Radio can, however, be issued to all Soldiers for voice and data transmissions separately from Nett Warrior.

Figure 10. Two Potential Linkage Options Using Nett Warrior's AN/PRC-154A Handheld Rifleman Radio SRW Link between Nodes.



Potential solution space could exist for 6LoWPAN to meet operational requirements and reduce weight burdens.

Figure 11. Two Potential Linkage Options Replacing Nett Warrior's AN/PRC-154A Handheld Rifleman Radio SRW Link with 6LoWPAN at TL Level.

3. Operational Scenario

In this operational scenario, the situation includes an infantry platoon conducting a presence patrol in a hostile urban setting. The objective is to ensure safety within the local market by executing a coordinated dismounted movement through a market area just prior to peak business hours. The friendly forces include the dismounted platoon, the medical casualty evacuation (MEDEVAC) team, and the local populace. Potential threats include elements embedded within the population planning to deny communication channels and split the dismounted unit in order to ambush a smaller unit subset. It is assumed each TL has a 6LoWPAN device that automatically passes location data among platoon nodes and stands prepared to pass additional data messages between platoon nodes in a fully meshed topology as shown in Figure 10. This also includes BFT information subsequently distributed across the larger joint battle command (JBC). The time is 1500 hours, local.

Each Soldier observes his assigned sector of fire, maintaining appropriate spacing to prevent a grenade blast from incapacitating more than one platoon member. The PL and PSG engage local shop owners and security forces with the help of assigned translators. At 1530 hours, the platoon leader, currently within 50 meters of each SL and seeing all nodes of his platoon on his display window receives a time-sensitive tip of a nearby meeting potentially involving a high-value target (HVT). The PL dispatches an audience-specific movement command over Nett Warrior on his display window that only his SLs and PSG all receive on their display windows. The PSG and first squad maneuver to a better supporting position as the PL maneuvers with second and third squads. At this point, the two platoon elements are no longer within LOS. At 1600 hours, from a building two blocks away, unexpected sniper fire wounds a member of second squad, Bravo team. The TL immediately shouts the suspected direction of the sniper and moves to cover before reporting the casualty over the platoon network via voice with an estimated distance and direction of the sniper. Immediately, all remaining elements move to cover-and-concealment while the Soldiers closest to the casualty attempt to drag him to a safe position. The PL attempts to better identify the location of the shooter over the platoon network. All networked leaders digitally provide their point of view in attempts

to locate the shooter. The suspected enemy location is entered into the platoon's BFT overlay using standard procedures for dismounted operations. By 1610 hours, the fire team establishes security and a casualty collection point (CCP) around the Soldier and earmarks the location in the BFT overlay, as the platoon medic treats the casualty. Meanwhile, the battalion's unmanned aerial vehicle (UAV) in overwatch has arrived on station to observe the uploaded sniper position transmitted to the higher echelon's BFTs. The PL's Nett Warrior allows live UAV feed streaming. Overwatch of the suspected position aids in locating the suspected sniper. Simultaneously, the medic informs the PSG the casualty requires immediate medical evacuation (MEDEVAC). The PSG directs the SL, who in turn directs his TL, to transmit a multicast MEDEVAC request. By 1615 hours, the PSG's remaining element is set in overwatch position; the PL's element performs flanking movements until reaching the bottom floor of the suspected building. Any lifting or shifting of fires is done using friendly position data on the BFT overlay. At 1630 hours, assuming the building size and layout is within the element's ability to clear, second and third squads enter the building with appropriate tactics moving from room to room. Within the building, Soldiers methodically clear and secure each room. For at least 30 minutes, available team members ascend to the suspected sniper position until neutralizing the threat. Simultaneously, the PSG's element is monitoring the building for any fleeing personnel out of the building of interest. Upon confirming neutralization of the threat by 1730 hours, the PL re-establishes internal platoon communications, re-establishes accountability while simultaneously observing each team's location on the BFT overlay. The CCP element, having assisted the MEDEVAC team, rejoins the PSG's element. Subsequently, the PL provides a follow-up report across the higher command network and coordinates follow-on actions.

From this single scenario, many key aspects of the TL links become apparent. Soldiers may default to voice communications when speed necessitates though data leaves a longer footprint that populates the master overlay. Two necessary parameters of geolocation are distance and direction from known position data. They can be determined without a map overlay, but this does necessitate a need for a screened display showing the user's location and distance and direction to other friendly nodes regardless of

surroundings. Terrain association, however, allows Soldiers to enter an enemy location to the network overlay or any point of interest without a self geo-locating capability. Obviously, the system must interface with Nett Warrior or physical map. Assuming a patrolling speed of no greater than two meters/second and a location accuracy of plus or minus ten meters, automatic position updates even every ten meters equate to an update rate of ten seconds. Building clearing operations typically reduce movement speed, decreasing the refresh rate requirement. This hypothetical mission lasted less than three hours but despite best plans, situations largely affect mission times. A system should not require battery recharge or replacement during mission execution, but this should be achievable quickly should the need arise. The automated communications between nodes must be secure enough to prevent spoofing or denial of service. Range between nodes averaged 50 meters, line of sight (LOS), but could extend beyond 200 meters, or even face obstructed LOS (OLOS) if within earshot, or relatively close distances, and sometimes as close as 20 meters with varying multipath interference during room clearing operations. Current doctrine for squad level tactics dictate that every Soldier should remain within sight of the team leader and every team leader should maintain visual contact with the squad leader. Doctrine trains leaders to control movement through use of hand and arm signals (U.S. Army 2007). Physically, cover and concealment pose a threat to communication systems requiring line-of-sight (LOS) communications. Team leaders typically receive more information than transmit and transmissions may often be standardized report formats. Voice commands often transmit over the platoon network but typically exchange between the PL or PSG to the SLs. A pre-formatted MEDEVAC request reduces time and bandwidth over free-text. However, pre-formatted reports require on-board caching and storing demands on each node. Sender and receiver identifications inherently populate using unique IP addressing. Command actions given digitally could require one byte per character or a preset listing of commands potentially using fewer bytes. Four bytes, for instance, allow for 2^4 or 16 options. Five bytes allows for 32 options versus a five-letter free-text word. Automated location reporting requires transmission and receipt of military grid reference system (MGRS) grid location, shift from a known point. Timing requires only an hour, minute, and second entry if not time-

stamped by the network. The requirement to transmit and receive textual commands still exists but could be reduced by use of specifically selected emojis knowing the age-old adage that "a picture is worth a thousand words." A requirement exists to locate and adjudicate enemy locations across a network, another potentially pre-formatted report. Soldiers and leaders may require node hopping to reach an intended audience necessitating additional indirect receiving and transmitting by each node at some rate. In this single scenario, no outside entities required entry into the platoon network allowing for static addressing. Lastly, Soldiers using network technology expect a way to troubleshoot a broken communications link and, therefore, expect a user-friendly interface for such purposes without additional tools or parts incurring more weight and space.

Various Army field manuals define reports common to platoon and squad-level operations. The operational situation above highlights a medical evacuation (MEDEVAC) report, shown in Table 5. A pre-formatted 9-line MEDEVAC request requires at least 57 bytes in a wartime setting, and potentially far more in a peacetime setting where an expectation of descriptive fields exist. An example of a generic call for fire (CFF), shown in Table 6 requires a maximum of 40 bytes for any one transmission but could be as low as 33 bytes for any one transmission assuming a preformatted message. Preformatted messaging offers lessened cross-traffic being sent but more internal storage capacity at each node. This assumption would require additional exploration to determine the associated power drain to perform this role at each node. For any report, the byte requirement for each assumes cached reports exist on all nodes, inferring an additional storage capability.

Table 5. An Example of a Pre-formatted 9-Line Medical Evacuation Request and Expected Byte Consumption

Line/Item	Example	Total Bytes (max)
1/Location of pickup site by grid coordinates with grid zone letters	MD 73245 23949 or 48S MD 73245 23949	15
2/Requesting Unit Radio frequency, call sign, and suffix	FM153.843*, Bravo21	20 (depending on call sign length).**
3/Patient Precedence Code and Quantity	A-1; B-1; C-3;D-2	8
4/Special Equipment Required	A	4
5/Number of Patients by evacuation type required	A-6, L-2 Or L8	4
6/Security of Pickup Site (wartime only)	N,P, E, or X	1 (wartime only)
6b/Number and type of wound, injury, or illness (peacetime only)	# + explanation	(unspecified) (peacetime only)
7/Method of marking pickup site	A,B,C,D, or E with optional description such as C, Green for green smoke (using a two letter color code)	3
8/Patient Nationality and Status	A,B,C,D, or E	1
9a/CBRN contamination (Chemical/Biological/Radiation/ Nuclear) (wartime only)	N,B, or C	1 (wartime only)
9b/Terrain Description	Descriptive details	Unspecified (peacetime only)
Peacetime Total (worst case)		55 + unspecified description fields
Peacetime Total (worst case) leveraging IP addressing for sender identification		35 + unspecified description
Wartime Total (worst case)		57
Wartime Total (worst case) leveraging IP addressing for sender identification		37

Adapted from FM3-21.7, Table 6-1, pages 6-12 through 6-13. *The radio frequency of the unit leadership net may not be the same as the unit network. Note, each character consumes one byte of data. **Using IP, address labels are placed on every transmitted packet, alleviating the need for line 2.

