NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RADIO FREQUENCY FOOTPRINT COMPARISON OF THE TLS AND MLS SECURITY PROTOCOLS

by

Ching-Ting Yuan

December 2023

Thesis Advisor: Britta Hale
Co-Advisors: Joseph W. Lukefahr
Aurelio Monarrez Jr.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
RADIO FREQUENCY FOOTPRINT COMPARISON OF THE TLS AND MLS SECURITY PROTOCOLS

5. FUNDING NUMBERS

6. AUTHOR(S) Ching-Ting Yuan

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.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

This thesis presents an analysis of the effects on radio frequency (RF) of secure channel establishment methods, focusing on the comparison between Transport Layer Security (TLS) and Message Layer Security (MLS) protocols. The study explores the impact of these protocols on RF footprint and network utilization in wireless communications, especially under varying message sizes. Simulations were conducted to examine the channel power, network utilization, and spectrogram analysis of both protocols. The results highlight TLS's higher power output and network bytes requirement compared to MLS. The findings also reveal that TLS also exhibits increased RF footprint over MLS, an important consideration for military operations emphasizing Low Probability of Detection (LPD) and Low Probability of Intercept (LPI). This research contributes to the understanding of secure communication protocols in RF environments, offering insights into their practical applications and paving the way for future work in optimizing secure communication strategies in wireless networks.

14. SUBJECT TERMS Message Layer Security, MLS, Transport Layer Security, TLS, radio frequency, RF, footprint, data transmission	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

RADIO FREQUENCY FOOTPRINT COMPARISON OF THE TLS AND MLS SECURITY PROTOCOLS

Ching-Ting Yuan
Lieutenant, United States Navy
BSE, Walla Walla University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2023

Approved by: Britta Hale
Advisor

Joseph W. Lukefahr
Co-Advisor

Aurelio Monarrez Jr.
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis presents an analysis of the effects on radio frequency (RF) of secure channel establishment methods, focusing on the comparison between Transport Layer Security (TLS) and Message Layer Security (MLS) protocols. The study explores the impact of these protocols on RF footprint and network utilization in wireless communications, especially under varying message sizes. Simulations were conducted to examine the channel power, network utilization, and spectrogram analysis of both protocols. The results highlight TLS's higher power output and network bytes requirement compared to MLS. The findings also reveal that TLS also exhibits increased RF footprint over MLS, an important consideration for military operations emphasizing Low Probability of Detection (LPD) and Low Probability of Intercept (LPI). This research contributes to the understanding of secure communication protocols in RF environments, offering insights into their practical applications and paving the way for future work in optimizing secure communication strategies in wireless networks.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AS Authentication Service

C2 Command and Control

DS Delivery Service

EM Electromagnetic

IETF Internet Engineering Task Force

IoT Internet of Things

IP Internet Protocol

LPD Low Probability of Detection

LPI Low Probability of Intercept

MLS Message Layer Security

OSI Open Systems Interconnection

RF radio frequency

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

This thesis project, spanning several months, has been a transformative journey. Initially, I felt overwhelmed and intimidated, especially when struggling to find a suitable topic. However, through this process, I've grasped the understanding of the important contribution my thesis may have on real world applications. I am immensely grateful for the patience and support of my advisors throughout this journey.

I would like to express my deepest gratitude to my thesis advisor, Dr. Britta Hale, for her invaluable guidance and expertise. Her knowledge and insights were instrumental in sparking my interest in this topic, making this thesis a possibility. I deeply respect her steadfast commitment and professionalism. It has been an honor to work under her mentorship.

My sincere thanks also go to my co-advisors, Mr. Joe Lukefahr and Mr. Aurelio Monarrez. Their approachability and assistance were crucial in overcoming the numerous challenges I encountered. The advice and insights they provided will have a lasting impact on my academic and professional journey.

I am equally thankful to Mr. George Lober and Ms. Lauren Callihan at the Graduate Writing Center. Their expertise made the daunting task of writing far more manageable. I am also amazed at their skill in deciphering my drafts and thankful for their guidance in steering my writing towards a coherent and understandable thesis.

I am grateful for the camaraderie and insights shared with my classmates. Learning alongside them has been an enriching experience, contributing significantly to my growth and enjoyment of the rigorous program at NPS.

Finally, I must acknowledge the love and support of my friends and family. Studying at NPS and being close to my hometown has been a blessing, allowing me to balance academic rigors with cherished moments with loved ones. And for the new friends I made during this journey, thank you for the wonderful memories. Let's stay in touch!

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Traditionally, how we think of data communication from one system to another has mostly been divided into two parts: the radio frequency (RF) as the waveform that carries the data between the systems, and the protocol that holds the data packets with actual communications within them. In reality, data communication should be considered as one piece, i.e. that the need to transfer data itself incurs a cost on the radio frequency footprint. The amount of RF required to ensure the protocol can connect and successfully send packets of data is important to consider from a networking perspective. Under traditional wireless data transmission, RF *is* the essential means of transportation for data. Its signal strength, waveform, and behaviors under a given environment can affect the transmission success or failure of data going from sender to receiver.

During wireless communication, the sender and receiver are not directly connected, meaning data passes through an open environment, vulnerable to interceptions. Security protocols ensure confidentiality, availability, and integrity. One widely-accepted system is the Internet Protocol (IP) that aids devices in communication. The Transmission Control Protocol (TCP) ensures data packet delivery. Security protocols like Transport Layer Security (TLS) and the emerging Message Layer Security (MLS) enhance data safety. The latter, unlike TLS, can secure group communications involving more than two entities.

This thesis project is to compare the established TLS with the increasingly popular MLS. Research object comparison involves analyzing the RF footprint under different data packet encryption, such as MLS over TCP versus TLS over TCP, and measuring RF emissions for optimal data transmission conditions. The research sets up tests with these protocols to ascertain the best communication quality in a given environment.

Research objectives being pursued in this work includes:

- Analyzing what the RF footprint looks like for different data packet encryptions such as MLS over TCP and TLS over TCP.
- Measuring RF emission for an optimum condition that allows data to transmit between two systems securely and efficiently.

This thesis explores the relationship in which wireless data transmission inherently impacts the RF footprint. It analyzes and compares the behavior of a current and common protocol for protecting data, TLS, and the new end-to-end encryption protocol, MLS, to aid in understanding of how security protocols affect RF footprint. By conducting data transmission tests using prototype applications for TLS over TCP and MLS over TCP, and collecting RF measurement such as power utilization and data traffic activity such as network utilization, a comparison on the performance of the two protocols is observed. The findings reveal that MLS, in comparison to TLS, exhibits distinct RF emission characteristics, such as less power output and less bytes transmitted. These insights shed light on the RF implications of different security protocols and pave the way for further considerations in wireless communications design while balancing efficiency and security.

1.1 Application in Military Operations

In military operations, the strategic significance of communication under constraints such as Low Probability of Detection (LPD) or Low Probability of Intercept (LPI) cannot be overstated. These criteria are often essential for the success of sensitive operations [1], where maintaining Command and Control (C2) between decision-makers and field operatives is crucial. It directly impacts operational security by safeguarding sensitive data from enemy detection. This includes protecting crucial information like target coordinates, mission objectives, or identities of operatives. The ramifications of such data falling into adversarial hands are severe, potentially compromising mission integrity and risking lives. Unauthorized access to this information, whether through intentional espionage or accidental leaks, can lead to disastrous consequences, including mission failure, exposure of covert operations, and endangerment of personnel. The use of RF signals that are brief and limited in spectrum spread is a key tactic in minimizing detection or interception risks [2]. However, the RF costs incurred by networking protocols that are sent using such signals is less understood.

Enhancing cybersecurity and protecting secrecy are two high-stake tasks in the field of wireless communication. With better understanding of the nuances of RF footprints in secure communication protocols, this thesis project aims to explore the interrelationship between RF and encryption protocols. It will identify factors that contribute to maintaining more secure communications in scenarios requiring LPD or LPI.

1.2 Thesis Organization

The following chapters are organized as follows:

Chapter 2 focuses on the key concepts of RF, TCP, TLS, MLS, and how data flows from one wireless device to another wireless device.

Chapter 3 discusses the methodology for conducting the tests needed for this thesis. This chapter will include explanation of the hardware and software used in the testing.

Chapter 4 analyzes the information collected from the testing, and then discusses the findings.

Chapter 5 draws conclusions based on the presented results and findings. Offers suggestions for future work in this area of study.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background Research

In order to understand how information flowing from one device to another wirelessly, both RF and network architecture will be explored further in this chapter. Beginning with the understanding of RF and the principles underlying wireless transmission, and shifting discussion to network architecture and various network protocols such as TCP [3], TLS [4], and MLS [5] that provide reliable and secure communication over a computer network.

The exploration of the interrelation and the effects of radio frequency and data transmissions is not common. The existing literature predominantly offers segmented views. Engineers and scholars predominately concentrate on either the RF aspects of wireless communication or the properties of the data transmission protocol at the network layer. Currently the studies on the specific behavior of how various data transmission changes in the RF domain is sparse. Most academic writing such as textbooks on RF by Weisman [6], or wireless data communication by Stallings [7], break down both the theory of how a signal traverses through the environment, and the components of antennas and de/modulators. However, such writing does not go beyond interpreting the signals into 1's and 0's and the various protocols within the network devices . At best, research related to RF in the field of wireless communication covers the Physical layer and Data Layer, but is limited on research beyond the Data Layer. For example, an article written by Radhakrishnann and others [8] discussed Inter-Satellite Communication from the view of Physical layer, Data Layer, and fringe of Network Layer; however, the article does not go further into Network layer and Transport layer where security and transmission protocols take place. Therefore, this thesis will attempt to explore the effects of RF on wireless data transmission beyond the Network Layer.

In the theory of Networks, for devices to send and receive data packets, an address system is necessary for data to travel to the correct destination. The IP is a standard format in the areas of networking that is created to help devices communicate data between one another. Devices with proper IP information will then be able to send data via transport protocols. One of the most common and reliable transport protocols is the TCP. TCP, using the three-way handshake, is a way for data packets to be handled and delivered correctly to the intended

recipient. Once the transport protocol is established, the data is ready for transmission over the network and ready to be understood in the application layer. TLS, used in sending emails or performing banking transactions,is a common Internet security protocol for maintaining privacy and data security between the sender and the receiver; because TLS can encrypt the data, authenticate the parties exchanging the data, and maintain integrity of the data. Another security protocol that is gaining traction is the MLS protocol. Different from TLS, MLS can provide secure group communication among more than two entities [9].

To provide a general concept of a communication system, Figure 2.1 focuses on several elements.

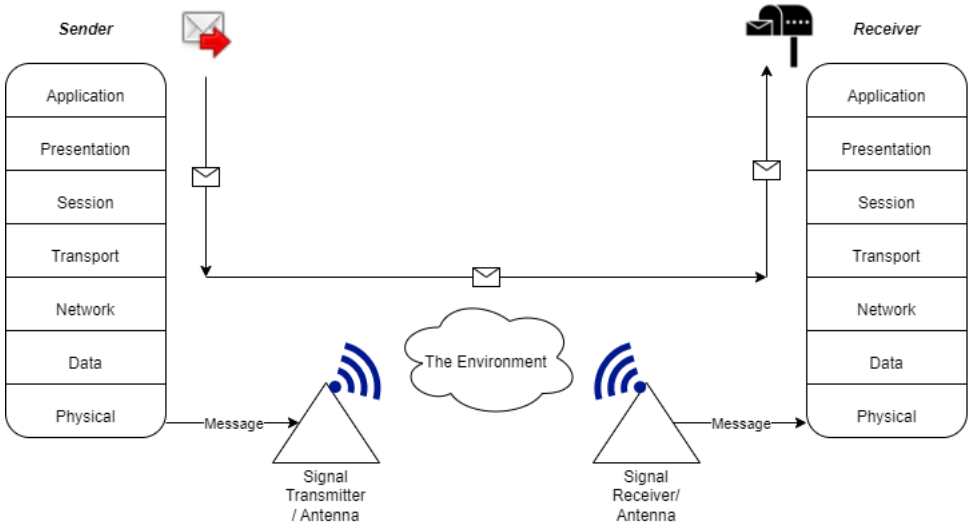

Figure 2.1. General Wireless Communication Concept. Adapted from [7], [8], [10].

Beginning with the data source, the data can come from any device that emits a signal. A few examples include a radio, laptop, or walkie-talkie. The information being transmitted by the devices can be analog or digital, and it can be voice or data. In a controlled environment, the information leaving the device for an intended destination is encrypted, and only the intended recipient has the code to decrypt the message.

2.1 Radio Frequency

According to NASA, RF is a type of an Electromagnetic (EM) radio waves in the atmosphere that oscillates through the environment. The oscillation is described as frequency, which is

a rate of oscillation cycles per second, known as Hertz. The range of RF goes from 3kHz to 300GHz [11]. The lower spectrum is characterized by longer wavelength and limited bandwidth; thus, the wave carries less data. The higher spectrum, on the other hand, has a shorter wavelength and more bandwidth, which means the wave can carry more data.

The data that an RF carries is encoded into the electromagnetic waves in the forms of bits denoted in 1's and 0's. The transmission of the strings of waves traverses through the atmosphere of various noise and other disturbance in the environment. The receiver calibrated to the appropriate RF settings and equipped with the correct decoding methodology can demodulate the encoded data from the waves. This technique of transmitting data via RF is used in many modern day applications using wireless data communication, such as texting between mobile phones, controlling various Internet of Things (IoT) devices, and browsing the internet using Wi-Fi.

Radio frequency (RF) is a fundamental concept of wireless data transmission. The basic hardware components shown in Figure 2.2 to make wireless communication work are an antenna, amplifier, filter, modulator, and a device with data. A device sending the data uses modulation to encode the data into electric signals that go through the amplifier to strengthen the signal before the signal carries the data into the space through the antenna as airborne waves. On the receiving end, the inverse process is performed as the antenna captures the airborne waves carrying data, amplifies the signals that are received by the receiving device, which then demodulates the electric signal to restore the data back to its original form.

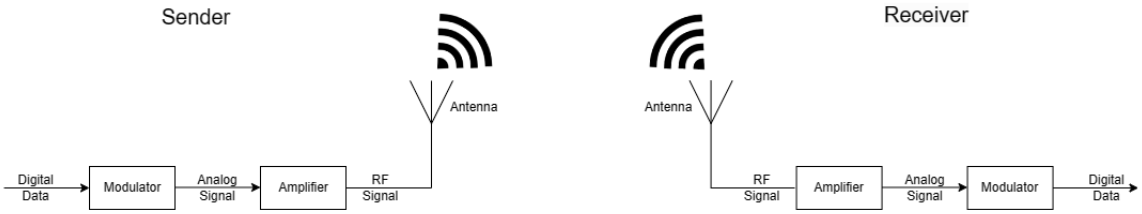

Figure 2.2. Hardware Components of Wireless Communications. Adapted from [6].

The next component of the communication concept is the signal transmitter. In the case of terrestrial microwave transmission, it is known as the antenna. A radio antenna's primary

function is to transform the energy it receives, which comes as a radio frequency alternating current signal, into an electromagnetic wave. This wave can then traverse the distance separating the transmitting and receiving antennas as shown in Figure 2.3 [12]. The reverse steps are applied to the receiving antenna to extract the data from the signals.

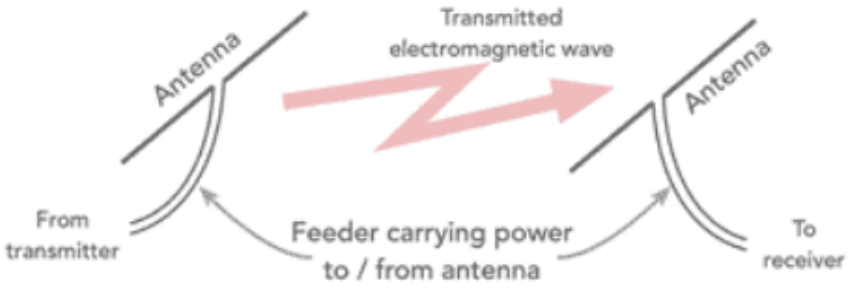

Figure 2.3. Antenna Theory. Adapted from [12].

An essential aspect of RF technology is understanding the power levels of signals, typically measured in dBm. dBm is an abbreviation for "decibels relative to one milliwatt," where one milliwatt (mW) is defined as the reference power level. This logarithmic scale is crucial in the field of telecommunications because it allows for a convenient representation of very large or small power levels, which are common in RF communications [13].

The use of dBm in RF is largely due to its ability to represent power levels in a manageable way. RF signals often vary greatly in power, ranging from very strong signals (like those close to a radio transmitter) to extremely weak ones (like those at the edge of a cell phone's range). The logarithmic nature of the dBm scale compresses this wide range of values into a more readable and comparable format [14].