The operational situation above also highlights a constant exchange of position data. Line one of Table 5 highlights that only 15 bytes are required for position data, to obtain an accuracy of ten meters.

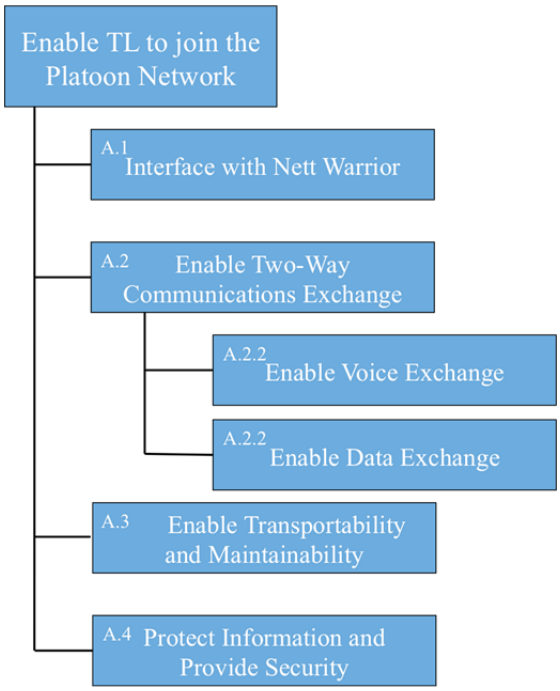
Table 6. An Example of a Pre-formatted Call for Fire (CFF) Exchange and Expected Byte Consumption per Transmission. Adapted from U.S. Army (1991).

Transmission/Item	Example	Total Bytes (max)
1a/Observer call sign and fire direction center (FDC) call sign	"Bravo45, this is Bravo21"	16
1b/Type of Mission and size of element	Adjust Fire, Fire for Effect, Suppress, Immediate Suppression/Smoke, followed by an optional last letter of call sign of desired FDC	4*
1c/Method of Target Location	Polar, laser polar plot, shift from known point, grid	3*
1d/Potential transmission of target location if immediate effects are requested or shift from a known point	AA 12345 54321 Or shift from AA1122	16
	Total	**40**
	Total (leveraging IP addressing for sender identification)**	**24**
	Total Received Back from FDC	Less than 40 (or 24 leveraging IP addressing)
2a/Position of Target	AA 12345 54321 or Direction 2300, Left 350, Add 400 (2300MIL,L350,A400)	15
	Total**	**15**
	Total Received Back from FDC	Less than 15
3a/Target Description	Dismounted Battalion in the open (free text)	Less than 30
	Total**	**Less than 30**
	Total Received Back from FDC	Less than 30
3b/Requested Munition	HE,WP,ICM (various weapon types)	3
	Total**	**33**
	Total Received Back from FDC	15 + 2 bytes challenge
4/Authentication	I authenticate "alpha"	2
	Total**	**2**
	Total Received Back from FDC	-

*Assuming brevity codes become doctrinal. All transmissions to and from the observer could feasibly remain under 24 bytes but the initial transmission could drop the location data in initial transmission if performed in near concurrent time by pre-programmed BFT updates. Thus making the worst case become less than 30 bytes required for any one transmission.** Using IP addressing, sender identification and authentication gets accomplished each transmission.

Compiling the operational requirements leads to a list of required functions and results in answering the research question of where 6LoWPAN could interface current

capabilities. The functions in Figure 12 enable the TL to join the platoon voice and data network.



The functions cleanly translate into operational requirements from which technical requirements can be derived.

Figure 12. Essential Functions for Networking TLs to the Platoon Network.

The same approach allows analysis of requirements to enhance current capabilities such as integrating the Soldier level below the TL level. The same operational scenario allows extraction of Soldier level usage profiles if necessary, leading to a near identical functional decomposition. Measuring relative advantage over current capability must evaluate the effectiveness of adding both capability and weight to the Soldier level. These functions each possess objectively measurable and technical thresholds, or requirements.

B. BFT BACKHAUL TECHNICAL REQUIREMENTS

The technical requirements of the BFT backhaul capability must trace back to the aforementioned operational requirements. Table 7 places performance metrics on

operational requirements, quickly deriving system technical requirements for operational use at and below the platoon blue force tracking backhaul capability.

Table 7. Translation of BFT Backhaul Operational Requirements to System Technical Requirements.

Operational Requirement	System Technical Requirement	Performance Metrics
A.1 Interface with Nett Warrior	The system must be IP based The system should be compatible with Nett Warrior physical connection interfaces with no net power exchange	Network Interfaces Hardware Interfaces
A.2 Enable Two-Way Communications	The system must operate at a maximum range of 300 meters The system must be capable of over 7.5 hours (T)(x3 expected usage time); or 25 hours (O)(x10 expected usage time) continuous hours of operation Support multi-hop performance or mesh networking; support ≤3 hops	Meters Duration (hours) Hop Count (number)
A.2.1 Enable Voice Exchange	System must transmit and receive acceptable (subjective) voice quality with acceptable error rate	Throughput (bps), Latency (seconds) Message, Packet Error Rate (%)
A.2.2 Enable Data Exchange	The system must successfully transmit and receive position data, 15 bytes maximum (T) from all assigned nodes; transmit and receive pre-formatted reports, 57 bytes maximum (O)	Message Length (bytes) Data Rate (bps) Message Assuredness (% packets lost)
A.3 Provide Geolocation	The system must automatically maintain device geolocation data to an accuracy of ±10 meters at a moving speed of 2 m/s	Distance (meters) Latency (seconds)
A.4 Enable Dismounted Soldier Transportability and Maintainability	The system must be lighter than the AN/PRC-152A weighing less than 1.7 pounds (0.77kg) (T), or 50% relative advantage, weighing less than 0.85 pounds (0.385kg) (O) The system must be self-powered (Untethered) (T), use standard battery size such as AA or AAA (O) The volume must be less than the AN/PRC-152A 7.6” x 2.5” x 1.6”.	Repair Time (seconds) Weight (kilograms) Battery Powered Volume (cubic inches)
A.5 Protect Information and Provide Security	The system must ensure all sensitive data meets NSA Encryption standards for wireless traffic	Encryption Standards

The transition requires a measure of assumption and generalization but a thorough process of operational analysis enables extraction of technical requirements the system must accomplish. Measurements such as the maximum physical size are inferred by the current size, weight, and power of the AN/PRC-154 radio (Source: Thales Communications, http://www.thalescomminc.com/userimages/Documents/Data%20Sheets/Thales_ANPRC154B_Rifleman.pdf, 2016).

Success of a system replacing BFT backhaul at the TL level or enhancing current capabilities at the TL to connect the Soldier level rests on meeting the specified system technical requirements.

C. COMBAT SUPPORT SCENARIO

1. Potential Opportunities

The Army presently requires an integration mechanism for managing power and energy on installations as well as giving Soldiers and leaders a multimedia interface through which to measure, manage, control, prioritize, and redistribute resources (Army Capabilities Integration Center–Research, Development and Engineering Command–Deputy Chief of Staff, G-4, U.S. Army 2010). The white paper's energy security goals show potential solution space for 6LoWPAN by reducing energy consumption and increasing efficiency (Army Capabilities Integration Center–Research, Development and Engineering Command–Deputy Chief of Staff, G-4, U.S. Army 2010). As stated earlier, some of the current commercial uses achievable by 6LoWPAN include control of interior lighting, audio and video, thermostat control, or multiple monitoring systems. Industry's use of 6LoWPAN technology includes remote sensor and actuator control in monitoring or automation processes (Toscano and Bello 2012). Army base infrastructure requires many, if not all, of the same functionalities. Automatic dimmer switches today connect to room motion sensors and save on unnecessary lighting expenses. Motion sensors beneath water and soap spigots reduce unnecessary waste. Automatic timer-cutoff switches reduce fuel or battery waste. However, motion sensor control possesses problems of inconsistent performance experienced by anyone attempting to wash his or her hands underneath one. Additionally, timer-based cutoff switches risk costly unnecessary startup and shutdown procedures.