Understanding the conversion between dBm and milliwatts is vital for practical applications. The formula to convert dBm to milliwatts is:

$$P_{\mathrm{mW}} = 1\mathrm{mW} \times 10^{\left(\frac{P_{\mathrm{dBm}}}{10}\right)} \text{ [15].}$$

where P_{mW} is the power in milliwatts and P_{dBm} is the power level in dBm. This conversion is crucial in scenarios where you need to know the actual power in milliwatts, such as when

ensuring that a transmitter complies with regulatory limits or when assessing the power consumption of a device.

Research papers and articles often delve into more specific aspects of RF communication, such as advanced modulation techniques [16], antenna design [17], or the effects of signal interference [18]. While the fundamental relationship between dBm and milliwatts is a basic concept not typically the subject of research papers, understanding dBm and its relationship to milliwatts is a cornerstone in RF technology. It provides a practical and effective way to measure and compare power levels, which is integral to designing, testing, and operating RF communication systems.

For this thesis, the power levels (in milliwatts) will be analyzed and compared between TLS and MLS in Chapter 4. We will briefly address RF affects again in Chapter 2.4 after discussion of networking layers. The background on RF is relevant to understanding the various components and influencing factors of data communication.

2.2 Network Communication

The Open Systems Interconnection (OSI) framework can be used to describe how information is traversed through the network. The OSI model helped set a standard for network communication and allows network engineers and manufacturer to design devices that can communicate based on the standardized architecture [19]. The OSI model is a 7-layer network architecture consisting of the following layers: Physical, Data, Network, Transport, Session, Presentation, and Application layers.

According to the OSI reference model:

1. Physical Layer: The foundational layer of the OSI model, the Physical Layer, is concerned with the raw transmission of unstructured data over a physical medium [10]. It defines the hardware components of networking, including cables, switches, and network interface cards. Specifications related to electrical voltages, pin layout of connectors, and signal frequencies are outlined at this layer. It ensures data, in the form of bits, traverses from one device to another without errors, but this layer does not manage error correction itself.

2. Data Link Layer: This layer bridges the physical hardware to the software components of a network. The Data Link Layer is bifurcated into two sub-layers: Logical Link Control

(LLC) and Media Access Control (MAC) [10]. While LLC offers flow control and framing, MAC provides a unique identifier (MAC address) for each device and manages access to the shared medium. Essential functions like error detection (but not correction) and frame synchronization are managed at this layer.

3. Network Layer: Acting as the linchpin for data routing and forwarding, the Network Layer is indispensable for large-scale networks, especially the internet. Here, logical addressing (e.g., IP addresses) and path selection are determined [10]. Devices like routers operate at this layer, leveraging routing protocols (like OSPF and RIP) to determine the most optimal path for data packet traversal.

4. Transport Layer: Ensuring data integrity and delivery from the source to the destination is the purview of the Transport Layer [10]. Two of the most widely known transport protocols are TCP and TCP. While TCP ensures reliable data delivery through error correction, acknowledgments, and sequencing, TCP offers a faster but potentially less reliable connectionless communication. Flow control, segmentation, and reassembly are vital functions at this juncture.

5. Session Layer: As the name implies, the Session Layer manages sessions or connections between applications on different devices. It ensures data consistency throughout a session and can establish, maintain, or terminate connections [10]. Furthermore, it manages dialog control, determining whether communication should proceed in half-duplex or full-duplex modes.

6. Presentation Layer: Acting as a translator, the Presentation Layer addresses data format inconsistencies, ensuring the data sent and received is in a format both sender and receiver can understand [10]. It is here that encryption, decryption, and data compression mechanisms come into play, providing a transparent transition of data from the lower layers to the Application Layer.

7. Application Layer: At the pinnacle of the OSI model, the Application Layer interfaces directly with end-user applications [10]. It provides diverse network services to these applications, ensuring effective communication, data transfer, and overall network utility. It is important to know that this layer is not to be confused with applications like web browsers. Instead, this layer encompasses various network processes that cater to end-user

functions.

A scenario of how this OSI model is applied in a real world communication would be Alice and Bob sending an email to one another. Practical Networking illustrated the steps for these layers in following scenario [20]:

1. Application Layer (Layer 7): Alice opens her email client and composes a message for Bob. The email client, functioning at the Application Layer, provides a user interface for Alice to interact with the networking services. Once she clicks "Send," the email data is passed down to the Presentation Layer.

2. Presentation Layer (Layer 6): This layer ensures the data is in the right format. It might encode the email's text using a standard like UTF-8 and ensure attachments are properly encoded in MIME format. If Alice's email client has encryption like S/MIME set up, the email content is encrypted here.

3. Session Layer (Layer 5): The email client establishes a session with the email server using protocols such as IMAP or SMTP. This layer ensures that the connection to the server remains intact while the email is being transferred.

4. Transport Layer (Layer 4): The data is segmented into smaller packets to be sent across the network. If the email client uses a reliable protocol like TCP (common with SMTP), it ensures the data's reliable delivery, sequencing the packets and preparing acknowledgments for received data.

5. Network Layer (Layer 3): The IP address of the email server is determined and the packets are assigned this destination IP. The Network Layer on Alice's computer decides the best path to take to reach the server, often involving multiple routers. At this layer, the router reads the IP address and forwards packets accordingly.

6. Data Link Layer (Layer 2): Here, the data packets are framed and prepped for the journey. The MAC address of Alice's gateway, usually her router, is determined. The packet, now with both MAC and IP addresses, is sent over the local network. Each switch or hub on the local network that the packet encounters uses this layer to determine where to forward the packet.

7. Physical Layer (Layer 1): The digital data is converted into electrical, optical, or radio wave signals to traverse the medium, be it Ethernet cable, fiber optics, or Wi-Fi. On Alice's end, this process involves her Ethernet card sending electrical pulses through a cable or her Wi-Fi card transmitting radio waves.

Now, the email travels over the internet, passing through various devices, possibly including switches, routers, and servers. Each of these devices only processes the layers relevant to its function. For instance, routers primarily work at the Network Layer.

Once Bob's email server receives the email, the process is reversed, moving from the Physical Layer back up to the Application Layer:

7. Physical Layer: Bob's email server receives the electrical/optical signals representing the email data.

6. Data Link Layer: The server confirms the MAC address and checks for errors in the data frames.

5. Network Layer: The server reads the IP address to ensure the packet has arrived at the right destination.

4. Transport Layer: The server sequences the packets as needed, acknowledging their receipt.

3. Session Layer: A session between Bob's email server and his email client is established.

2. Presentation Layer: The server decodes the data, translating it into a readable format. If the email was encrypted, it is decrypted here.

1. Application Layer: Finally, the email appears in Bob's email client, ready for him to read.

In essence, the OSI model has been pivotal in creating a standardized approach to network communication. By segregating vast and intricate network functionalities into seven distinct layers, the OSI model facilitates a modular approach to network design, where issues in one layer can be resolved without tampering with the other layers. This compartmentalization is instrumental for network troubleshooting, design, and understanding. The concept of the OSI model is an essential background for this thesis because of the importance in understanding how data is transmitting and received from one device to another.

2.3 Security Protocols

With respect to data transmission, the encryption mechanism is done in the form of a protocol. The two types of protocols considered for this research are the Transport Layer Security (TLS) [4] and Message Layer Security (MLS) protocols [5]. They are selected because TLS is currently one of the most commonly used secure-channel establishment protocols, and MLS is a growing concept in communication protocol, especially for a group of users needing to communicate in the same session [21]. Therefore, the data collected from running both TLS and MLS may show significant differences in how both protocols will affect their RF footprints.

Transport Layer Security (TLS)

TLS traces its roots back to Secure Sockets Layer (SSL), a protocol developed by Netscape in the 1990s to secure communications over the nascent World Wide Web. SSL went through several versions, with each iteration addressing vulnerabilities and incorporating stronger cryptographic practices. Recognizing the broader application and necessity of the protocol beyond just web browsers, the Internet Engineering Task Force (IETF) [22] took over the development, renaming it TLS and releasing TLS 1.0 in 1999 [23].

Over the years, TLS has seen multiple versions, with TLS 1.3 being the latest as of the last update in 2018. Each version has brought improvements in efficiency, security, and speed.

At its core, TLS provides a secure channel between two communicating parties (typically a client and a server) [24]. The protocol ensures data integrity, confidentiality, and authentication. It operates above the transport layer (like TCP) and below application protocols (such as HTTP) [25], effectively encapsulating application data and ensuring it reaches its destination securely.

The Transport Layer Security (TLS) protocol is a widely standardized protocol used today and designed to provide encryption, authentication, and integrity of data [26]. Once a TLS connection is established, all data exchanged is encrypted, ensuring that eavesdroppers cannot decipher the contents. This secure connection is achieved using symmetric encryption, where both parties share a secret key. TLS uses digital certificates to authenticate communicating parties. Typically, servers are authenticated to ensure clients are connecting to legitimate servers and not imposters. In certain scenarios, client-side authentication is also

employed; when both authentications are communicating with each other. This process are often referred to as mutual authentication. Data integrity in TLS, "ensures that the data received by the recipient is exactly the same as the data sent by the sender" [27] with no alterations, deletions, or insertions. Ensuring integrity is crucial to prevent various kinds of attacks, such as man-in-the-middle attacks, where an attacker might intercept and modify the data in transit.

TLS provides encryption, authentication, and data integrity with the two main components: handshake protocol and record layer protocol [26]. Utilizing the ideas of public and private keys, the two entities will be able to communicate information that can only be decrypted by the intended person(s) [4]. The TLS handshake protocol occurs when the sender initiates and ultimately establishes a secure connection with the receiver. The communication sequence starts with authentication of the communicating parties, by exchanging keys, followed by certificate request and verification, and lastly both the sender and the receiver will negotiate a cipher mode to start their secured communication and parameter. Figure 2.4, depicts an interpretation of the activity of a TLS handshake [28].

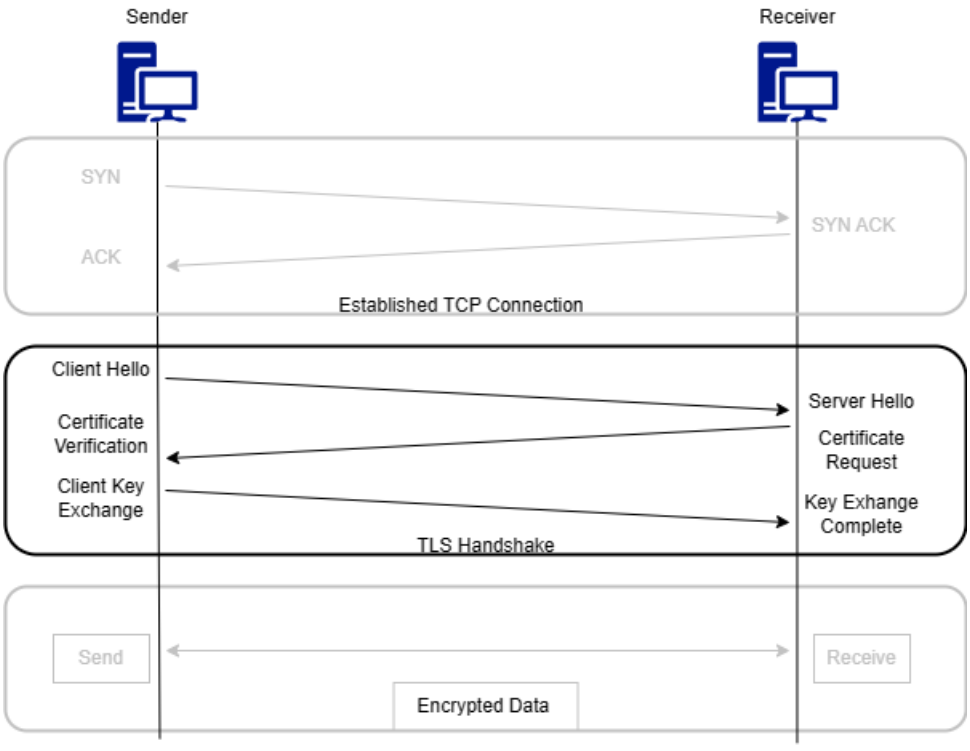

Figure 2.4. TLS Handshake Protocol. Adapted from [28].

The TLS handshake establishes a secure channel for communication, while the TLS record layer protocol protects the communication traffic between sender and receiver [29]. In the record layer, the data is segmented into manageable blocks and authenticated and encrypted. Finally, a record header is added to each segment, which includes necessary information such as the TLS version and the length of the data, thereby completing the formation of the secure packet [4], [30].

With TLS, there is a secure channel from the client and the server (but not end-to-end between clients). Furthermore, the use of digital certificates ensures that users are connecting to genuine servers and, if mutual authentication is used, that servers are connecting to genuine clients. TLS also provides forward secrecy, so even if keys are compromised, data from past sessions remains safe.

In the case where more than two entities (i.e., one sender and one receiver) need to communicate securely together using TLS protocol will require a series of pairwise handshakes within the secure channel. TLS facilitates these handshakes, ensuring each pair of individuals can securely exchange their public keys and agree on encryption parameters. As seen in Figure 2.5, for a secure communication among five people using TLS, a total of ten TLS handshakes is required in order for all five people to communicate securely with each person receiving the other four people's public key, as well as the negotiated encryption parameter for this particular secure channel. The equation to describe this key exchange can be denoted as N(N-1)/2. When the same principle is applied for a very large group of a thousand, the number of keys required would be 499,500 TLS handshakes.

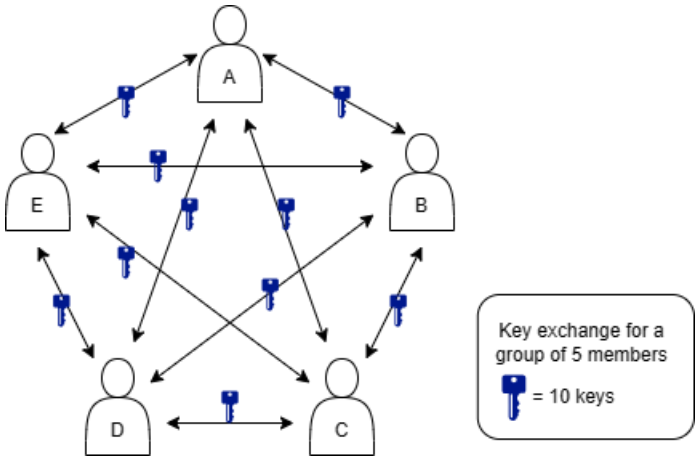

Figure 2.5. Required Handshakes with Symmetric Keys. Adapted from [31].

The number of key exchanges required is one of the drawbacks of TLS because it drastically increases the amount of data to transmit between the sender(s) and the receiver(s) within a secured environment, which results in latency. It can also potentially introduce vulnerabilities if the keys or the Certificate Authority are not managed properly.

This thesis will utilize the specifications set by the IETF community and implement TLS libraries in the experiment of the wireless data transmission using TCP, which is also a standardized method for establishing network conversation and maintaining a network [4].

Messaging Layer Security (MLS)

The other form of data transmission that will be used in this thesis was developed less than a decade ago. This method is the Message Layer Security (MLS) protocol which was standardized by the IETF in July 2023. Its advantages are starting to gain traction. The basic idea is that MLS encrypts the message itself, rather than the transport path of the data [32]. A deeper understanding of the MLS protocol will provide a valuable comparison of how data transmission may affect the RF footprint versus using TLS.

At its essence, MLS is designed to provide end-to-end encryption for group messaging systems, ensuring security even in the face of members joining or leaving the group. Unlike conventional methods that might require updating and sending new keys to every member when someone joins or leaves, MLS efficiently handles these changes, ensuring forward and backward secrecy without extensive computational costs.

A primary concept in MLS is the use of a "group state," which includes the set of group members and a binary tree of node keys for tracking members. These tree node keys allow members to compute a shared group secret. When a change (like adding or removing a member) occurs, MLS processes it through a series of proposals and commits to update the group state.

One of the initial benefits of MLS is in the use of messaging and cloud applications and providing a fully end-to-end security for user communication that goes through a server or a cloud to reach the intended recipient. With MLS, the server distributing the message will not be able to decrypt the message. In the case of adversarial attacks on the server, the secured group communication through those servers will not be compromised. The concept of MLS is illustrated in Figure 2.6.