Two-way networking offers separate savings, in time and resources. Strong potential exists in personnel or equipment location within a defined space, or smart building. Thus, further applications of 6LoWPAN include processing of frustrated cargo, vehicle tracking, hospital patient monitoring, or equipment monitoring. Even sensitive

resources such as donated blood within a temperature-controlled storage room require near real-time data on location, temperature, and shelf-life.

2. Stakeholder Perspective

A stakeholder's analysis of smart building technology provides insight to the most important capabilities of an operational system. Within a defined space such as a military hospital, equipment and patient tracking commonly occurs when an employee physically locates the equipment or patient through annotating last known location. A nurse keeping track of unused monitors of interest or patients in the infectious disease wing desires knowing near real-time locations of both. Attending nurses in search of doctors also desire knowing near real-time locations of the doctoral staff. The hospital staff in search of usable blood could record and automatically update inventory in near real-time. The hospital patients and staff demand anonymity from outside onlookers and the associated equipment must prevent unwanted tampering of information. Security, mobility, and timeliness emerge as paramount to the stakeholder. Therefore, any additional technology must be untethered, lightweight, capable of reporting location, and offer appropriate data throughput.

3. Combat Support Scenario

In this operational scenario, the situation includes a combat support hospital (CSH) staff responding to a combat related sniper wound being brought in for emergency treatment. The objective is to save the life and limb of the Soldier. The friendly forces include the hospital staff, the patients, and the visitors. Potential threats include lost time due to misplaced equipment or any local national personnel hired to work within the building desiring to disrupt operations for any reason. It is assumed each hospital staffer, patient, and shared equipment has a 6LoWPAN device, and integrated 802.11 routers capable of interfacing 802.15.4 devices cover the hospital footprint. The 6LoWPAN devices continually pass location and patient data throughout the field hospital. The field hospital occupies a concrete shelter built by local contractors of the host country. The time is 1500 hours, local.

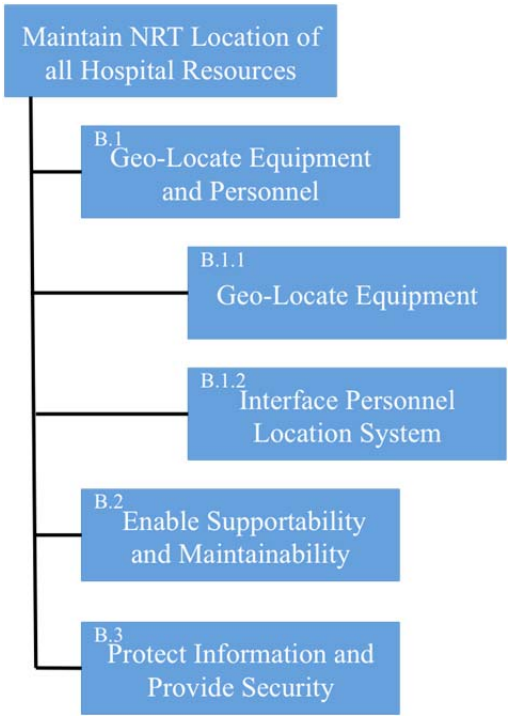
A MEDEVAC support team notifies the combat support hospital (CSH) they are inbound with a wounded Soldier and his leg is bleeding badly. All staffers dutifully execute assigned roles and move to assigned locations. The anesthesiologist is in the chow hall while the chief surgeon is resting in his bunk. Those in the emergency wing detect the locations of the 802.15.4 devices assigned to the needed personnel. Meanwhile, a nurse scans a bag of blood on a networked scanner that immediately gets transmitted over the network to update the inventory. The needed doctors are notified by either a runner knowing their positions or messaged on personal 6LoWPAN devices interfacing a display screen. High-value high-demand equipment is easily located using the master overlay. A coordinated effort, accelerated by use of 6LoWPAN, saves the Soldier's life. In the days following the emergency surgery, the Soldier's vital signs in recovery begin to fall. A 6LoWPAN device transmits an alarm tone to specific medical personnel based on threshold values dynamically set on a blood pressure monitor wirelessly connected to the network. The monitoring nurse immediately checks on the patient while the doctor adds the patient next in his queue to check. Information dynamically set by each sensor transmits to a database cataloging desired data. All vital and shared medical equipment gets tracked real-time with location and battery status. A local national and his device enabled cleaning equipment get noticed entering a restricted area cueing military police to immediately intervene.

From this single scenario, many key aspects of the smart building data links become apparent. Location of personnel and assets also require precision inside ten meters. Additionally, the capability must geo-locate without an additional interface. Coupled with a static map overlay, distance and direction to items quickly gets determined. Hospital staffers need real-time location data on doctors, such as an anesthesiologist. Near real-time (NRT) position updates provide location and pattern of movement. Hospital staffers and equipment require a lightweight, non-obtrusive, untethered device containing identification consistent with their role. A very large area network, with high-power, long-range, and heavy-throughput capability may unnecessarily expend energy and resources. Data matching persons and locations in a non-hostile environment poses little threat to security but may warrant encryption in a

hostile environment. A fixed network node within a building offers opportunity for connection to fixed power sources. A wireless network creates vulnerability to denial of service attacks. A low-powered network attenuated by exterior walls emits a lessened footprint and reduces the risk of eavesdropping or malicious nodes even sensing a network. However, in this case, any nodal transmission should be less than what is required to pass through floors or exterior walls. Therefore, static nodes would need to be placed appropriately to relay information from any rooms back to a compiling system. The lightweight, non-obtrusive, untethered device requirement translates to battery operated, less than a few square inches, and weigh no more than cellular phones of today. Each floor could contain a single integrated router or each section of a floor could contain an integrated router. Topology and routing dictate power requirements at differing levels or roles. A compiling system with a BFT overlay, presumably viewable at each nurse's workstation, enables multi-viewing and querying. Therefore, an interface must exist to a system networking multiple locations and capable of displaying received information to all users simultaneously. Any PC, laptop, or even smart phone on the market today possesses ample capability to receive IP based packets, glean the information contained therein and display on a map or multi-dimensional model executed at the application layer of the TCP/IP protocol stack. The system must be maintainable by hospital staff with minimal effort. Any device carried by personnel must be highly transportable. A device requiring a battery change out or being below a disposable cost-point both offer reasonable levels of maintainability. An IP-based system easily allows IP-capable devices, such as smart phones, to join the larger network and participate in data exchange assuming a security layer exists between the external interface and the nodes. Incorporation of smart phones as user interfaces and user input mechanisms presumably ensures the highest level of adoption. Therefore, accomplishing indoor geolocation of personnel through means of Wi-Fi triangulation is assumed to provide sufficient accuracy. Implementation requires that users allow location sharing with the intended application on the device. Personnel without a Wi-Fi capable personal device should carry a dedicated 6LoWPAN device. Lastly, a system node on common equipment

should last at least one month, or 30 days, without requiring battery swap out. Nodes worn by individuals should last no fewer than 24 hours and ideally as long as 30 days.

Compiling the operational requirements leads to a list of required functions and results in answering the research question of where 6LoWPAN could interface current support capabilities. The functions in Figure 13 accomplish maintaining near real-time location of all hospital resources and personnel.



The functions cleanly translate into operational requirements from which technical requirements can be derived.

Figure 13. Essential Functions for Maintaining Near Real-Time Location of all Hospital Resources and Personnel.

D. COMBAT SUPPORT TECHNICAL REQUIREMENTS

The technical requirements of maintaining near real-time location of all hospital resources must trace back to the aforementioned operational requirements. Table 8 places performance metrics on operational requirements, quickly deriving system technical requirements for operational use as a smart-building equipment and personnel tracking

system. Success of a system enhancing NRT locating of hospital resources and personnel rests on meeting the specified system technical requirements.

Table 8. Translation of a Smart Building's Operational Requirements to System Technical Requirements.

Operational Requirement	System Technical Requirement	Performance Metrics
B.1 Geo-Locate Equipment and Personnel	The system must geo-locate other nodes at least 20 meters through obstructed line-of-sight (OLOS) equivalent to a 10-inch thick concrete wall. (Equivalent to 200 m LOS) Position must update once every 10 minutes	Range (meters) Frequency (minutes)
B.1.1 Geo-Locate Equipment	The system must be capable of geo-locating equipment without use of a separate system capability to an accuracy of 5 meters (O) but as low as 10 meters (T).	Accuracy (meters)
B.1.2 Interface Personnel Location System	The system must be capable of accepting geolocation from personal smartphones.	Definition of Interface (exchange of energy, information)
B.2 Enable Supportability and Maintainability	The added system weight must not exceed 0.45kg (1 pound) (T); must not exceed 0.28kg (0.5 pounds)(O). Devices on personnel must last no less than 24 hours before battery replacement Devices on equipment must last no less than 30 days before battery replacement. Device size must remain smaller than device to which it attaches	System Weight (pounds) Duration (hours, days) Size (relative)
B.3 Protect Information and Provide Security	The system must not allow uninvited nodes from joining network The system must prevent compromising of personally identifying information	Accepted security practices in place

The transition requires a measure of assumption and generalization but a thorough process of operational analysis enables extraction of technical requirements the system must accomplish.

IV. ANALYSIS OF 6LOWPAN FEASIBILITY

This chapter addresses 6LoWPAN protocol performance against derived system requirements. In doing so, the chapter answers the research question of assessing feasibility for Army usage in both an operational setting and support setting. Measures of performance within a communication system at each setting defined in previous chapters lead to measures of success, or feasibility. Both scenarios provide an opportunity to address the research question on SWAP costs.

A. OPERATIONAL SETTING

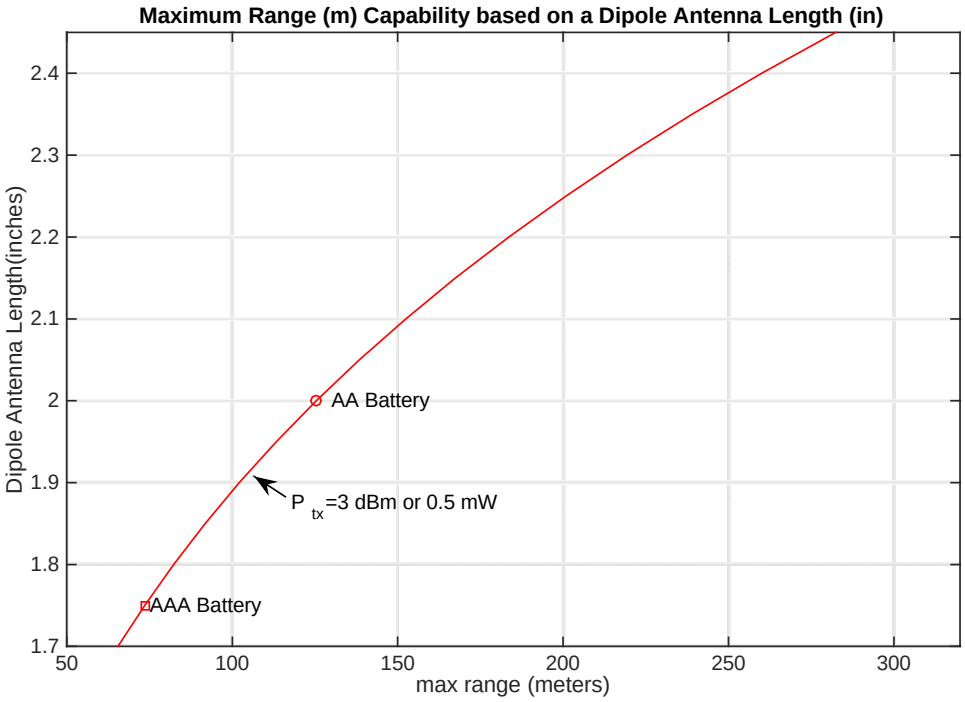
In a BFT backhaul role, analyzing sufficiency for operational use, can begin at any point since all performance requirements (device size, range, throughput, duration, topology, and security) must be assessed against all others. This analysis demonstrates only a subset of calculations. Assessments in this chapter initially assume a star topology with intent to minimize size and power while meeting throughput and range requirements.

1. Range

In attempts to keep size and weight as small as possible, the device should be no larger than the battery size if possible. The dominant dimension of a standard AA battery is 5.05 centimeters (2 inches) and a standard AAA battery is 4.45 centimeters (1.75 inches). Antenna gain advantage (Equation 2.2) amplifies the signal on both the transmitting and receiving ends. Considering input parameters consistent with Table 9, Friis' free space equation (Equation 2.1) is used to calculate the LOS transmission range. The results of these calculations fail to meet the worst-case operational requirement of 300 meters using just 0.5 mW of transmission power, as shown in Figure 14. However, dipole antenna length affects the transmission power at a non-linear rate of change. The analysis assumes equal antenna lengths and associated gains on both the transmitting and receiving devices.

Table 9. Input Parameters to Friis' Free Space Equation

Input Parameter	Value
Dipole Antenna Length (inches)	1.70 to 2.45
Transmission Power (dBm)	-3
O-QPSK Frequency (MHz)	2450
Receiver Sensitivity (dBm) (O-QPSK)	-85
Noise Factor (dB)	3

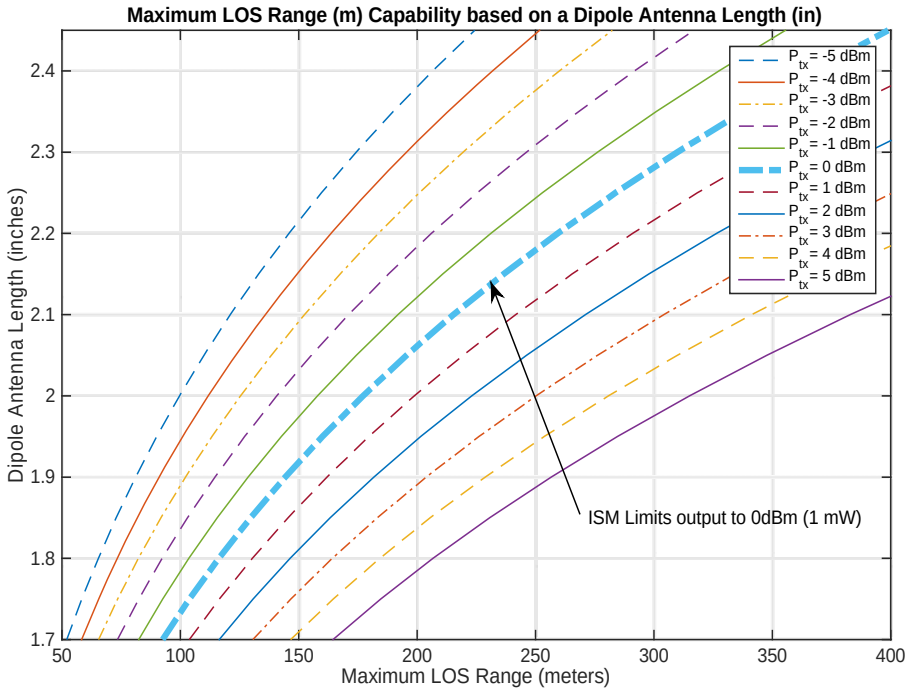


The relationship demonstrates the effect antenna length has on range. Beyond 300 meters range, atmospheric attenuation reduces range at rates not reflected by the relationship.

Figure 14. Range Capability as a Function of Minimum Power and Dipole Antenna Length

An optimized solution meets the required distance with the least amount of power but must balance overall device length as an additional constraint from the user. Figure 15 shows a series of maximum range capabilities based on varying dipole antenna length and transmission power. Achieving 300 meters is possible by 0 dBm (1 mW) but requires

a dipole antenna length of at least 2.3 inches. However, decreased dipole antenna length directly increases transportability to the user.



Observing the 300-meter requirement, lower transmission strength requires more dipole antenna length. At 2 inches, at least 5 dBm of Transmission power is required. ISM Band restrictions limit maximum output to 0 dBm. Therefore, at 0 dBm, at least 2.3 inches of dipole antenna length are required.

Figure 15. Relationship between Antenna Length, Transmission Power, and Range

User requirements should define a maximum device dimension but be mindful of the direct influence on required energy. Optimizing a minimum size suggests a maximum dimension no larger than the required battery size. However, the minimum power able to reach beyond 300 meters with only -2 dBm (0.63 mW) is approximately 2.45 inches dipole length.

The resultant range values use an estimated loss factor of 3 dB due to internal componentry. Removing this factor essentially increases the range by a multiple of 1.414, the square root of two. This thesis does not perform analysis on obstructed LOS, though

equations such as the Okamura-Hata model equations exist and can be used to determine radio frequency behavior for urban areas given specific input parameters.