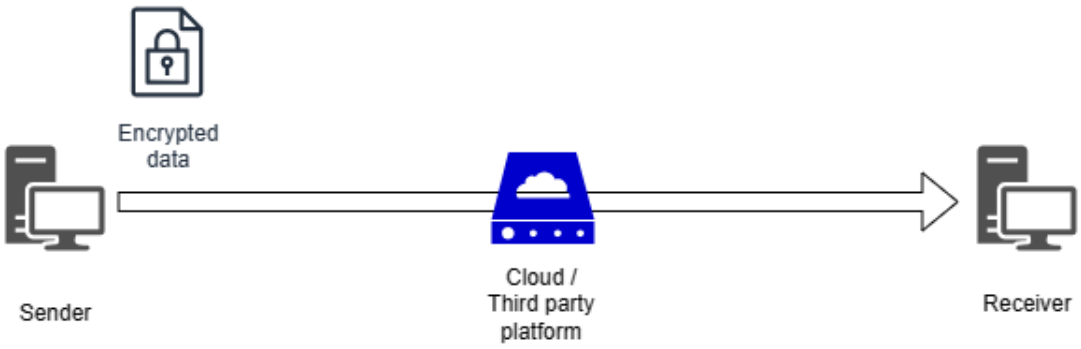

Figure 2.6. Message Layer Security. Adapted from [33].

MLS operates with two services provided: Authentication Service (AS) and Delivery Service (DS) [34]. The authentication service allows the group members to verify the credentials of other group members or incoming group members. The delivery service is how MLS messages are sent to all members of the group. The secure communication group via MLS has the ability to add additional members who are initiated by the current member(s) in the group, updating and distributing the keys to the group, and removing members, and then following up and distributing an updated key to the remaining members [35].

One of the advantages of MLS is the key distribution, which requires much less overhead than that of TLS. Similar to TLS, each member will hold their own individual public and private keys. In addition, MLS uses a structure in which all members of the group also hold a group key that allows them to encrypt and decrypt the messages within the group. However, the advantage of MLS structure is that it does not require handshakes with each and every member like the TLS protocol. The group key management is used to maintain the secrecy of the group (Figure 2.7 [36]); and provides a new group key to authorized members upon any addition, removal, or update of members. This key management strategy reduces the amount of data sent for authentication alone.

While TLS is designed to encrypt messages between one client and one server, MLS is designed to encrypt messages among groups of devices, where a group can have more than two members. MLS can support client/server or request/response architectures, as with TLS, but it can also support publish/subscribe architectures, which are more commonly used within groups of autonomous systems. For example, as one possible DS implementation,

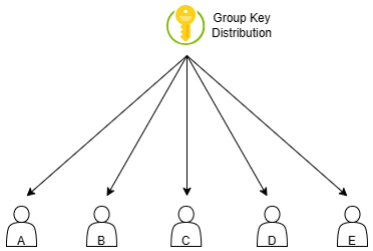

Figure 2.7. Binary Tree method for Key Distribution. Adapted from [36].

the members of the group act like a subscriber and a leader as the group administrator who publishes information on the shared key for the group. Regardless of how messages are distributed, upon receiving the information on a new group key, all members ratchet forward on their current keys to maintain group communication. One of the requirements for MLS, according to the IEFT document, is the ability to ensure key packets are sent and received in order. One method to consider is establishing a TCP connection which provides ordered and reliable delivery. Figure 2.8 interprets the MLS architecture via TCP connection based on the IETF's publication on MLS [21], [32].

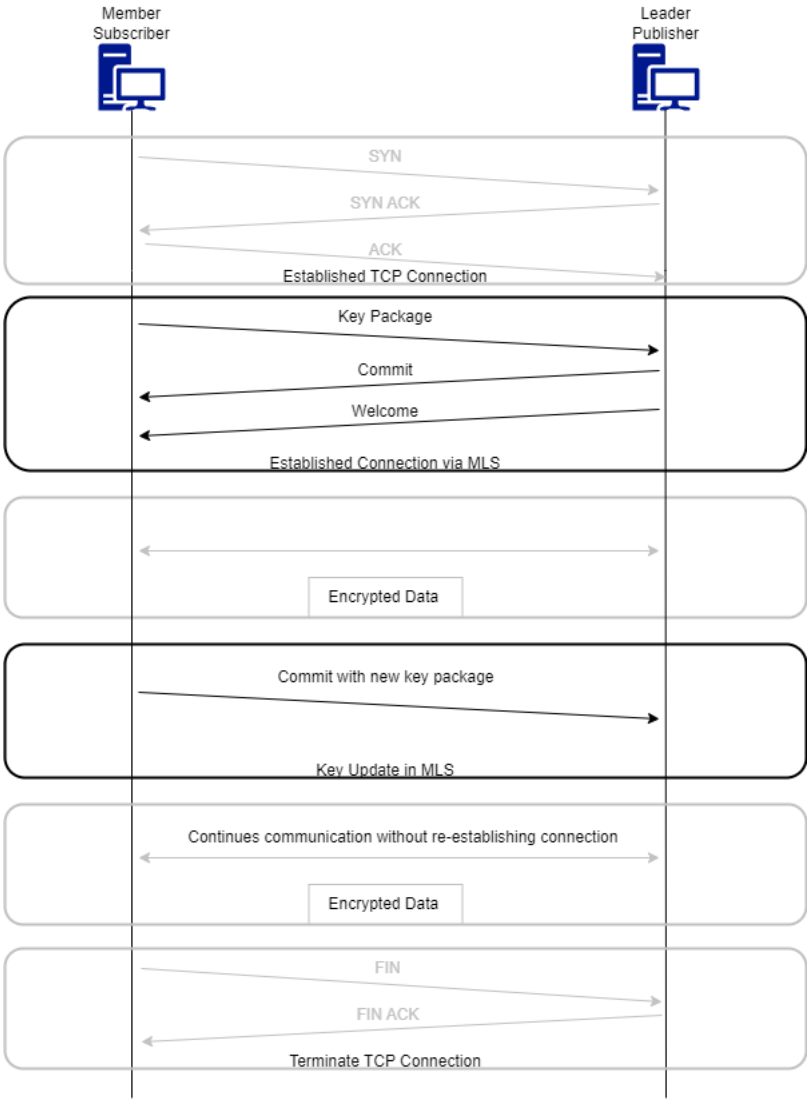

Figure 2.8. MLS Concept.

2.4 Layer 4 Protocols

Transmission Control Protocol

As the need for a standardized network protocol became apparent with the growth of early computer networks, the U.S. Department of Defense commissioned the development of the Internet Protocol Suite, commonly referred to as TCP/IP [37]. TCP, which stands for Transmission Control Protocol, was developed alongside the Internet Protocol (IP) by Vint Cerf and Bob Kahn, with the first paper published in 1974 titled "A Protocol for Packet Network Intercommunication" [38].

TCP is a connection-oriented protocol operating in the transport layer of the internet protocol suite. Its primary role is to guarantee that data bytes are transmitted in sequence, free from errors, between applications on hosts that interact over an IP-based network. [7] [39].

According to Stallings's Data and Computer Communications [7], there are several foundational concepts of a TCP:

- Segments: Data is split into packets, known as segments, for transmission. Each segment is assigned a sequence number for orderly reassembly [40].
- Flow Control: This ensures that data senders do not overwhelm receivers by transmitting too much, too quickly. The receiving side provides "window" size information, which specifies how much data it can accept.
- Error Checking: TCP uses a checksum for this, ensuring data integrity.

Furthermore, Stallings also described the establishment of a TCP connection that is characterized by a three-way handshake [7]:

- SYN: The client sends a segment with the SYN (synchronize) flag set, indicating an initial sequence number [41].
- SYN-ACK: The server responds with its own sequence number and acknowledges the client's sequence number by sending a segment with both SYN and ACK (acknowledge) flags set.
- ACK: The client acknowledges the server's sequence number, and the connection is established.

This handshake ensures that both sides are ready for data transfer [42] and establishes initial sequence numbers for proper data synchronization.

User Datagram Protocol

Contrasting with the TCP's emphasis on reliability and sequencing, the User Datagram Protocol (UDP) prioritizes speed and simplicity.

The origins of TCP trace back to 1980 when it was introduced in RFC 768 [43]. As the internet and its associated technologies rapidly evolved during the late 1970s and early 1980s, there emerged a need for a simpler transport protocol that could function alongside the more complex Transmission Control Protocol (TCP).

TCP is a connectionless transport protocol. It works by delivering data packets, known as datagrams, from one device to another without the need to establish a connection beforehand [44]. Key aspects of TCP include:

- Connectionless Nature: Unlike TCP, TCP does not perform handshakes. It sends datagrams without prior communication between the sender and receiver.
- No Guarantee of Delivery: TCP does not guarantee that datagrams will be delivered, nor does it ensure the order in which they are received. It is a "best effort" service.
- Header Simplicity: The TCP header is made up of just four components: the source port, destination port, length, and checksum.
- Stateless Protocol: TCP does not track the state of communication between sender and receiver. Each datagram is an isolated transmission.

How TCP differs from TCP is that TCP focuses on speed and simplicity, which is used in many modern-day applications such as streaming and VoIP or video conferencing. These applications can result in the occasional loss of packets, resulting in the lag or the delay the user experiences. If the two user wants to engage a secured end-to-end encrypted communication, and one packet that contains frames to important encryption keys is lost, or the packets were not delivered in order; the recipient may not be able to properly decrypt the data [45]. The characteristics of the TCP architecture is the reason why TLS is not usually sent through TCP; i.e., because TLS needs a reliable channel like TCP to transmit data packets in order. To overcome this limitation, IETF published a standard on Datagram

Transport Layer Security (DTLS) [46] that is able to transport over TCP by adding a "retransmission timer to handle packet loss" [46]. There are studies on DTLS, such as Banerjee and others' study on eeDTLS [26] in which they looked at the energy efficiency of DTLS on IoT devices. Studies on DTLS show that TCP has a potential for providing reliable and secured connection between devices. However, this thesis project will focus on maintaining a common baseline between test points, thus only TLS over TCP and MLS over TCP will be considered. Further differences may occur if these security protocols are run over other transports.

2.5 RF Effects in Wireless Communication

As noted previously, RF is an essential component in wireless communication. However, the interrelationship between RF and network communications has not been widely explored in research at the networking and application layer. As introduced earlier in the chapter, engineers and researchers usually focus on designing better equipment to propagate and capture signals more effectively, but the research focus does not go beyond the signals conversion of bits.

As the 5G network becomes more prevalent and is coupled with the growing use of IoT applications today, a resulting increase in wireless communication will occur. Since RF is required to move the data for wireless devices, a drastic increase in wireless communication also means increase in activities in the RF environment.

Another concern in the RF spectrum is detectability. Interference in the RF environment means wireless devices are experiencing unwanted or unexpected signals [47]. In military application, any RF interference equates to possible detection of the RF signal Therefore, this thesis will also attempt to compare TLS and MLS protocol's affect on RF from the aspect of maintaining LPD and LPI.

2.6 Chapter Summary

The ability to wirelessly transmit data over vast distances is one of the most significant technological advancements in communication. Yet, navigating this data through various environments is not without challenges. It is combining the complex factors of RF signals,

the medium through which wireless data is sent; and the various data transmission protocols that move the data from one device to another.

In the realm of network communication, RF plays a pivotal role, especially in wireless data transmission and detectability. Oscillating at specific rates, RF signals traverse diverse environments, and their efficiency is significantly influenced by obstacles like buildings, which can reflect or attenuate signals, and atmospheric conditions such as rain or humidity that can affect propagation.

Understanding the behavior and challenges of RF signals in wireless communication sets the stage for a deeper examination of the protocols that govern data transmission over these networks. The efficiency and reliability of RF signal transmission directly influence how protocols operate and achieve their objectives. Hence, the shift from discussing the physical aspects of RF signals to exploring the logical layers of network protocols is crucial. Different protocols such as TCP and TCP, despite being built upon the same RF-driven wireless networks, differ significantly in their approach to data transmission, security, and integrity.

As we transition from the wireless sphere to the protocol domain, the Transmission Control Protocol (TCP) stands out with its intrinsic design focused on ensuring reliable data exchange. TCP's sequence numbers, acknowledgments, and checksums cater to data integrity, while its three-way handshake ensures a secure and consistent connection establishment. In contrast, the User Datagram Protocol (UDP), with its connectionless nature, offers speed due to minimal overhead but lacks the inherent security features present in TCP. Instead, TCP often leans on higher-layer applications or accompanying protocols to provide encryption and data integrity. This variance in TCP and TCP brings us to the OSI model's Layer 3, which forms the backbone of global internet communication.

Layer 3, also known as the Network Layer, integrates logical addressing, as observed with IP addresses, and path selection to seamlessly route data across complex network topologies through protocols like TLS or MLS, to ensure they reach their desired destinations. In essence, the confluence of RF principles, protocol designs, and the OSI model's layered approach collectively underscore the complexities and intricacies inherent in secure and efficient network communication.

Building upon the understanding of RF signals and data transmission protocols, the next chapter will delve into the methodology employed to simulate these protocols and observe their effects on the RF environment. The simulations will allow us to practically examine TLS over TCP and MLS over TCP, each with their unique characteristics, and how the functions within network layers impact RF signal behavior. The methodology will outline the simulation environment, parameters, and metrics used to evaluate these effects. This approach is essential to bridge the theoretical concepts discussed so far with practical observations, thereby providing a comprehensive view of network communication dynamics.

CHAPTER 3: Methodology

With a deeper understanding of the TLS and MLS protocols' architecture, this thesis project will test each protocol's behavior and affects on the RF footprint. The key events for TLS over TCP include establishing the TCP connection, the TLS handshake, and the closing of TCP connection. Meanwhile the key events for MLS over TCP include establishing the TCP connection, transmitting Key Packages, Key Updates, and closing the connection. A successful setup will give a comparison and a qualitative measurement on whether one protocol outperforms another from an RF perspective in a wireless data transmission scenario.

Two scenarios are tested for signal comparison analysis:

1. Transmission with small message size (1kb)
2. Transmission with large message size (1MB)

3.1 Test Setup and Instruments

Hardware

- Laptops
  - Model: MSI Prestige 15 (A10SC)
  - Operating System: Ubuntu 20.04.6 LTS
  - CPU: Intel Core i7-10710U @ 1.10GHz x 12
  - GPU: NV167/Mesa Intel UHD Graphic (CML GT2)
  - RAM: 31.2GiB
  - Network Interface: MSI USB GBE Adapter
- CAT 5/6 Unshielded Twisted Pair (UTP) Cable
- Signal Hound (BB60C)
  - Tx/Rx Frequency Range: 9kHz-6GHz
  - Sampling Frequency: 20MHz
  - Sweep Speed: 24Ghz/sec
  - Antenna: Omni-directional, polarized

- Radios
  - Persistent Systems MPU5 S-band handheld multiple-in multiple-out (MIMO) mobile ad-hoc network (MANET) radios
  - Model: RF-2100, MIMO 2W maximum transmit power per MIMO channel (6W maximum total transmit power)
  - Operating Parameters
    - Frequency: 2.242GHz
    - Bandwidth: 5MHz
    - Transmit power: 25dBm (0.316 W) per channel
  - Antennas
    - Model: ANT-2003
    - Gain: 2.15 dBi
    - Omni-directional
    - Vert Polarized

Software

- **Spike, a spectrum analyzer software** [48]. In the area of RF analysis, Signal Hound's Spike software is a powerful tool that works specifically with Signal Hound's line of spectrum analyzers and related equipment [48]. One core function of Spike is its real-time spectrum analysis in which the RF signal can be visualized in real-time. Furthermore, it has the ability to record the real-time signal for playbacks and analysis at a later time. To record real-time signal, the spectrum analyzer scan across a specified frequency range to measure and analyze signals within that spectrum, this process is called a *sweep*. Another standout features of Spike is its ability to produce waterfall plots. The waterfall plot is a visualization method that displays time, frequency, and amplitude on a single dynamic graph, which helps analyzers understand the behavior of signals over a period of time. While the two top features discussed were mainly used in this thesis, there are other useful features of Spike in regards to RF analysis that can be utilized in future studies.
- **Wireshark** [49]. The Wireshark is a free and open-source network protocol analyzer that lets users capture and visually display the details of network traffic in the forms of packets [49]. It supports numerous protocols and provides various inspection

capabilities, offering insights into communication details of networked systems and many other functions to analyze the traffic on the network. Wireshark uses PCAP (Packet CAPture) format, which is a standard file format used for storing network traffic, to decode and inspect individual packets within a PCAP file.

- **Prototype TLS Client/Server App written in Python** [50]. The code is written in Python with built-in libraries. The SSL library is used to setup the TLS protocol in Python. While Secure Sockets Layer (SSL) is outdated, and has since been replaced by TLS, the wrapper around the sockets for encrypted communication is the same. Therefore, despite its name, the ssl module in Python will support the TLS protocol [51]. For this prototype we use mutual-authentication between the client and the server for the TLS handshake and have certificates for both the server and the client.
- **Prototype MLS Group Messaging App written in Rust** [52] is configured as client/server application using TCP as the transport layer protocol. This thesis utilizes a prototype secure group messaging application developed at the Naval Postgraduate School [53]. A prototype software for secure messaging using the MLS protocol employs OpenMLS 0.5 [54], an open-source MLS protocol implementation. This software specializes in encrypting messages for groups larger than two, managing dynamic group states and key updates as the group size changes. It supports different network transport architectures, including a Local Area Network (LAN) with mobile ad-hoc network (MANET) radios for line-of-sight (LOS) communications, and the Internet using Message Queuing Telemetry Transport (MQTT) services for beyond line-of-sight (BLOS) communications. This development paves the way for further research and application of MLS in securing communications within both manned and unmanned teams.