2. Throughput

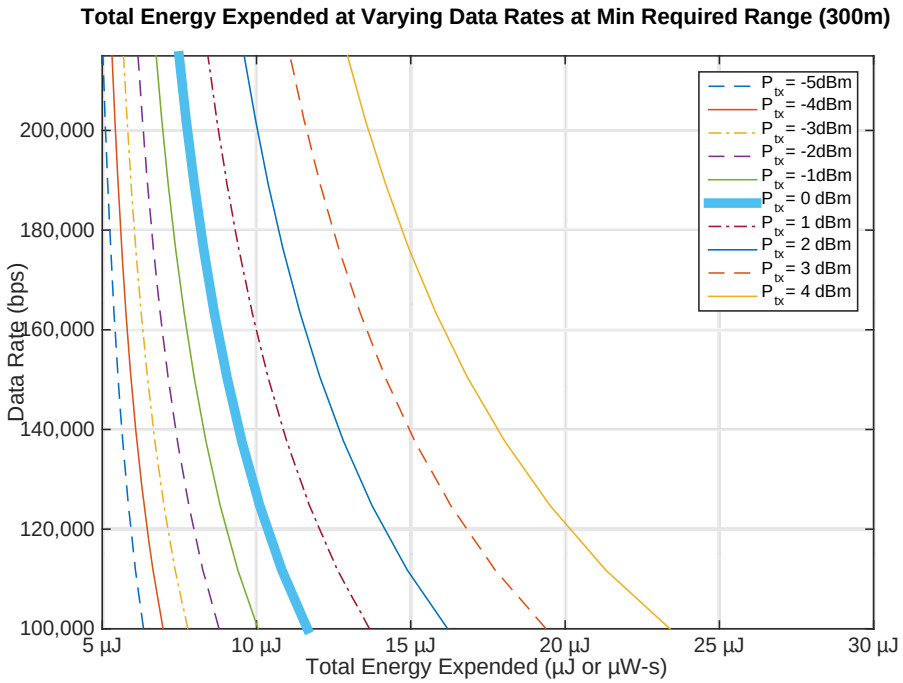
Only actual realized data rate determines performance. Detractors from data rate include headers, or overhead, at each layer discussed in Chapter II. In the best case, headers reduce the 127-byte message to carrying 78 bytes of payload traffic. This factor of actual payload versus message length results in 61.5% of the intended 250 kbps throughput, equating to approximately 153 kbps. In the worst case, only 35.4% of 250 kbps transmits payload, equating to approximately 88 kbps actual realized throughput. Further still, CSMA-CA protocols reduce throughput as a function of distance, a factor of 0.86 at 300 meters and 0.96 at 30 meters. Thus, resulting in a maximum realized throughput between 76 kbps and 132 kbps at 300 meters, and 85 kbps to 147 kbps at 30 meters.

Voice communications could feasibly occur with high compression rates performed by compressor-decompressor (codec) devices. However, this thesis does not measure the acceptability of voice performance, scalability effects from additional users, or additional power consumption a codec may draw. In any case, additional users reduce the amount of available throughput and additional processing requires additional power.

3. Power and Energy

Energy measurements are calculated based on intended throughput reduced only by the CSMA-CA factor since it affects transmission rates. Figure 16 uses Equation 2.5 to display the energy expended for a device containing a dipole antenna of 2.45 inches in length, and transmitting a full-length message of 127 bytes to a range of 300 meters. Figure 16 shows the energy expended in Joules for data rates ranging from 250 kbps, the theoretical maximum of 2.4 GHz, at 300-meter separation using CSMA-CA protocols, to 100 kbps, an alternate value specified in the protocol. Figure 16 also shows the energy expended based on varying transmission powers ranging from -5 dBm (0.316 mW) to 4 dBm (2.5 mW).

Incorporating Equation 2.4, data aggregation costs further energy at a rate of 5 nJ per bit. Thus, full-length messages of 127 bytes cost 5080 nJ per transmission for data aggregation alone. Expecting a CSMA-CA throughput performance of 215 kbps at the maximum ISM power of 1mW (0 dBm), a full-length message expends an estimated 4064 nJ. Compiling both energy decrements using Equation 2.6, the total energy expended as a function of message length, distance, transmission power, and throughput is displayed in Figure 16.



The data aggregation energy adds to the transmission energy for total energy expended based on a 300-meter range. The figure also represents a CSMA-CA factor of 0.86, and sending a full message length of 127 bytes plus 5 nJ/bit of aggregation.

Figure 16. Total Energy Expended per Message for Various Data Rates and Transmission Powers using CSMA-CA Protocols at 300 meters

Thus, assuming a linear battery drain profile to simplify analysis, a fully charged AAA rechargeable battery discharging at 1.2 volts contains 1000 mA-hours, 4320 Joules, or 4320 Watt-seconds. A fully charged AA battery discharging at 1.2 volts contains 1700 mAh, or 2040 mW-hours, or 7344 Joules. Another option is to use a disposable AA or

AAA battery discharging at 1.5 volts that contains even more energy. This option is a simple calculation difference and not investigated in this thesis. Each message, depending on the data rate and message length, takes a specific time to send. This transmission time is denoted as t_{trans}. Hence, combining the amount of energy expended per message, E_{FS}, t_{trans}, and applying CSMA-CA protocols at 300 meters, the worst-case device duration times can be calculated. The device duration times are shown in Table 10. As a walkthrough example, at 250 kbps, the CSMA-CA protocols throttle the actual throughput down by a factor of 0.86 at 300 meters to 215 kbps. A 127-byte message equates to 1016 bits and dividing the length by rate computes t_{trans} in seconds per message. The total Watts expended per message, as calculated in Equation 2.6, vary by transmission power, message length, processing power assumption, and bit rate. The duration of a device varies by energy source size. Table 10 only highlights the results for -2 dBm and 0 dBm for both battery types and various bit rates.

Table 10. Device Duration (High-Low limits, -2 dBm and 0 dBm) by Data Rate in Continuous Operation using AA or AAA Battery

Data Rate (kbps)	Actual Data Rate (kbps) using CSMA-CA protocols at 300 m	Actual Throughput (kbps), variable header plus CSMA-CA at 300 m	t_{trans} (s/msg) L/R	Total Watts expended per message (-2dBm)	Total Watts Expended per message (0 dBm)	AAA Duration		AA Duration	
						-2 dBm (hours)	0 dBm (hours)	-2 dBm (hours)	0 dBm (hours)
100	86	30 to 53	0.0102	1.3E-05	1.7E-05	0.56	0.48	0.73	0.63
115	98.9	35 to 61	0.0088	1.2E-05	1.5E-05	0.58	0.51	0.76	0.66
130	111.8	39 to 69	0.0078	1.1E-05	1.4E-05	0.60	0.53	0.79	0.69
145	124.7	44 to 77	0.0070	1.0E-05	1.3E-05	0.62	0.55	0.81	0.71
160	137.6	48 to 85	0.0064	9.7E-06	1.2E-05	0.64	0.56	0.83	0.73
175	150.5	53 to 93	0.0058	9.3E-06	1.2E-05	0.65	0.58	0.85	0.75
190	163.4	58 to 101	0.0053	9.0E-06	1.1E-05	0.66	0.59	0.86	0.77
205	176.3	62 to 109	0.0050	8.7E-06	1.1E-05	0.67	0.60	0.88	0.79
220	189.2	67 to 117	0.0046	8.5E-06	1.0E-05	0.68	0.61	0.89	0.80
235	202.1	71 to 125	0.0043	8.3E-06	1.0E-05	0.69	0.62	0.90	0.81
250	215	76 to 132	0.0041	8.1E-06	9.8E-06	0.70	0.63	0.91	0.83

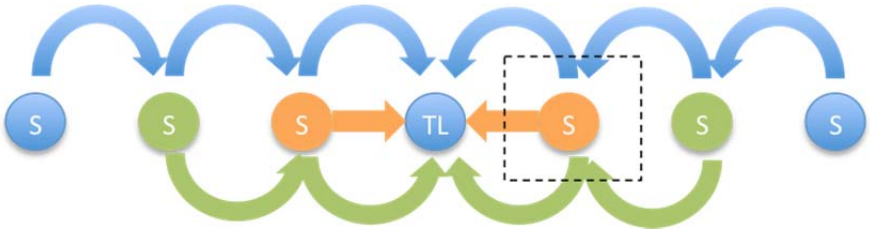
This table depicts expected device duration of various data rates transmitting full-length messages for a six-member fire team. It also assumes 5 nJ/bit for processing.