3.2 Test Procedure

Hardware Setup

Laptops:

- Laptop 1:
  1. Connect Ethernet cable
  2. Power on the laptop

3. Ensure Wi-Fi is off
4. Open Terminals for TLS and MLS execution

- Laptop 2:
  1. Connect Ethernet cable
  2. Power on the laptop
  3. Ensure Wi-Fi is off
  4. Open Terminals for TLS and MLS execution
- Laptop 3:
  1. Power on the laptop
  2. Ensure Wi-Fi is off
  3. Attach USB cable (USB 2.0) from Signal Hound
  4. Launch SPIKE and select from preloaded settings

Radio:

- Radio 1:
  1. Connect MPU5 Radio 1 to Laptop 1 via Ethernet cable
  2. Power on the radio
- Radio 2:
  1. Connect MPU5 Radio 2 to Laptop 2 via Ethernet cable
  2. Power on the radio

Signal Hound:

1. Attach antenna
2. Attach USB cable (USB 3.0 end) to Signal Hound
3. Attach USB cable (USB 2.0 end) to Laptop 3

Figure 3.1 shows What the setup would look like.

Figure 3.1. Setup for testing.

Execution

Running TLS Commands

In order for the prototype TLS script [55] to work properly, the laptop acting as the server needs to generate a self-signed certificate called “server.crt” [56] and a private key called “server.key” [56] must be created and stored in the same folder of the TLS script to be executed.

For this thesis, Laptop 1 is designated as the “Server” and Laptop 2 is designated as the “Client”. The Server will open its IP address and listen for incoming connections. The Client will try to connect to the IP address denoted as the Server. Both the server and client will verify certificates and exchange keys in order to set up a secure communication channel.

From the terminal, we execute the “Server” code on Laptop 1, which will display that the Server is listening on (’IP Address’, Port Number). Once the “Server” listening, execute the “Client” code on Laptop 2, follow the print out prompt to set the number of messages to “4” that is transmitted every 1 second (e.g., four 1kb messages).

The focus of the RF behavior is on the three-way handshake, the data transmission, and the re-synchronization of the connection.

Running MLS Commands

In this thesis, Laptop 1 is designated as "Alice" and Laptop 2 is designated as "Bob." Both laptops have the same program structure, and it is in the command line in which the role of "Alice" and "Bob" is assigned.

To execute the MLS code for "Alice" in the Terminal of Laptop 1, enter RUST_LOG=debug target/debug/test_tcp -l alice. The -l denotes designating "Alice" as the leader[1] of this MLS group communication. For Laptop 2, enter RUST_LOG=debug target/debug/test_tcp –num-updates 1 –server-addr 192.168.1.1 –msg-sz 1000 bob.

There are a few more setting to establish a connection for "Bob." –num-updates 1 means the number of key updates for each execution, and within the code (one), the number of messages in a test is hard coded to 4 messages to match the tests for TLS (each message at the respective sizes of 1kb or 1Mb). –server-addr 192.168.1.1 is to input the IP address of "Alice" –msg-sz 1000 is to specify the size of the message for transmission is 1,000 bytes (or 1kb) and 1,000,000 is used for 1MB tests.

Upon code execution, TCP connection is established: "Bob" sends a KeyPackage, "Alice" produces a Commit and Welcome message, and the MLS connection is established. Secured data transmission can pass between "Alice" and "Bob" until the next Commit message with a key update for all members of the group to update keys and maintain secured communication without re-establishing connection.

RF Measurements

The first set of measurements was collected in a large facility using 2.242GHz, the setting prescribed in Section 3.1. Having a different signal than local Wi-Fi of 2.4GHz helped narrow the collection of the signals. Another location where RF measurement was conducted was within a semi-confined concrete area below ground level. The intent was that concrete walls and basement help block out some signals in the environment; thus, the testbed can potentially minimize the signals collected to just the radios in testing and other unavoidable signals in the environment.

[1]The *leader* is not a construct of MLS but rather testbed terminology for this MLS simulation. It notates "Alice" as the leader which sends "Commit" and "Welcome" messages to new member simulated by Laptop 2 that establishes MLS connection.

Another consideration was the frequency in which the radios are authorized to transmit. Commercially available Wi-Fi radios are certified to operate in unlicensed RF bands. Therefore, there is no permission required to use them. However, careful consideration is necessary if the radios operating in licensed bands due to risk of interference with licensed equipment [57]. The benefit to operating radios in such frequencies is reduced noise due to fewer (or in our case, no) devices operating on these frequencies. For this experiment, we tuned our MANET radios to a previously cleared frequency.

The following procedure is used to ensure consistency and elimination of environmental noise during RF measurements.

1. Turn off Wi-Fi and Bluetooth radios on personal electronic devices and test laptops to minimize noise in the RF environment and ensure data is transmitted only through the test radios.
2. Start screen record with audio recording running Spike software for documentation
3. Start Sweep Recording on Spike
4. Allow Spike to record without any testing for approximately 15 seconds
5. Turn on Radio 1 and Radio 2
6. Wait for the radios to initialize (approximately 30 seconds)
7. Start recording Wireshark on Laptop 1 and Laptop 2.
8. Start TLS in Terminal
    a. On Laptop 1, Run “Server.py”
    b. On Laptop 2, Run “Client_1kb.py”
    c. Input “4” to simulate transmitting 1kb of message 4 times
    d. Close the connection
    e. Repeat 2 more times
    f. Exit both server and client application
    g. On Laptop 1, Run “Server.py”
    h. On Laptop 2, Run “Client_1MB.py”
    i. Input “4” to simulate transmitting 1MB of message 4 times
    j. Close the connection
    k. Repeat 2 more times
    l. Exit both server and client application

9. Start MLS in Terminal
    a. On Laptop 1, enter RUST_LOG=debug target/debug/test_tcp -l alice
    b. On Laptop 2, enter RUST_LOG=debug target/debug/test_tcp –num-updates 1 –server-addr 192.168.1.1 –msg-sz 1000 bob
    c. Applications will simulate transmitting 1kb of message 4 times.
    d. Close the connection.
    e. Repeat 2 more times.
    f. On Laptop 1, enter RUST_LOG=debug target/debug/test_tcp -l alice
    g. On Laptop 2, enter RUST_LOG=debug target/debug/test_tcp –num-updates 1 –server-addr 192.168.1.1 –msg-sz 1000000 bob
    h. Applications will simulate transmitting 1MB of message 4 times.
    i. Close the connection.
    j. Repeat 2 more times.
10. Exit all Terminals
11. Turn off Radio 1 and Radio 2
12. Stop recording on Wireshark
13. Stop Sweep Recording on Spike
14. Stop screen record

3.3 Data Collection

In addition to using Spike and Wireshark, the screen recording feature on the laptop is executed. The screen recording function is a built-in feature of Microsoft Operating Systems. More than its name suggests, the screen recording function can also capture audio recordings through a laptop's microphone. For this experiment, screen capture with audio recording helped with timeline establishment. The data collector can narrate through the data collection process while the recording is running by verbally saying major events such as "Turn on the radios now," "Recording on Wireshark now," "Executing TLS now," and "Key updates now," etc. Those major events can correspond to noticeable signals detected on SPIKE, which can also correlate to the packet capture by Wireshark.

It is important to address the timing of the captures. Initially, when the Spike begins recording, the first 15 seconds of the recording are allotted before any applications are executed. This allocation is to set a baseline of the signal measured when there are no

activities conducted. We can refer to the signals captured during this period of inactivity as the ambient noise. Once the radios are turned on, another 15 seconds are allotted to capture the signals between the radios. This segment of the RF signal includes the basic management communication between Radio 1 and Radio 2. The execution of both TLS and MLS protocols is done in a certain order to produce RF signals in a consistent manner. The closing of each test run is executed in the reverse order of how it started to ensure all signals are properly captured before recording is stopped.

It is also important to note that this thesis designed the simulation to transmit 1kb (and 1MB) in message size 4 times for each of the iterations. This limitation is because the spectrogram window in the Spike software is only large enough to display a snapshot of the following components: the TLS and MLS connections, four 1MB messages, and an additional handshake for TLS (respectively a key update for MLS). Any more data transmission would result in the initial TLS and MLS connections falling outside of the spectrogram window and causing difficulty in providing a good visual representation of the entire simulation. Furthermore, during the simulation design, it was observed that the spectrogram displaying the data transmission of the message regardless of size remains largely consistent; it is the TLS handshakes and MLS Key Package (and key Updates) that showed interesting differences. Additionally, 3 simulations were conducted in each tests to keep the entire test to a manageable length yet still able to capture all the significant activities of both the TLS and MLS architectures. Future research can naturally expand on the number of tests.

Upon the completion of RF measurement, the collected information can be used for analysis.

From Wireshark, analysis on the network utilization over time is performed and compared between TLS and MLS simulations. Figure 3.2 is a screenshot of Wireshark displaying network traffic captures of TLS over TCP transmitting 1kb message size every 1 second for 4 iterations.

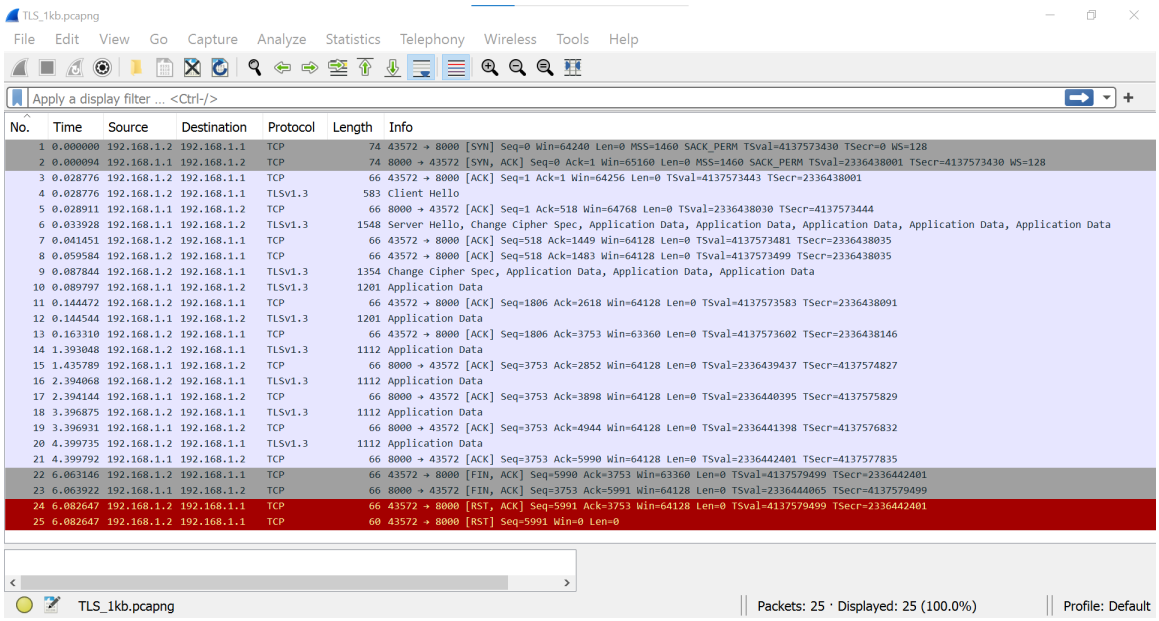

Figure 3.2. Wireshark Screenshot Capture.

Analysis used for this project looks at channel power for the RF signals throughout the data transmission. Figure 3.3, shows the channel power measured for one test run. The results will be explored in the next chapter.

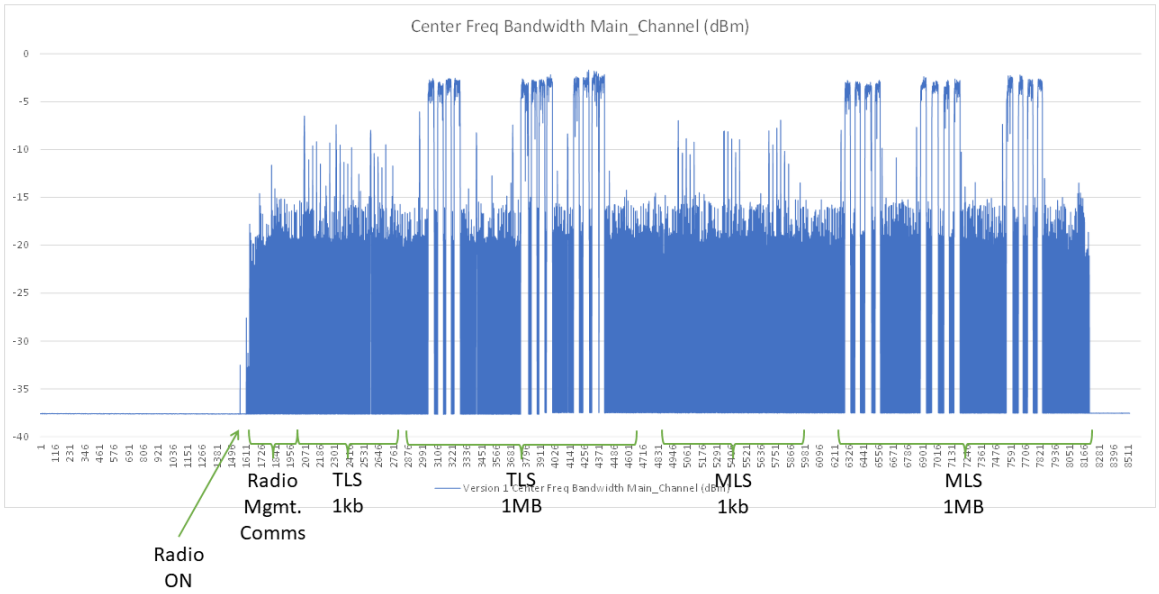

Figure 3.3. Measurement of Channel Power during TLS and MLS Data Transmission.

Spike software with the spectrogram displayed in the middle as shown in Figure 3.4 provided visual representation of the RF signals during data transmissions.

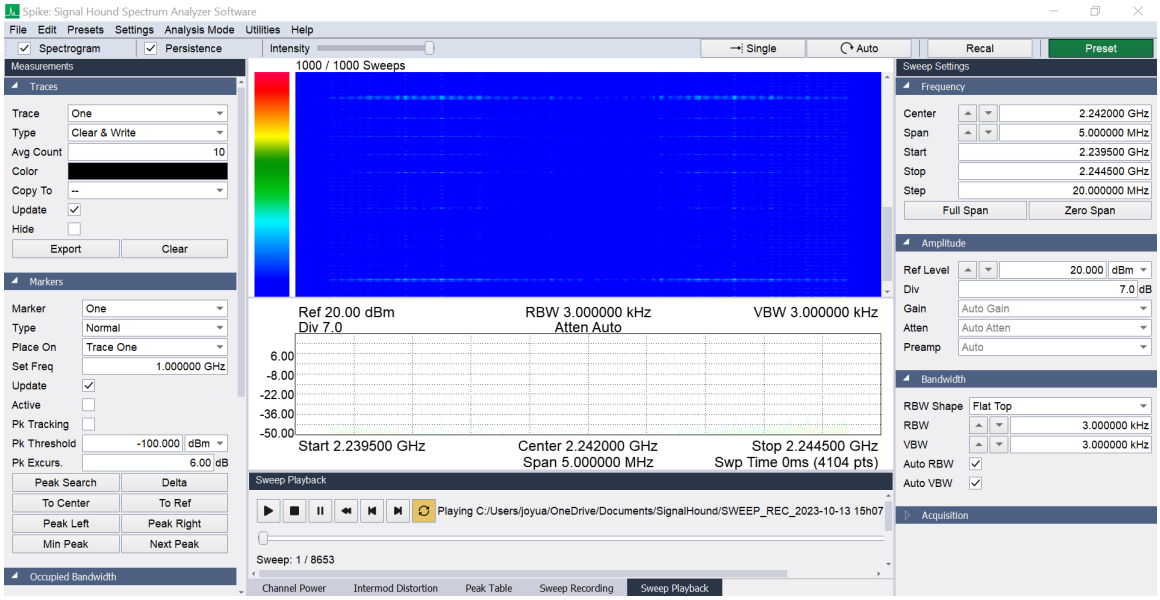

Figure 3.4. Spike Software layout with Spectrogram displayed in blue.