Assuming constant transmission and data aggregation at an actual rate of 215 kbps based on 250 kbps transmitted for a star topology, and -2 dBm (0.63 mW) output power, a 6LoWPAN device using an AA battery would last no less than 0.91 hours, or 55 minutes. Similarly, using an AAA power source with identical inputs allows continuous operations for no less than 0.70 hours, or 42 minutes. A sensitivity analysis on data aggregation energy shows that doubling the required power to 10nJ/message reduces the expected lifetime of the same parameters of an AA powered device to last approximately 43 minutes, and AAA powered devices to last approximately 33 minutes.

Constant transmissions, however, may not be necessary per the requirement that data position updates occur only once every 10 seconds. This requirement updates the message per hour rate to 360 messages per hour, far less than 762,000 messages per hour used for continuous transmissions. Therefore, the anticipated device duration at 300 meters, transmitting at -2 dBm once every 10 seconds, and using CSMA-CA protocols lasts 26.5 hours (AA Battery) or 20.3 hours (AAA Battery).

4. Topology

The data presented thus far describe a star network performance. However, mesh topologies can be supported for a team size element must take three or fewer hops to support requirements A.2 and A.3. Considering each retransmitted message requires the same amount of energy as an original message, a team member acting as a cluster head should expect to pass traffic from additional nodes at a rate equal to the overall team size, *n*, plus his or her own every ten seconds, as shown in Figure 17. Similarly, nodes closest to a cluster node should nominally expect to pass traffic from additional nodes, at a rate half the size of the team, *n/2* times as often also shown in Figure 17. Obviously, nodes serving in a cluster head role require additional energy sources.



The number of messages a meshed device should expect to pass depends on the team or squad position. The closest in, or orange, team member (surrounded by the dotted line box), setup by this specific routing configuration should expect to pass 3 messages (shown in blue, orange, and green to highlight separate messages) every 10 seconds.

Figure 17. The Number of Messages Any Device Should Expect to Pass

Therefore, a node operating as a team member node should nominally expect to pass three times the amount of messages every 10 seconds in a six member team. Additionally, scaling to a mesh network practically precludes voice traffic already on the minimum edge of acceptability in a point-to-point configuration. Table 11 displays the resultant duration expectancies for a team member device in a data-only transmission environment.

Table 11. Team Member Device Duration (High-Low limits, -2 dBm and 0 dBm) by Data Rate given Expected Traffic Demand UsingAA or AAA Battery

Data Rate (kbps)	Actual Data Rate (kbps) using CSMA-CA protocols at 300 m	Actual Throughput (kbps), variable header plus CSMA-CA at 300 m	t_{trans} (s/msg) L/R	Total Watts expended per message (-2 dBm)	Total Watts Expended per message (0 dBm)	AAA		AA	
						Duration at -2 dBm (hours)	Duration at 0 dBm (hours)	Duration at -2 dBm (hours)	Duration at 0 dBm (hours)
100	86	30 to 53	0.0102	1.0E-05	1.7E-05	9.42	8.11	12.28	10.57
115	98.9	35 to 61	0.0088	9.5E-06	1.5E-05	9.80	8.51	12.78	11.09
130	111.8	39 to 69	0.0078	9.0E-06	1.4E-05	10.14	8.86	13.22	11.55
145	124.7	44 to 77	0.0070	8.6E-06	1.3E-05	10.43	9.17	13.59	11.95
160	137.6	48 to 85	0.0064	8.3E-06	1.2E-05	10.68	9.44	13.93	12.31
175	150.5	53 to 93	0.0058	8.0E-06	1.2E-05	10.91	9.69	14.22	12.64
190	163.4	58 to 101	0.0053	7.8E-06	1.1E-05	11.11	9.92	14.48	12.93
205	176.3	62 to 109	0.0050	7.6E-06	1.1E-05	11.29	10.12	14.72	13.20
220	189.2	67 to 117	0.0046	7.4E-06	1.0E-05	11.45	10.31	14.94	13.44
235	202.1	71 to 125	0.0043	7.2E-06	1.0E-05	11.60	10.48	15.13	13.67
250	215	76 to 132	0.0041	7.1E-06	9.8E-06	11.74	10.64	15.31	13.88

This table depicts expected device duration of various data rates transmitting full-length messages for a six-member fire team with each team member only sending traffic once every 10 seconds. It also assumes 5 nJ/bit for processing.

In a mesh topology, if each device attempts transmission only once every 10 seconds and assuming 85 kbps realized throughput based on 250 kbps transmitted, and -2 dBm (0.63 mW) output power, a 6LoWPAN device using an AA battery would last no less than 15.3 hours. Similarly, using an AAA power source with identical inputs allows operations for no less than 11.7 hours. Further, if only position data (15 bytes) gets transmitted, an AA battery lasts over 17.5 hours and an AAA battery lasts over 13.4 hours.

The addition of a second battery simply doubles the lifetime, but adds associated weight. Though frequency and spectrum management may limit transmission power, antenna length for additional gain most directly maintains range at lesser transmission power.

5. Security

The NIST allows sending SBU information over an AES-CCM-128 network. All estimates of throughput, energy, and duration anticipate a byte requirement consistent with AES-CCM-256. Authorizing traffic at the appropriate level to transmit SBU saves 18 bytes per message, or 144 bits per message. The savings of 18 bytes can be realized by increased payload space, resulting in increased throughput. Therefore, the shorter messages directly reduce energy consumption and increase device longevity.

A star topology may fit current Infantry tactics, techniques, and procedures (TTPs) of being within LOS of the Team Leader. Making the team leader (TL) a cluster head, the network devices search only for one target. Because the network is mobile and low power, the likelihood is lessened that an adversary could capture any payload data, or even affect the header data (that is unencrypted), thus negating the need for any further security in this area.

Overall, network architecture limited only by IPv6, determines routing and hop count conditions. A route-over or mesh-under configuration determines necessary levels of security. The assumptions made in this analysis used worst-case values to ensure appropriate consideration of feasibility.

The military's DOD Information Assurance Certification and Accreditation Process (DIACAP) must assess the network architecture. This thesis assumes firewall functionality exists at the interface between 6LoWPAN devices and the larger network to allow less than AES-CCM-256 encryption.

6. Geolocation

Geolocation in a mobile ad-hoc network (MANET) requires data rates outside of the capability of this protocol. In a best-case scenario, attempting to triangulate location requires at least three additional stationary nodes. The nodes required to be stationary must self-report as stationary. This functionality requires additional programming to the processor, also requiring additional energy drain outside the scope of this thesis. This thesis assumes an interface to an external GPS device such as the DAGR, weighing one pound with battery.

B. SUPPORT SETTING

Applying the same process for analyzing sufficiency to a support setting demonstrates the robustness of the model. The same model process measures feasibility of 6LoWPAN for secure Army use in a general support setting.

1. Range

Much closer range requirements exist within a combat support hospital. Often thin tent walls do little to attenuate signals at such close distances but employment within an occupied concrete structure could significantly alter the expected range of performance and act as a worst-case figure. Internal building attenuation of a 10-inch concrete wall, not uncommon in desert-area construction, of 10 dB nominally equates to a range reduction of one-tenth. Therefore, a requirement of 20 meters OLOS equates to ranging 200 meters LOS. Referring back to Figure 15, a 2.1 inch dipole antenna ranges 200 meters LOS at 0 dBm (1 mW) and a 2.2 inch dipole antenna ranges 200 meters LOS at -2 dBm (0.63 mW).

2. Throughput

Throughput remains consistent between both models employing CSMA-CA and header options. Reduction in message sizes, fewer nodes, and closer ranges increase throughput.

3. Power and Energy

Power and energy calculation methods remain consistent between both models but the requirement for the number of messages per unit time differs. Requirements for equipment updates within a facility differ depending on the relative importance of the piece. Assuming a position update frequency every 10 minutes, a lower range requirement, and potential for shorter message lengths, the battery life extends well beyond the BFT use. Table 12 shows an abbreviated version of expected device duration at varying data rates, 5 nJ/bit of data aggregation, suggested upper and lower transmission powers for each battery type, star topology, position only message lengths, and frequencies.