Next chapter will focus on analyzing the comparison of channel power utilization over time for TLS and MLS; as well as the comparison on network utilization over time for both protocol.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Analysis and Results

This chapter analyzes the testing results between TLS and MLS, transmitting different sizes of data over TCP. There are three areas of focus: visual analysis of the spectrogram, channel power analysis, and network traffic analysis. Both the spectrogram and the channel power analysis used information from the Spike software in conjunction with the Signal Hound Spectrum Analyzer. Network traffic analysis used packet capture from Wireshark that was recording in both Laptop 1 and Laptop 2. The results showed differences in the signals and data transmission activities between TLS and MLS protocols.

One complete simulation consists of the following:

1. TLS over TCP – three iterations of the following steps:
    - Establish TCP Connection and TLS Handshake
    - Transmission of 1kb message size follow by 1 second pause
    - Transmission of 1kb message size follow by 1 second pause
    - Transmission of 1kb message size follow by 1 second pause
    - Transmission of 1kb message size
    - Close connection
2. TLS over TCP – three iterations of the following steps:
    - Establish TCP Connection and TLS Handshake
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size
    - Close connection
3. MLS over TCP – three iterations of the following steps:
    - Establish TCP Connection and send Key Package
    - Transmission of 1kb message size follow by 1 second pause
    - Transmission of 1kb message size follow by 1 second pause

- Transmission of 1kb message size follow by 1 second pause
- Transmission of 1kb message size
- Send Key Update

4. MLS over TCP – three iterations of the following steps:
    - Establish TCP Connection and send Key Package
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size follow by 1 second pause
    - Transmission of 1MB message size
    - Send Key Update

4.1 Channel Power

In RF communications, a channel is a band of frequencies allocated for a specific signal or type of transmission. Furthermore, channel power is the total power contained within a defined bandwidth of frequencies. The Spike software has the ability to log channel power in the form of a .csv file. In this thesis, the channel is plotted where the y-axis is the power level (in P_{dBm}) and the x-axis is the time (in seconds).

Figure 4.1, shows the the channel power utilization for TLS over TCP on a data transmission of 1kb of message size. The first spike occurred around 0.832 seconds, and is the establishment of TCP connection followed by the TLS handshake, which last until about 1.162 seconds. The subsequent 4 "spikes" are the data transmission events in which 1kb in message size is transmitted every one second for 4 iterations. Finally, at time 7 seconds, the "spike" event indicates the close of TCP connection.

On the other hand, Figure 4.2 shows the channel power utilization for MLS over TCP on data transmission of 1kb of message size. While the figure looks similar to Figure 4.1, the event in which the signal is recorded is slightly different. At time 0.833, the "spike" denotes the establishment of TCP connection as well as the transmission of a Key Package. Similar to the TLS simulation, the subsequent 4 "spikes" are the data transmission events in which 1kb in message size is transmitted every one second for 4 iterations. The signal for key update transmission is captured at time 6.971 second.

Both figures shows the channel power utilization for small message size of 1kb per message, and the behavior closely matched the events recorded on the Spike software as well as the network traffic captures on Wireshark.

The same analysis is performed for large message size of 1MB per message. Figure 4.3 shows the channel power utilization for TLS over TCP transmitting 1MB of message size every 1 second for 4 iterations. Figure 4.4 is the channel power utilization for MLS over TCP with the same iterations.

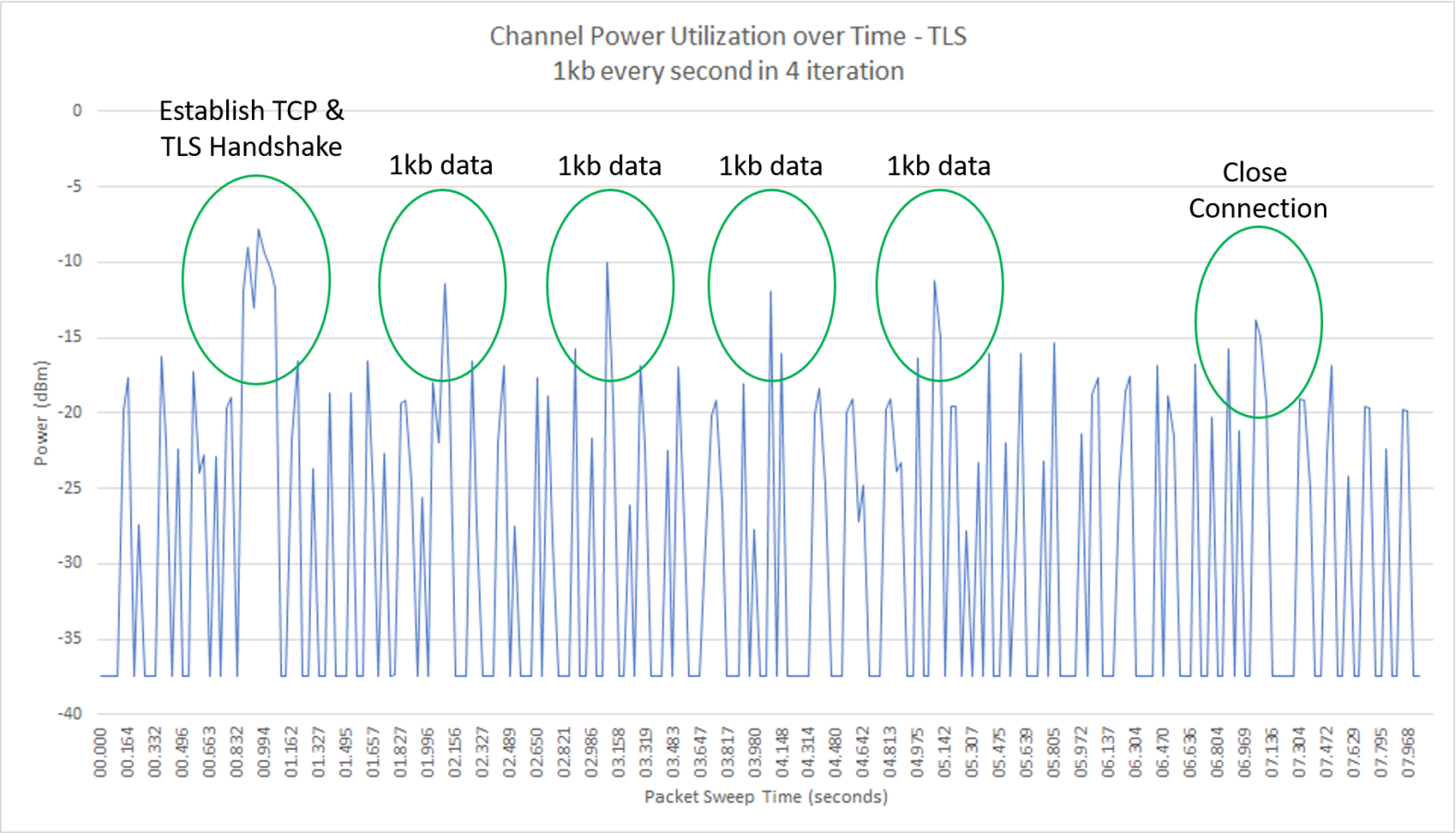

Figure 4.1. Channel Power Utilization over Time for TLS on 1kb Message Size.

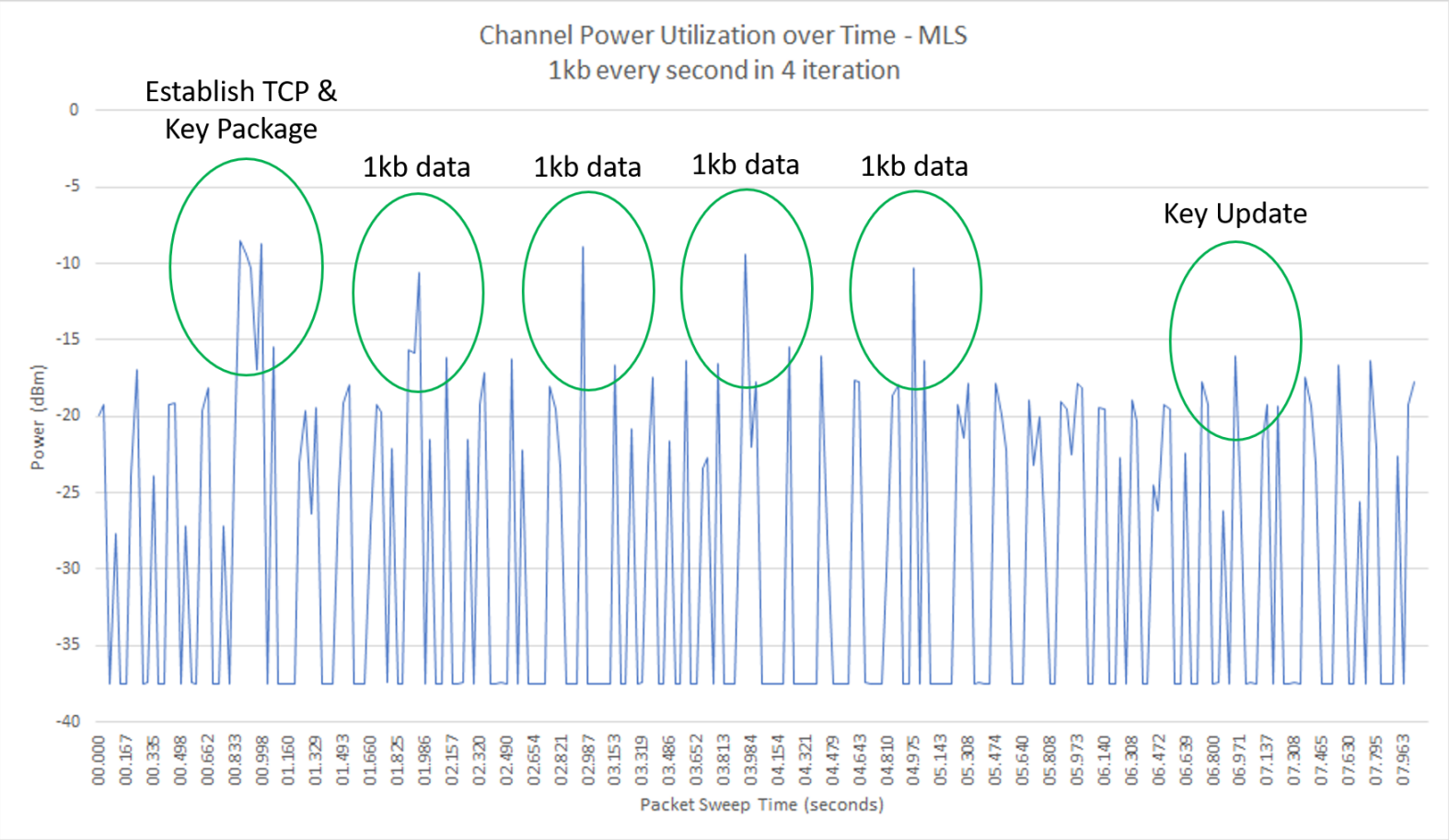

Figure 4.2. Channel Power Utilization over Time for MLS on 1kb Message Size.

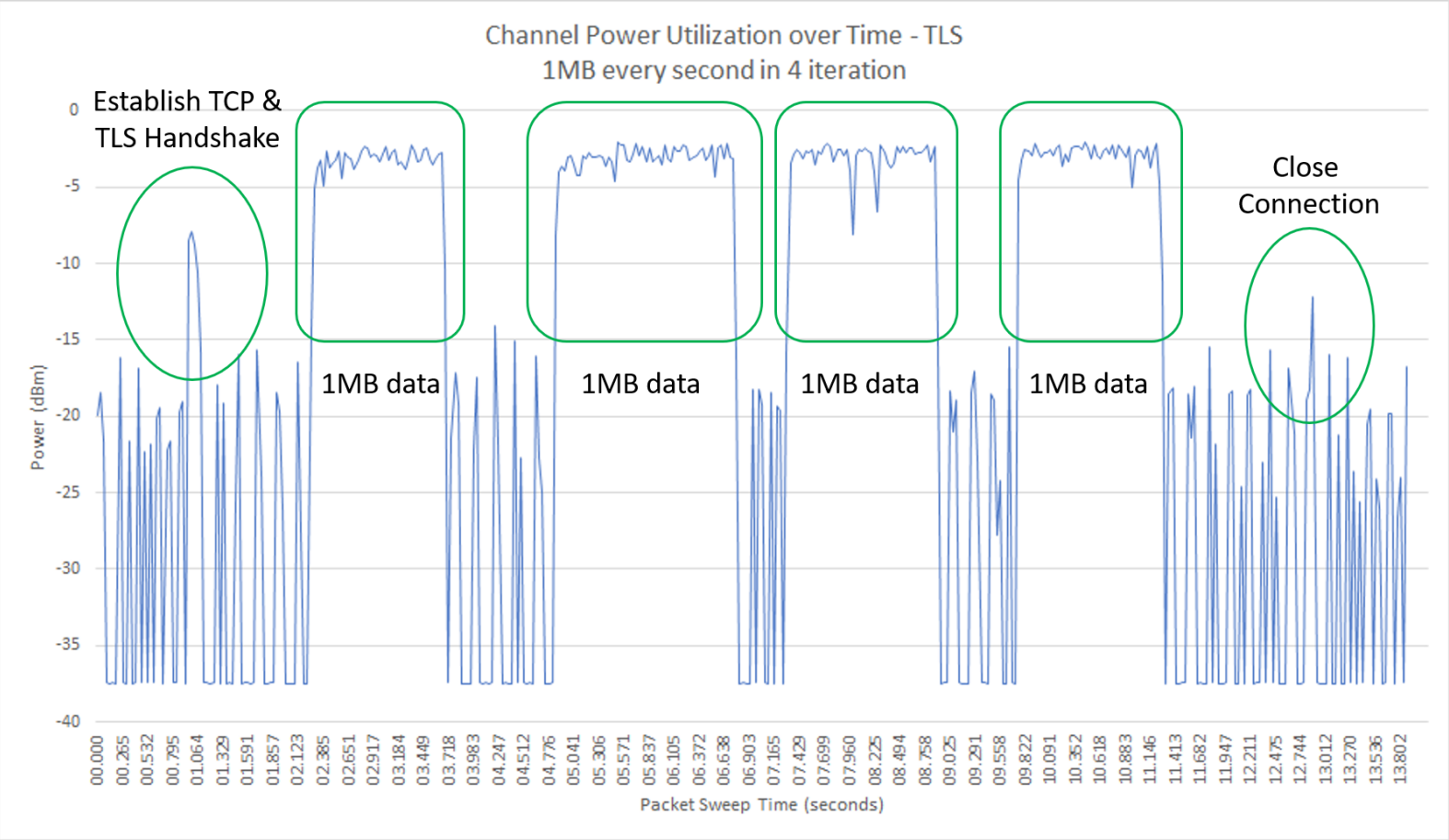

Figure 4.3. Channel Power Utilization over Time for TLS on 1MB Message Size.

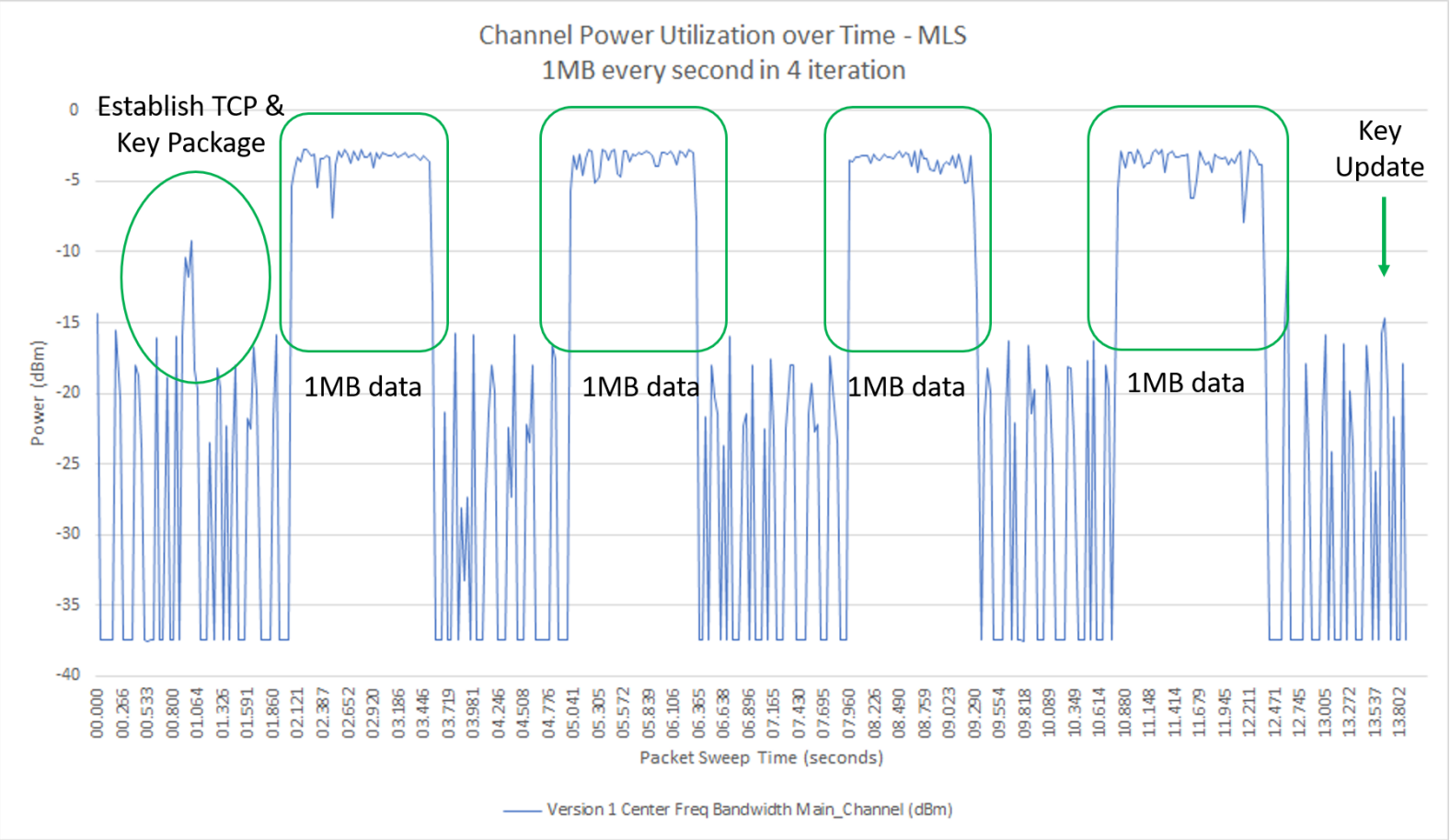

Figure 4.4. Channel Power Utilization over Time for MLS on 1MB Message Size.

For RF signals captured in Spike measured by the Signal Hound, P_{dBm} is a unit of power expressed in decibels relative to one milliwatt (mW). Since the P_{dBm} scale is logarithmic, it is necessary to convert the power unit to watts for further analysis based on the previous discussion in Chapter 2.1 regarding RF power in data transmission. Therefore, the channel power log in a .csv file displaying in dBm was converted to P_{mW} using the equation discussed in Chapter 2. The total power in milliwatts was calculated for each measurement duration for comparison.

To maintain similarity of data points for comparison, 30 sweeps (as defined in Chapter 3.1, referring to how the spectrum analyzer scan across a specified frequency range to measure and analyze signals within that spectrum) before the initial signal capture is included and 30 sweeps after TCP session closed for TLS or key update transmission for MLS is included so both TLS and MLS will have the same measurement duration. The summary of result is showed in Table 4.1.

Table 4.1. Comparison of Power Output for TLS and MLS.

Data Size	TLS	MLS
1kb	2.18mW	2.11mW
1MB	99.91mW	80.04mW

MLS protocol shows an overall less power output than TLS. For the 1kb message size, TLS outputs approximately 3.32% more power than MLS, and 24.83% for simulation on 1MB message size.

4.2 Network Utilization

Wireshark is used to record packet capture from the laptops transmitting the data. The basic information provided includes the packet number in the sequence of capture, the timestamp of when the packet was captured, the source and destination IP address, the protocol used, the length of the packet (in bytes), and detailed information about the packet.

In order to understand the network activities for the measurement duration, a plot depicting the network utilization over time is shown in Figure 4.5. The x-axis displays the unit of milliseconds and the y-axis is the packet size transmitted. The initial “spike” is the amount

of bytes sent to establish the TCP connection and complete the TLS handshake. The next 4 “spikes” are the data transmission events in which 1kb in message size is transmitted every one second for 4 iterations. This simulation completes with the close of the TCP connection.

The same plotting technique is conducted to network activities on 1kb data transmission for MLS, as shown in Figure 4.6. Transmission of the key package instead of performing TLS handshake is one difference between TLS and MLS simulations, and the other difference is key updates at the end of 4 messages.

Network utilization analysis is also performed on large message size of 1MB for TLS (Figure 4.7) and MLS (Figure 4.8).

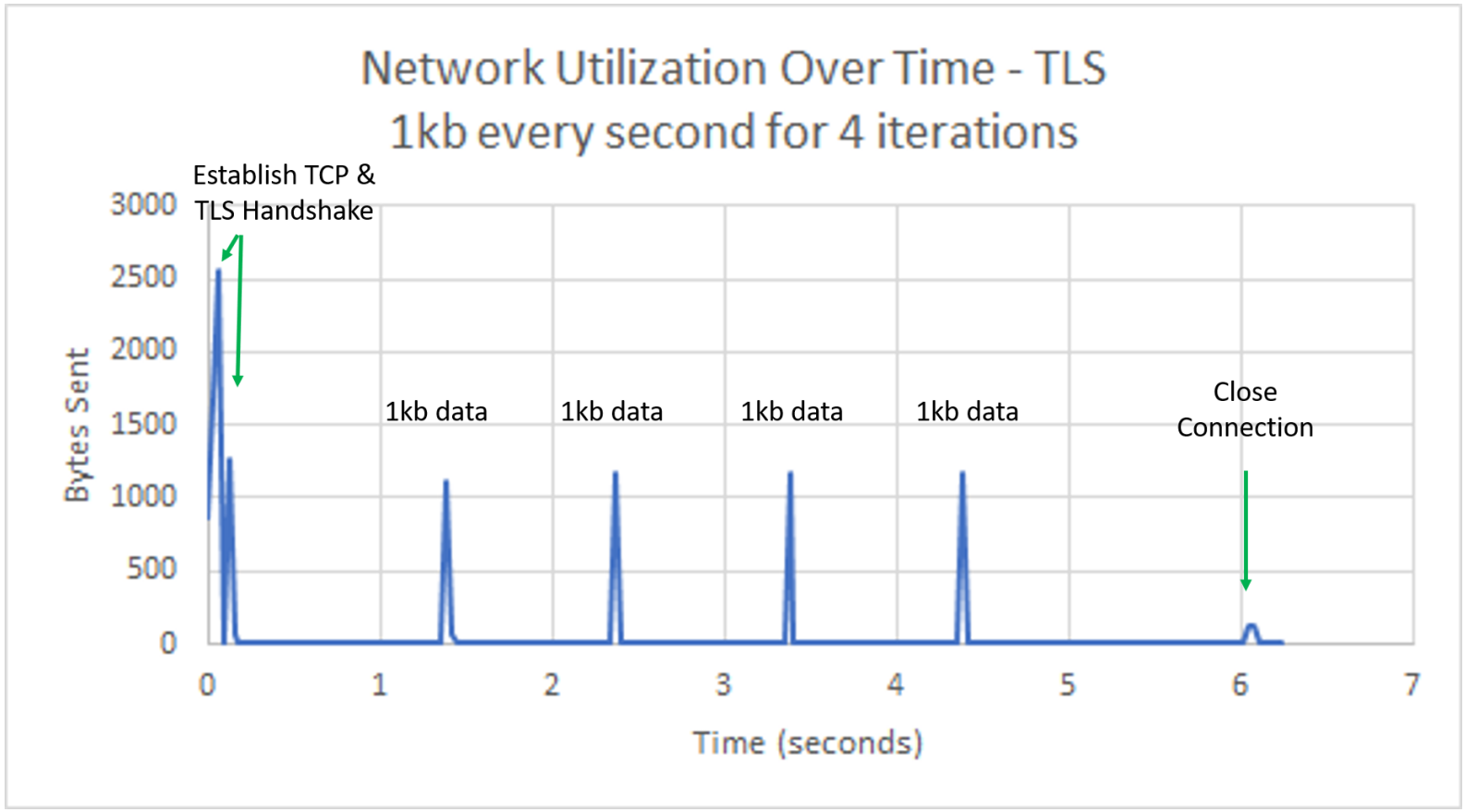

Figure 4.5. Network Utilization on 1kb Data Transmission for TLS.

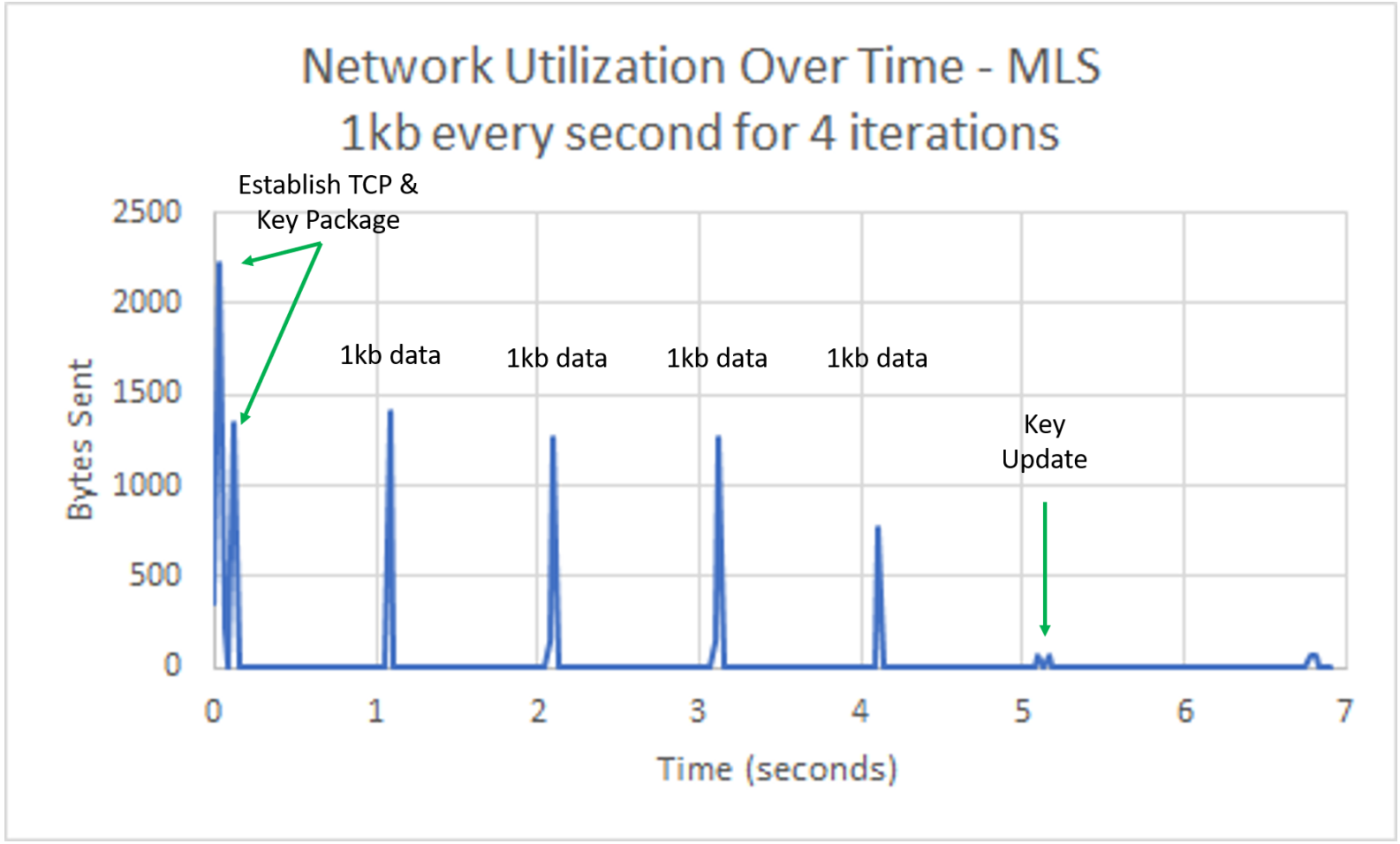

Figure 4.6. Network Utilization on 1kb Data Transmission for MLS.

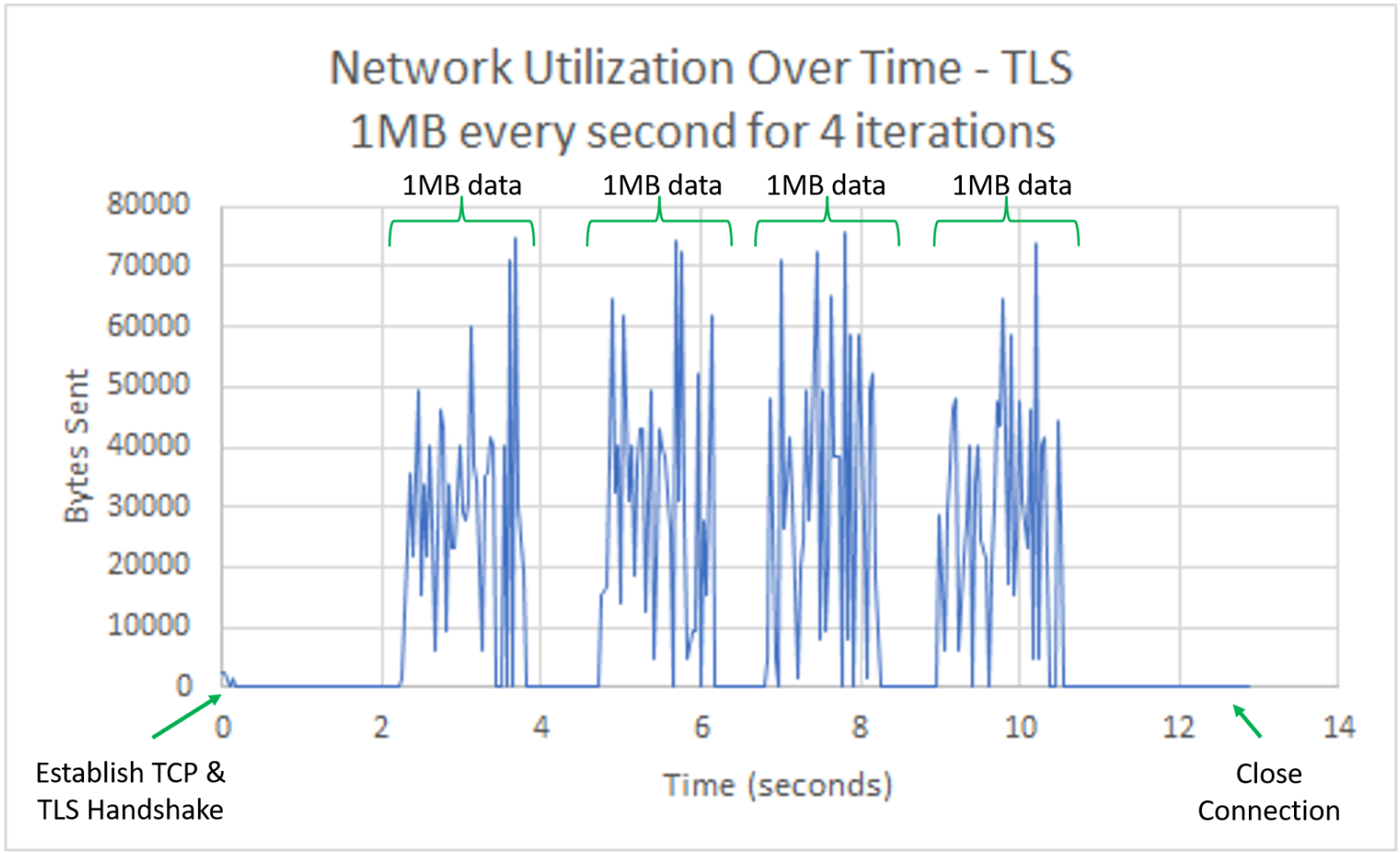

Figure 4.7. Network Utilization on 1MB Data Transmission for TLS.