Table 12. Item Tracker Device Duration (High-Low Transmission Powers, dBm) by Data Rate given Expected Traffic Demand using AA or AAA Battery

Data Rate (kbps)	Actual Data Rate (kbps) using CSMA-CA protocols at 200 m	Actual Throughput (kbps), variable header plus CSMA-CA at 200 m	t_{trans} (s/msg) L/R	Total Watts expended per message (-2 dBm)	Total Watts Expended per message (0 dBm)	AAA		AA	
						Duration at -2 dBm (hours)	Duration at 0 dBm (hours)	Duration at -2 dBm (hours)	Duration at 0 dBm (hours)
100	92	30 to 53	0.0078	9.6E-06	1.3E-05	169	147	233	206
175	161	52 to 93	0.0044	7.1E-06	9.0E-06	192	173	262	239
250	230	76 to 132	0.0031	6.2E-06	7.5E-06	205	188	277	257

This table depicts expected device duration of various data rates transmitting position-length only messages. Position messages only require 15 bytes of payload data as opposed to the 45-87 available bytes of full-length messages. The CSMA-CA rate estimated logarithmically between 0.86 (300m) and 0.96 (30m) to be 0.92 (200m)

Further observation of Table 12 reveals the duration of devices meet a requirement to last beyond seven days (168 hours) at -2 dBm. Coupled with a battery charger, assuming ideal battery performance, a long-term expectation of devices lasting at least one week is reasonable. Batteries could alternate weeks of use and re-charging in-between. To range 200 meters at -2 dBm, the device length must be at least 2.2 inches.

4. Topology

The scenario assumes a star topology requiring integrated access points capable of translating 802.15.4 protocol into 802.11x backhaul. Otherwise, a meshed network increases power demand on nodes closest to the access points as discussed in the prior topology analysis.

5. Security

Comprehensive security analysis depends on network configuration. As discussed earlier, the ability of nodes to enter and exit the network affects available levels of security. The requirement specifies a closed architecture, equating to a sub-router topology. Should a requirement arise to begin accepting out-of-network nodes, dedicated access points with firewall capabilities must filter traffic and process the nodes in a segregated manner until a network administrator adds the verified MAC address to an allowed address list.

6. Geolocation

Geolocation requires at least three stationary nodes that sense and report from a stationary standpoint. Feasibly, 802.11x access points or integrated routers could triangulate on a fourth node. However, if any node attempting to geo-locate is moving, measurement accuracy suffers. Lastly, processing time and power effects due to Geolocation place higher demands on the system.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY AND CONCLUSIONS

This chapter summarizes the steps used to evaluate 6LoWPAN against presumed user requirements and demonstrates how the same model can assess similar capabilities, or protocols, against similar requirements. Metrics used include throughput (bits per second), transmission power, receiver sensitivity power, antenna gain effects, internal noise factor, as well as size and weight. Associated monetary costs remain for follow on research. Finally, the model process used should prove applicable to similar communication-based requirements.

A. CONCLUSIONS

Desirability of 6LoWPAN comes from the just-enough power draw to accomplish a necessary mission resulting in significant savings on power and energy costs. 6LoWPAN also allows for interconnecting "things" at very little additional weight. Limitations of 6LoWPAN primarily include low throughput and short range. This thesis placed 6LoWPAN at the individual Soldier and possibly team or squad leader level in an operational setting leaving heavier backhaul capability to larger and more robust communications protocols. In an operational setting that often operates in a more static nature, 6LoWPAN interconnects "things" to any router access point. 6LoWPAN's security readily accepts AES-CCM-128 encryption, strong enough for the NIST to authorize transportation of SBU information. Security options available to 6LoWPAN include AES-CCM-128 encryption and though the specification does not discuss AES-CCM-256 encryption, it may be possible but requires additional testing. Security mechanisms most important to the Army depend on specific requirements. In the two associated scenarios, network topology affects energy and throughput values but does not affect attack resistance strength. Routing protocols and whether or not devices are dynamically or statically assigned affect resistance strength to the most common threats. Pre-assigned device, or node, addresses prevent most attacks involving malicious nodes. Operational employment of 6LoWPAN easily supports position and other small message size transmissions at sufficient ranges below the squad level. Functionality including

touch screen capabilities requires interfacing an external capability with additional processing and power. Employment of 6LoWPAN in a support setting shows strong potential for interconnecting any "thing" worthy of joining the larger network. Maximizing performance requires tradeoffs between range, device duration, and overhead. Throughput, security, routing options, and protocols all affect overhead amounts, or header length. Using 6LoWPAN devices to accomplish current functionality saves size and weight but sacrifices robustness of larger mission sets in different settings. Comparison against requirements established by the user community must ultimately determine sufficiency and feasibility of 6LoWPAN and whether or not the capability is worth acquiring. The notably small size, weight, and power of 6LoWPAN address the research question of whether or not 6LoWPAN and its usage against similar communication-based requirements merit additional exploration for the Army, and other services. This thesis demonstrates a method of evaluating feasibility of performance and security for use.

B. AREAS FOR FUTURE RESEARCH

This thesis covers a large amount of surface level assessment using various assumptions. Areas for future research include opportunities to refine the findings with empirical data or refined effects estimates. Additional areas of future research include application of the model to other communications-based requirements.

The first area of future research involves a deeper look at power drain given expected parameters facing 6LoWPAN operation. OLOS signal attenuation effects from various construction materials in the 802.15.4 range of operation could potentially couple with meshed networking to reboost signal strength but actual performance should be researched further. Urban and suburban multipath effects could be captured by Okamura-Hata empirical equations in anticipated usage environments to better estimate actual performance without empirical data from specific environments. Similarly, resiliency against additional threats may require increased security. However, increased security inevitably decreases available payload space for throughput or possibly more power consumption.

A second large area of future research includes detailed investigation of 6LoWPAN interfaces with existing or necessary capability. In this thesis, 6LoWPAN interfaces integrated access point routers. Any translation between protocols likely causes some amount of throughput and possibly latency degradation. A detailed study of the effects provides better fidelity to expected performance. Additionally, 6LoWPAN interfaces Nett Warrior. Nett Warrior offers capabilities far beyond 6LoWPAN alone. 6LoWPAN accomplishes what the SRW of the AN/PRC-152 accomplishes. The SRW SWAP characteristics of the handheld radio cannot be directly compared to 6LoWPAN, thus the additional capabilities of the AN/PRC-152, an already procured solution, could be compared. Other services without an already procured material solution, such as the United States Marine Corps, may gain from additional research in this area. Also, 6LoWPAN must interface a geo-positioning device such as the Army's DAGR. Therefore, additional research on the accuracy of 6LoWPAN geo-locating capabilities and associated overhead may render an external geo-positioning device unnecessary.

The amount of data aggregation power exchanged between interfaced devices also needs to be measured. For instance, a selectively capable smart phone device possesses processing power, screen displays, touch screen capabilities, and on-board storage capacity. Such a device similar to Nett Warrior's display device, may offer potential for similar functionality to Nett Warrior while benefitting from smaller size and weight. The duration capability of such a device to be commensurate with 6LoWPAN devices provides opportunity for future research. The resultant research could more appropriately compare 6LoWPAN with Nett Warrior at varying levels of employment. As observed in Figure 17, increasingly higher levels of command require significantly higher energy sources. Additionally, topology and routing impact energy source requirements. For instance, a squad configured into one single mesh may require a more distributed energy load balance below the squad leader, who in turn, would require a significantly higher energy source. Near-term research could determine power requirements at each level of the command given different network configurations set to match varying tactical configurations. Research is also necessary to determine whether or not on-board cache memory makes message disaggregation and re-aggregation at the physical layer sufficient

for required uses. This could allow larger messages with reasonable assurance of receipt by intended destination.

A third area of future research exists in material enhancements. Enhanced material densities of batteries offer longer durations at lighter weights. Increasingly smaller microprocessors and flash-memory devices offer smaller and lighter device dimensions thereby increasing the relative advantage over available capabilities. Additionally, antenna gain properties in this thesis assumed a worst-case dipole antenna. The dipole equation used typically applies to infinitesimally small antennas but other equations defining antenna gain differently or for different antenna patterns directly affect power and energy.

A fourth area of potential research lies in confirming all remaining assumptions made in this model. Confirming 5 nJ/bit for data aggregation requires empirical data that could potentially uncover further dependent variables. This research could also affect the research pertaining to 6LoWPAN interfaces. This thesis chose 1.2V rechargeable NiMH batteries for analysis. Other applications could require disposable batteries depending on transportability requirements. Such batteries typically discharge at a nominal 1.5 volts. Additionally, batteries draining at non-linear rates could affect analysis in ways warranting research.

A fifth area of research could encapsulate sufficiency from a user perspective given resultant throughput. Voice quality at rates less than 100 kbps requiring codec capabilities should be measured against subjectively defined acceptability. Similarly, future research could determine sufficiency of data messaging at maximum remaining payload in other applications.

A final area of potential research opportunities exists in applying the same model to different applications. Research could determine the suitability of this approach to model similar measures of performance and methods of measure applied to similar communication-based systems.

LIST OF REFERENCES

Alvestrand, H. 2004. "A Mission Statement for the IETF, RFC 3935." October 1. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3935.txt. Accessed January 10, 2015.

Agrawal, Dharma P., and Qing-An Zeng. 2014. *Introduction to Wireless and Mobile Systems*. 4th ed. Cengage Learning. MA.

Army Capabilities Integration Center–Research, Development and Engineering Command–Deputy Chief of Staff, G-4, U.S. Army. 2010. *Power and Energy Strategy.* White Paper, U.S. Army, Fort Monroe: U.S. Army TRADOC, pp6,8,12.

Barker, Elaine, and Allen Roginsky. 2015. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.* Special Publication, Computer Security Division, National Institution of Standards and Technology, Gaithersburg: National Institution of Standards and Technology.

Blanchard, Benjamin S., and Wolter J. Fabrycky. 2011. *Systems Engineering and Analysis.* 5th International ed. Upper Saddle River, NJ: Prentice Hall.

Buede, Dennis M. 2009. *The Engineering Design of Systems: Models and Methods.* 2nd ed. Hoboken, NJ: John Wiley & Sons.

Dawson, D. 2015. "Equipment Piece of the Week: Nett Warrior." *PEO Soldier Live.* August 17.

Duracell. 2016. OEM Technical Library. Accessed April 16, 2016. https://www.duracell.com/en-us/for-business/.

Ee, Gee Keng, Chee Kyun Ng, Nor Kamariah Nordin, and Borhanuddin Mohd Ali. 2010. "A Review of 6LoWPAN Protocols." Proceedings of the Asia-Pacific Advanced Network, Selangor, University of Malaysia, December 30.

Federal Communications Commission. 2016. "Telecommunications, Part 15- Radio Frequency Devices, Subpart A- General." *Electronic Code of Federal Regulations,* Title 47. Accessed March 28, 2016. https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet63/oet63rev.pdf.

Friedl, Karl E., and William R Santee. 2011. *Military Quantitative Physiology Problems: Problems and Concepts in Military Operational Medicine.* Fort Detrick, MD, December 1.

Gourley, Scott R. 2012. "Soldier Armed: Nett Warrior." *Association of the United States Army*, March.

Gutierrez, Jose A, David B. Durocher, Bin Lu, Ronald G. Harley, and Thomas G. Habetler. 2006. "Applying Wireless Sensor Networks in Industrial Plant Energy Evaluation and Planning Systems." Pulp and Paper Industry Technical Conference, Conference Record of Annual, Appleton, Eaton Corporation, June 18.

Harney, Robert C. 2004. *Sensor Elements—Part II Sensor Technologies.* Vol. 2, *Combat Systems*. Monterey, CA: Naval Postgraduate School.

Heinzelman, Wendi B., Anantha P. Chandrakasan, and Hari Balakrishnan. 2002. "An Application-Specific Protocol Architecture for Wireless Microsensor Networks." *IEEE Transactions on Wireless Communications* (IEEE) 1, no. 4 (October): 660-670.

Hersent, Olivier, David Boswarthick, and Omar Elloumi. 2012. *The Internet of Things: Key Applications and Protocols.* West Sussex: Wiley.

Housley, Russ. 2005. "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload, RFC 4309." The Internet Society. Herndon, VA. December 1. Accessed March 20, 2016. https://www.ietf.org/rfc/rfc4309.txt.

Hui, Jonathan W., and David E. Culler. 2008. "Extending IP to Low-Power, Wireless Personal Area Networks." *IEEE Internet Computing* (IEEE) 12, no. 4 (July): 37–45.

Hui, Jonathan, and Pascal Thubert. 2011. "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, RFC 6282. Internet Engineering Task Force, San Francisco. Accessed March 10, 2016. https://tools.ietf.org/html/rfc6282.

IEEE. 2011. *Standard for Local and Metropolitan Networks - Part 15.4 Low-Rate Wireless Personal Area Networks (LR-WPANs).* New York: IEEE Computer Society.

Jenn, David C., and Paul Sumagaysay. 2004. "Vulnerability of Wireless Networks in Indoor and Urban Environments." Faculty Publication, Monterey, CA: Naval Postgraduate School: 13.

Kushalnagar, Nandakishore, Gabriel Montenegro, and Christian Peter Pii Schumacher. 2007. "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals." Internet Engineering Task Force. Accessed March 10, 2016. https://tools.ietf.org/html/rfc4919.

Leland, Joe, and Issac Porche. 2004. *Future Army Bandwidth Needs and Capabilities.* Santa Monica, CA: Rand Corporation.

Lopez, C. Todd. 2010. *Nett Warrior to connect Soldiers to each other, leaders.* June 15. http://www.army.mil/article/40883/nett-warrior-to-connect-soldiers-to-each-other-leaders/ (accessed March 30, 2016).

Martinez, Jaacan, and Jose LM Lastra. 2011. "Application of 6LoWPAN for the Real-Time Positioning of Manufacturing Assets." *Interconnecting Smart objects with the Internet*: 3.

Montenegro, Gabriel, Nandakishore Kushalnagar, Jonathan W. Hui, and David E. Culler. "IPv6 over IEEE 802.15.4, RFC 4944." Internet Engineering Task Force, Fremont. Accessed March 14, 2016. https://tools.ietf.org/html/rfc4944.

National Security Agency. 2015. *Advisory Memorandum Information Assurance 02-15.* Advisory, July.

Nikander, Pekka, James Kempf, and Erik Nordmark. 2004. "IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756." Internet Engineering Task Force, Fremont. Accessed March 1, 2016. https://www.ietf.org/rfc/rfc3756.txt.

NXP Laboratories. 2013. *Calculating 802.15.4 Data Rates.* South Yorkshire, November 5.

Olsson, Jonas. 2014. *6LoWPAN demystified.* Texas Instruments. Dallas, TX: Texas Instruments Incorporated, October 1.

Pedram, Massoud, and Qing Wu. 1999. "Design Considerations for Battery-Powered Electronics." P*roceedings of the 36th annual ACM/IEEE Design Automation Conference, Los Angeles*, Association for Computing Machinery, June 1.

Rappaport, Theodore S. 2002. *Wireless Communications, Principles and Practice.* 2nd ed. Upper Saddle River, NJ: Prentice Hall.

Rockwell Collins. 2016 *HNV-660 Defense Advanced GPS Receiver.* March 25. https://www.rockwellcollins.com/Data/Products/Navigation_and_Guidance/GPS_Devices/Defense_Advanced_GPS_Receiver_-DAGR.aspx (accessed March 25, 2016).

Sarto, Jen. 2016. *Zigbee vs 6LoWPAN for Sensor Networks*. Accessed February 23, 2016. https://www.lsr.com/white-papers/zigbee-vs-6lowpan-for-sensor-networks.

Sastry, Naveen, and David Wagner. 2004. "Security Considerations for IEEE 802.15.4 Networks." *3rd ACM workshop on Wireless Security (WiSe), Berkeley*, Association for Computing Machinery, October 1.

Sikora, Axel, and Voicu F. Groza. 2005. "Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band." *IMTC 2005- Instrumentation and Measurement Technology Conference, Ottaw*, University of Ottawa, May 16.

Stallings, William. 2014. *Data and Computer Communications.* 10th ed. Upper Saddle River, NJ: Pearson.

Thales Defense & Security. 2016. *AN/PRC-154 Rifleman Radio.* April 1. http://www.thalescomminc.com/content/anprc154family.aspx (accessed April 1, 2016).

Toscano, Emanuele, and Lucia Lo Bello. 2012. "Scheduling for IEEE 802.15.4 Industrial Wireless Sensor Networks." *IEEE Transactions on Industrial Informatics* (IEEE) 8, no. 2 (May): 337-348.

U.S. Army. 1991. *Observed Fire.* Electronic. Washington, DC: Army Publishing Directorate, July 16. Accessed on April 6, 2016.

———. 2007. *The Infantry Rifle Platoon and Squad.* Washington, DC: Government Printing Office, March 28.

Vines, Russell D. 2002. *Wireless Security Essentials.* Indianapolis: Wiley Publishing, Inc.

Wheeler, Andrew. 2007. "Commerical Applications of Wireless Sensor Networks Using Zigbee." *IEEE Communications Magazine*, no. 4 (April): 70–77.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California