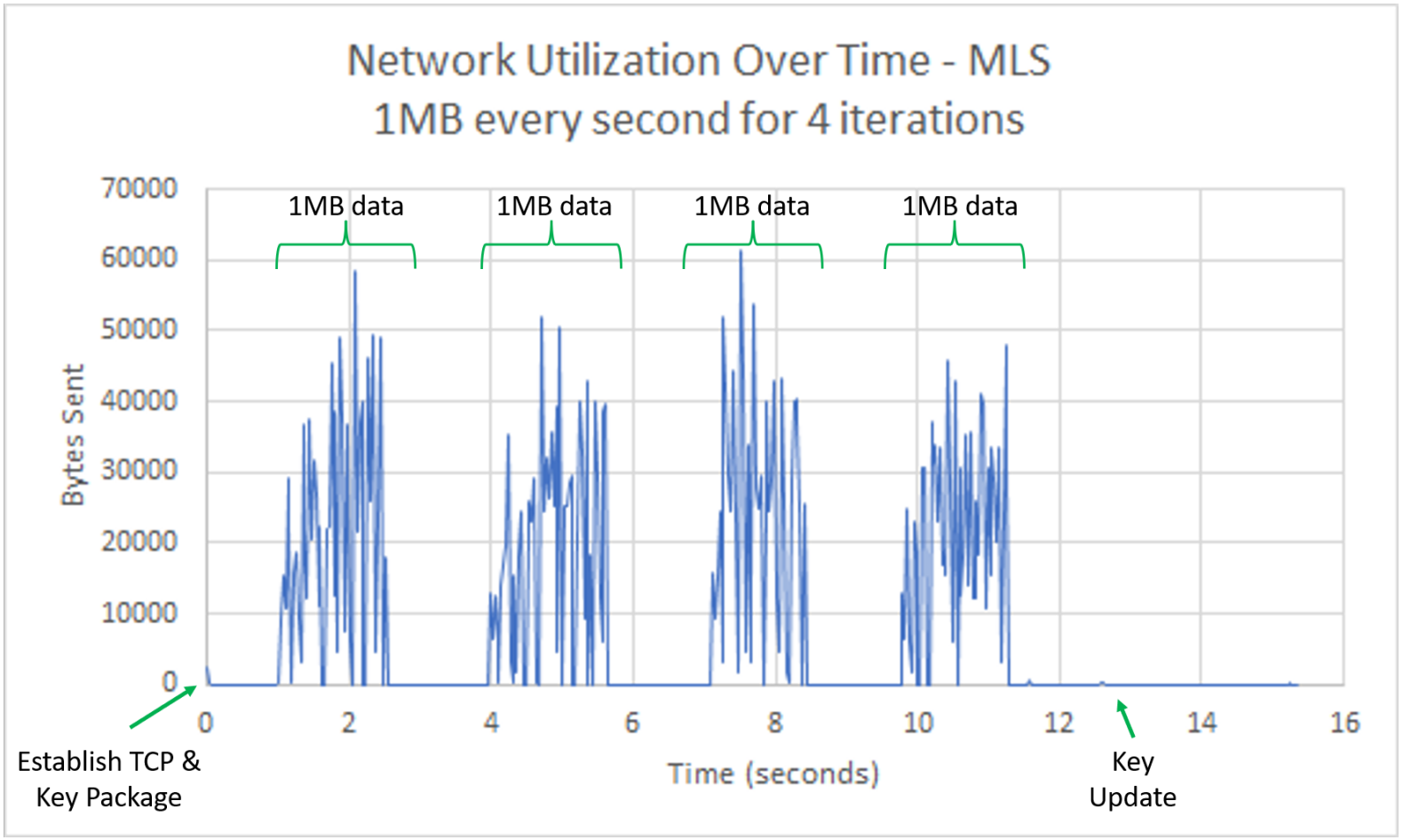

Figure 4.8. Network Utilization on 1MB Data Transmission for MLS.

Since amount of data will affect the RF signal in terms of power output, comparing the total data sent between TLS and MLS is also important. By using the "Analyze" tool in Wireshark, a particular string of related TCP communication can be extracted. On the Wireshark menu, click on "Analyze", "Follow", "TCP Stream", on a selected test run. The only packet displayed will be the packets related the same TCP session. Once the session is highlighted, the total packet length can be summarized by Wireshark. The table below captures the total bytes of each TCP session for TLS and MLS.

Table 4.2. Comparison of Data Transmitted for TLS and MLS.

Data Size	TLS	MLS
1kb	11401 bytes	9375 bytes
1MB	4480433 bytes	4263565 bytes

MLS protocol shows less bytes transmitted than TLS. TLS transmitted approximately 21.61% more bytes than MLS for message size of 1kb, and 5.09% more than MLS for message size of 1MB.

4.3 Spectrogram

Spectrogram is a good visual representation that can identify the signal activities that are significant during data transmission.

In RF signal analysis, spectrograms can help identify signal characteristics such as bandwidth, frequency stability, modulation, and the presence of noise or interference. They are especially useful for non-stationary signals [58], where the frequency content changes over time, and are crucial for applications such as wireless communication analysis. Spectrogram provides a visual understanding on the behavior of RF signals.

The Spike software features a display option call Spectrogram. The x-axis represents frequency, the y-axis represents time, and amplitude is represented using a color-coded scheme [59]. As the RF signal travels from one end to another at the specified frequency, it captures the RF behavior from the Time Domain perspective as seen in Figure 4.9 [60]. Thus, when Spike's Spectrogram sweeps and captures a signal, it may look like dotted line across the frequency spectrum. Furthermore, in some instances there is a horizontal

streak-like dark blue line mixed within the light blue display. This dark blue line is a result of the RF behavior in the environment and the timing of the sweeps. Such phenomenon is seen more distinctively in Figure 4.12 and 4.13.

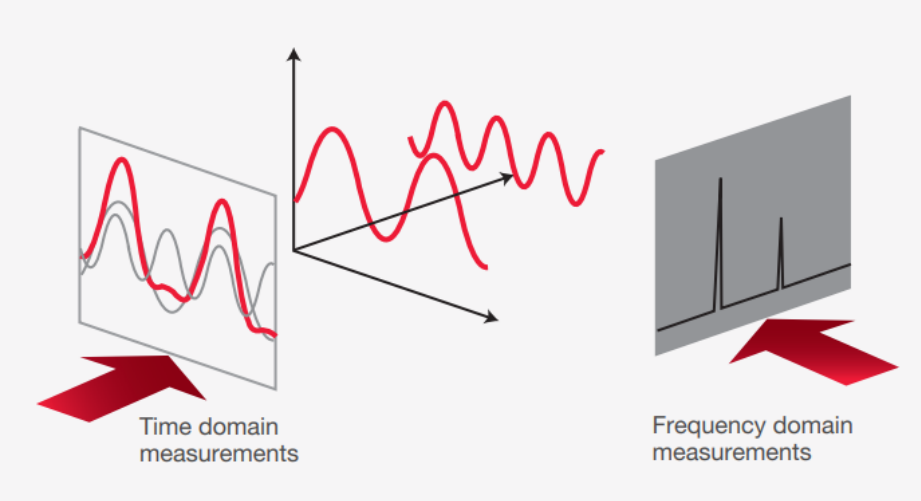

Figure 4.9. Spectrogram Capture Based on Time Domain Measurements. Adapted from [60].

The spectrogram for TLS over TCP on small data of 1kb per message is captured in Figure 4.10. The first light blue line indicates the establishment of a TCP connection plus the TLS handshake. The 4 subsequent light blue lines are the 1kb of data transmission at 1 second intervals. There is a fifth light blue line when the TCP connection is closed.

Similarly, for MLS over TCP on small data of 1kb, shown in Figure 4.11, the first light blue line is the establishment of a TCP connection plus the key package. The four subsequent light blue lines signify the 1kb of data transmission at 1 second intervals. What is different between the two spectrograms is the fifth light blue line which is the transmission of key update message – in practice, the key update message would replace the key package transmission in follow-on connections, reducing the power for those. The spectrogram shows a RF behavior that was expected based on the data transmission activities of wireless communication.

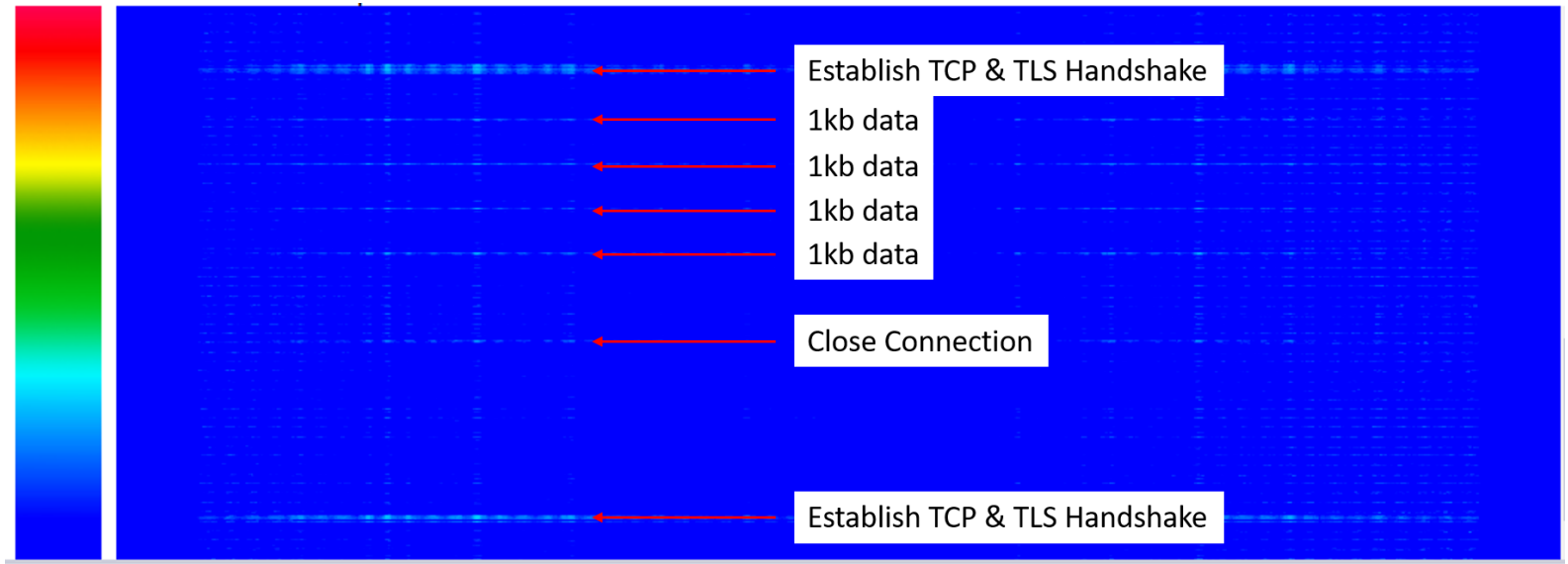

Figure 4.10. Screenshot of Spectrogram during 1kb Data Transmission for TLS.

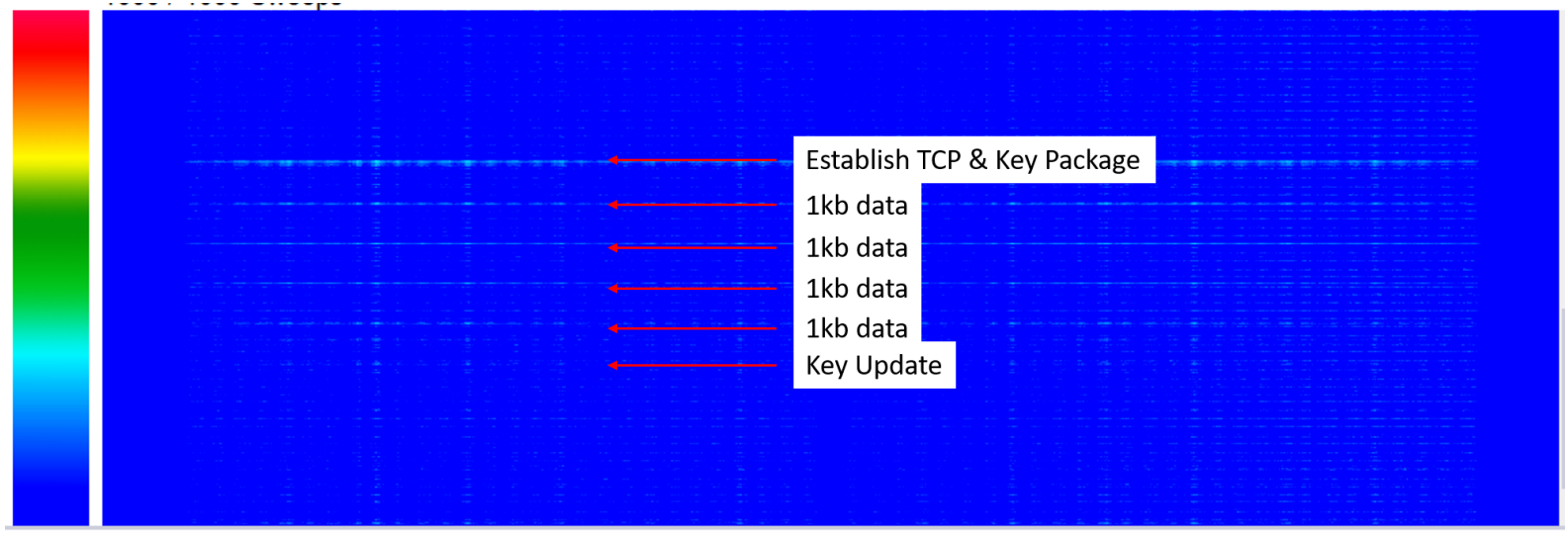

Figure 4.11. Screenshot of Spectrogram during 1kb Data Transmission for MLS.

Extending this analysis to larger data sizes, specifically 1MB, the spectrograms for both TLS and MLS over TCP exhibit distinct characteristics as compared to the 1kb data transmission as illustrated in Figures 4.10 and 4.11 respectively. In the case of TLS over TCP with 1MB data, as depicted in Figure 4.12, the initial light blue line representing the establishment of the TCP connection and the TLS handshake remains consistent with the 1kb scenario. However, the subsequent light blue lines, indicative of the data transmission, display a more prolonged and dense pattern, reflective of the increased data size. The closing of the TCP connection is also marked by a distinct light blue line, similar to the smaller data transmission scenario.

In contrast, the spectrogram for MLS over TCP with 1MB data, shown in Figure 4.13, demonstrates the density of the light blue lines corresponding to the data transmission as well as the key update message transmission. The denser light blue lines correspond to increased RF activities, which aligns with the expected behavior in wireless communications dealing with larger data sizes.

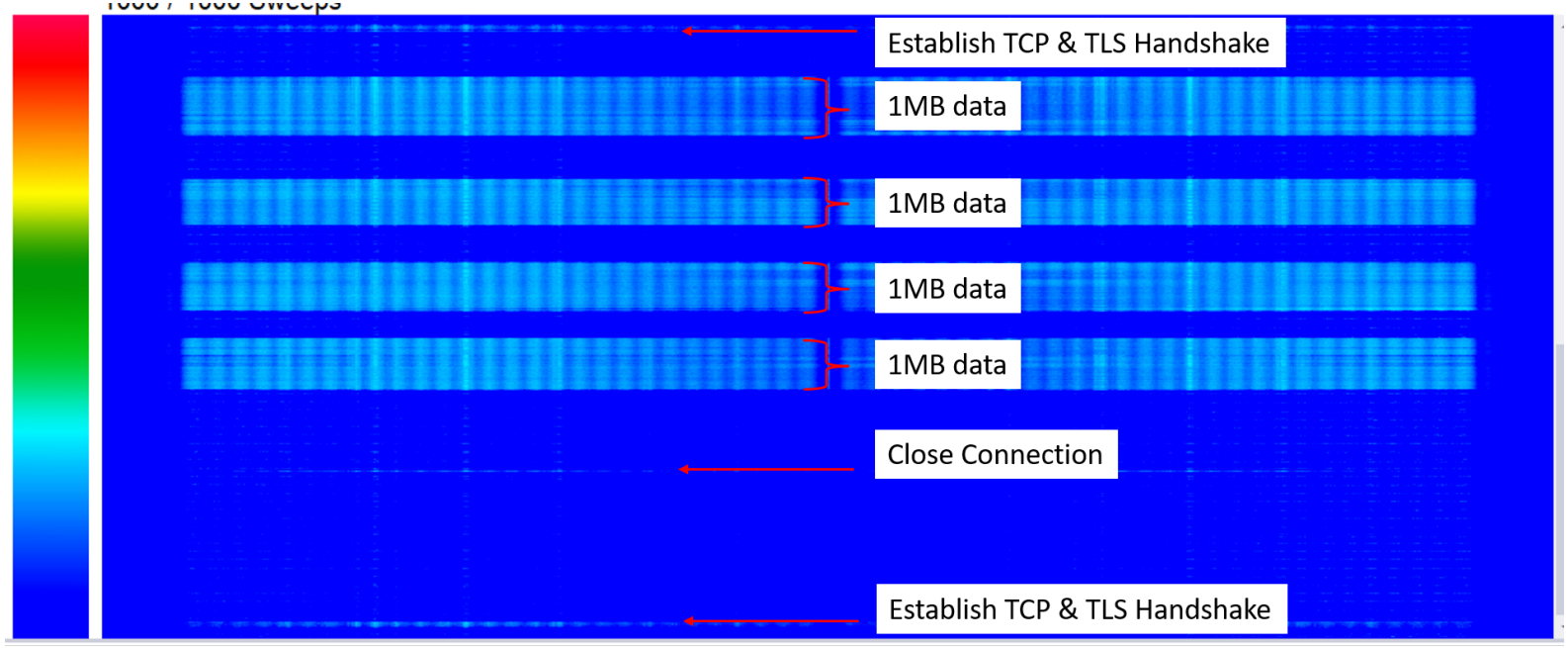

Figure 4.12. Screenshot of Spectrogram during 1MB Data Transmission for TLS.

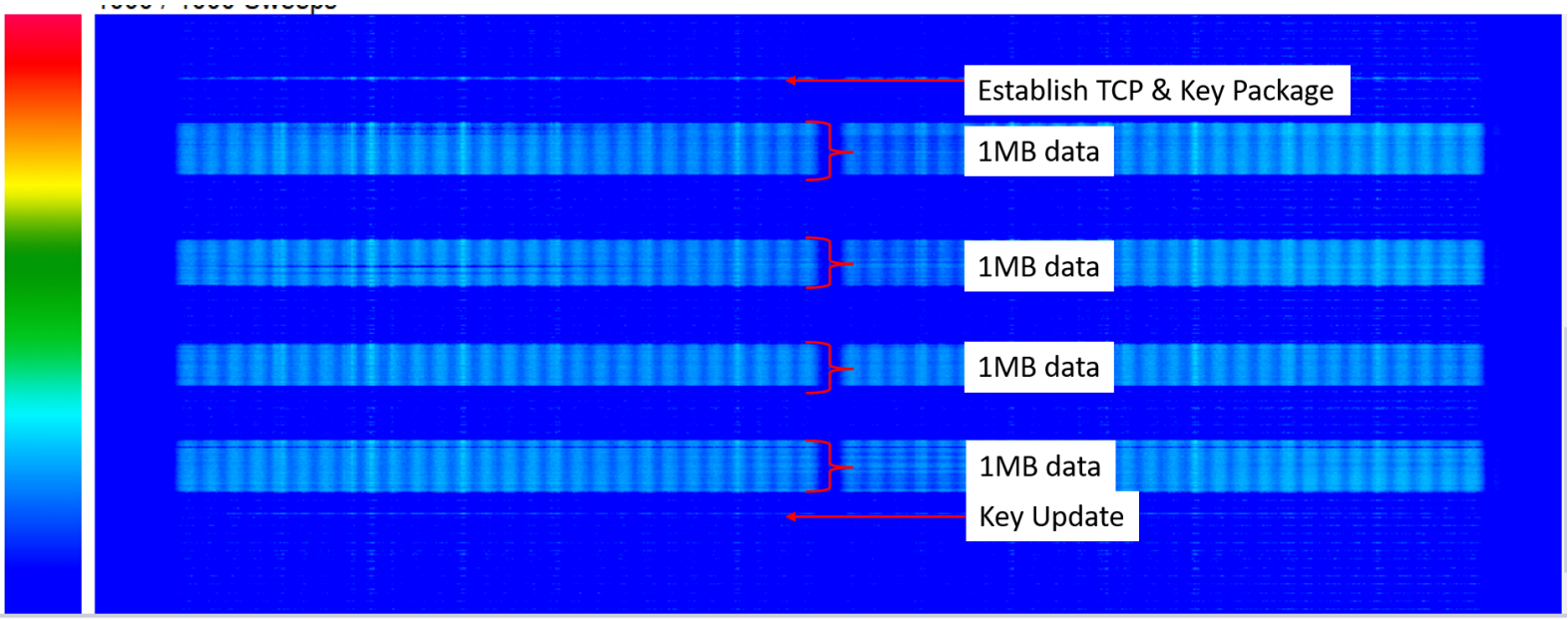

Figure 4.13. Screenshot of Spectrogram during 1MB Data Transmission for MLS.

4.4 Results

The analysis presented in Chapter 4 of this thesis provides insightful findings on the RF footprint and network utilization of TLS and MLS protocols. This discussion aims to delve deeper into these results, interpreting their significance in the broader context of secure RF communications and providing a comparative analysis of the two protocols.

Naturally, the data transmission of large message size results in an obviously larger footprint, as seen in both channel power and the spectrogram. Therefore, message size should be considered when LPD and LPI are important.

While analysis for the channel power utilization over time between TLS and MLS shows only subtle differences, the pattern of the utilization behavior was consistent. Furthermore, the finding on the network utilization over time for both protocols concurs with such a pattern.

Additionally, in both channel power and network utilization, there is a distinct behavior in which the MLS Key Package spiked only once and is replaced with a smaller spike during the "key update". This is notable as for all follow-on connections, MLS will use the key update process instead of the key package step, meaning that the initial spike should not be seen again. In contrast, for TLS, there will always be a TLS handshake spike for each connection.

One further significant finding from this thesis is the total power output and the total bytes transmitted between TLS and MLS. In both cases of 1kb and 1MB, TLS outputs more power than MLS. In regards to wireless devices, when such devices output more power, there will also likely be battery drain due their high transmission power while converting into RF energy. For military operations where RF footprint detection, the fact that TLS will output more power than MLS to transmit the same amount of data may be a consideration. Potential differences on battery drain are aso considerations.

The network utilization over time also provided comparable results. For transmitting the same amount of data, TLS will require more bytes than the MLS protocol. This finding is significant because as previous discussed in Chapter 2, the number of handshakes will grow drastically the more devices that need to remain connected. To reiterate, the size of the message and the size of RF footprint are correlated. Thus, TLS is not ideal for large group communications.

For this thesis, the simulation design was an exchange of 4 messages between two devices. However, the disparity between TLS and MLS will grow, especially over the course of continuous network traffic. As the number of devices increases, the duration of the data exchange increases, and the size of the message increases, the disparity will scale up as well. The findings of this thesis provided some experimental insight to power utilization and network efficiency between TLS and MLS, which are a few important considerations for maintaining secured data streams in the operational environment among multiple devices.

CHAPTER 5:
Conclusion and Future Work

This chapter summarizes the key takeaway from the experiment on the effects of RF signals based on TLS and MLS protocol. Several suggestions for future research ideas are also discussed below.

5.1 Conclusion

This thesis explored the effects of radio frequency on different data transmission methods between two autonomous systems. Studies on how various data transmission changes affect the RF domain are sparse, and existing literature either focuses on RF aspects of wireless communication or on data transmission protocols at the network layer. The focus of this thesis was to understand how security protocols like TLS (Transport Layer Security) and MLS (Message Layer Security) impact the RF footprint during data transmission more comprehensively.

A methodology was developed for setting up these protocols and the criteria for evaluating their performance. Two scenarios were tested: transmitting 1kb of data and transmitting 1MB of data for both TLS over TCP and MLS over TCP. While neither security protocol is tied to TCP, it is used as a common baseline for testing.

As expected, increased data volume directly correlated with greater power output for both protocols. The results provide a comparative analysis of established TLS versus emerging MLS techniques.

Key takeaways include:

- Data transmission incurs a cost on radio frequency footprint, so it is important to analyze RF emission behavior of different networking protocols.
- MLS exhibited slightly less channel power and data transmission than TLS, potentially due to a different protocol architecture of using key packages and key updates rather than performing the 3-way handshakes.

- As MLS uses key updates for follow-on connections, which require even less power and network utilization than in the key package transmission, it offers an added advantage over TLS over time. In contrast, TLS requires a complete TLS Handshake for each subsequent connection.
- Security protocol selection and message size can potentially affect the ability to maintain LPD and LPI.

The thesis initializes study within a gap in existing literature by linking RF characteristics with data transmission protocols, offering new insights into the comparative efficiency of TLS and MLS in terms of RF emissions and network performance. This foundational understanding sets the stage for further exploration and experimentation in the field, potentially leading to more efficient and secure wireless communication technologies.

Many military communications are conducted wirelessly: Ships at sea, mobile ground units ashore, and drone operations in space. This thesis adds strong relevancy in the military application. By beginning to explore the newly standardized MLS's behavior and affects in a wireless communication, and to provide comparative experiments to demonstrate the potential benefit of using MLS for secured group wireless communication, this research can help facilitate discussion in the DoD regarding the development of military tools using MLS.

5.2 Future Work

The future work proposed here aims to deepen our comprehension of how varying test conditions, scaling network environments, and refining data transmission methodologies impact protocol desirability, especially in terms of RF footprint. The insights gained from these research directions could significantly influence the development of next-generation wireless communication technologies, making them more resilient to diverse operational demands and environmental conditions.

Testing Variations

An additional avenue for future research that emerges from this thesis is the exploration of varied testing conditions and scenarios to assess their impact on the performance of TLS and MLS protocols. This investigation would involve altering the frequency and pattern of

messages sent within the network, deviating from the current test. By conducting tests with a greater number or different distribution of messages, and by varying the intervals between them, the research could uncover nuanced insights into how these changes affect the RF footprint.

Scaling Nodes

A critical area for future research based on this thesis project is scaling up the testing environment by incorporating more nodes (devices). This expansion would simulate more realistic and complex network scenarios, providing a broader understanding of how TLS and MLS protocols appear in power analysis under varied, denser network conditions. It could also offer insights into how network traffic, congestion, and RF footprint change with an increased number of devices.

Refining Data Transmission Methods

Another promising direction for future research is exploring ways to optimize data transmission for power analysis, particularly focusing on minimizing packet size or how protocols are used, contributing to Low Probability of Detection (LPD) and Low Probability of Intercept (LPI). Smaller packet sizes can reduce the RF footprint, making communication more covert and secure, which is crucial in sensitive communication scenarios. Investigating methods to reduce channel power without compromising data integrity and transmission quality is another key area. This could involve experimenting with other transport options like UDP or protocol selections such as emerging post-quantum solutions. Such research could lead to significant advancements in secure wireless communication, particularly in military or strategic applications where LPD and LPI are paramount. Understanding and optimizing these aspects of wireless communication can lead to more secure, efficient, and reliable communication systems, adaptable to various needs and environments.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] E. Ghashghai, *Communications Networks to Support Integrated Intelligence, Surveillance, Reconnaissance, and Strike Operations*. Santa Monica, CA: RAND Corporation, 2004.

[2] J. Choi, D. Park, S. Kim, and S. Ahn, "Implementation of a noise-shaped signaling system through software-defined radio," *Applied Sciences*, vol. 12, no. 2, 2022. Available: https://www.mdpi.com/2076-3417/12/2/641

[3] W. Eddy, "Transmission Control Protocol (TCP)," RFC 9293, Aug. 2022. Available: https://www.rfc-editor.org/info/rfc9293

[4] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018. Available: https://www.rfc-editor.org/info/rfc8446

[5] R. Barnes, B. Beurdouche, R. Robert, J. Millican, E. Omara, and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol," RFC 9420, July 2023. Available: https://www.rfc-editor.org/info/rfc9420

[6] C. J. Weisman, *The Essential Guide to RF and Wireless*, 2nd ed. USA: Prentice Hall PTR, 2002.

[7] W. Stallings, *Data and computer communications*, 10th ed. New Delhi: Pearson Education, c2014.

[8] R. Radhakrishnan *et al.*, "Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view," *CORE*, 2016. Available: https://core.ac.uk/download/pdf/148688059.pdf

[9] C. Cremers, B. Hale, and K. Kohbrok, "The complexities of healing in secure group messaging: Why cross-group effects matter," Cryptology ePrint Archive, Paper 2019/477, 2019. Available: https://eprint.iacr.org/2019/477

[10] "OSI reference model." [Accessed Online 2023]. Available: https://www.freeccnastudyguide.com/study-guides/ccna/ch1/1-3-osi-reference-model/

[11] NASA, "9.0 Communications - State-of-the-Art of Small Spacecraft Technology." [Accessed Online 2023]. Available: https://www.nasa.gov/smallsat-institute/sst-soa/soa-communications/

[12] S. Seetharaman, “Antenna Fundamentals & basic aerial theory.” [Accessed Online 2023]. Available: https://www.linkedin.com/pulse/antenna-fundamentals-basic-aerial-theory-s-seetharaman

[13] L. Goleniewski, *Telecommunications Essentials, Second Edition: The Complete Global Source*. Addison-Wesley Professional, 2006.

[14] K. Chang, *RF and Microwave Wireless Systems*. Wiley-Interscience, 2000.

[15] R. L. Freeman, *Fundamentals of Telecommunications, 2nd Edition*. Wiley-IEEE Press, 2004.

[16] N. Nkordeh, J. Olatunbosun, I. Bob-Manuel, and O. Oni, “Analysis of mobile networks signal strength for gsm networks,” in *Proceedings of The World Congress on Engineering and Computer Science 2016*, 10 2016.

[17] S. R. Best and H. R. Stuart, “The relationship between bandwidth and quality factor for electrically small antennas exhibiting closely spaced resonances,” in *2007 International workshop on Antenna Technology: Small and Smart Antennas Metamaterials and Applications*, 2007, pp. 27–30.

[18] X. Huang, Y. Chen, and Y. Wang, “Simulation of interference effects of uwb pulse signal to the gps receiver,” *Discrete Dynamics in Nature and Society*, vol. 2021, pp. 1–8, 07 2021.

[19] IEEE, “OSI: The Internet That Wasn’t.” [Accessed Online 2023]. Available: https://spectrum.ieee.org/osi-the-internet-that-wasnt

[20] “OSI Model – Practical Networking.net.” [Accessed Online 2023]. Available: https://www.practicalnetworking.net/series/packet-traveling/osi-model/

[21] B. Beurdouche, E. Rescorla, E. Omara, S. Inguva, and A. Duric, “The Messaging Layer Security (MLS) Architecture,” Internet Engineering Task Force, Internet-Draft draft-ietf-mls-architecture-10, Dec. 2022, work in Progress. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-architecture/10/

[22] IETF, “The internet engineering task force (IETF) - about.” [Accessed Online 2023]. Available: https:///www.ietf.org/about/

[23] C. Allen and T. Dierks, “The TLS Protocol Version 1.0,” RFC 2246, Jan. 1999. Available: https://www.rfc-editor.org/info/rfc2246

[24] D. Marchsreiter and J. Sepúlveda, “Hybrid Post-Quantum Enhanced TLS 1.3 on Embedded Devices,” in *2022 25th Euromicro Conference on Digital System Design (DSD)*, 2022, pp. 905–912.

[25] B. L. Laird, "A comprehensive review of internet of things waveforms for a DOD low earth orbit cubesat mesh network," Dec. 2022. Available: https://hdl.handle.net/10945/71494

[26] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-Efficient Datagram Transport Layer Security for the Internet of Things," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[27] F. J. Aufa, Endroyono, and A. Affandi, "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm," in *2018 4th International Conference on Science and Technology (ICST)*, 2018, pp. 1–5.

[28] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, "A comprehensive symbolic analysis of tls 1.3," in *ACM SIGSAC Conference on Computer and Commuincations Security*. ACM, Oct. 2017, pp. 1773–1788.

[29] S. Garfinkel and G. Spafford, *Web Security, Privacy Commerce*, 2nd ed. O'Reilly Media, 2002. Available: https://www.oreilly.com/library/view/web-security-privacy/0596000456/apbs02.html

[30] Microsoft, "Message Authentication Codes in Schannel." [Accessed Online 2023]. Available: https://learn.microsoft.com/en-us/windows/win32/secauthn/message-authentication-codes-in-schannel

[31] J. Fulp, "Crypto principles," Lecture Notes, Naval Postgraduate School, CS3690 Network Security, August 2022.

[32] R. Barnes, B. Beurdouche, R. Robert, J. Millican, E. Omara, and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol," Internet Engineering Task Force, Internet-Draft draft-ietf-mls-protocol-18, Mar. 2023, work in Progress. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/18/

[33] "Microsoft Developer Network, Chapter 3: Implementing Transport and Message Layer Security." [Accessed Online 2023]. Available: http://msdn2.microsoft.com/en-us/library/aa480582.aspx

[34] E. Omara and R. Robert, "The Messaging Layer Security (MLS) Federation," Internet Engineering Task Force, Internet-Draft draft-ietf-mls-federation-03, Sep. 2023, work in Progress. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-federation/03/

[35] A. Leon and C. J. Britt, "UXS authentication and key exchange requirements for multidomain operation and joint interoperability," 2022-06. Available: https://hdl.handle.net/10945/70738

[36] T. Wallez, J. Protzenko, B. Beurdouche, and K. Bhargavan, "TreeSync: Authenticated Group Management for Messaging Layer Security," Cryptology ePrint Archive, Paper 2022/1732, 2022. Available: https://eprint.iacr.org/2022/1732

[37] D. D. Clark, "The Design Philosophy of the DARPA Internet Protocols," *ACM SIGCOMM Computer Communication Review*, vol. 18, no. 4, pp. 106–114, 1988. Available: https://people.eecs.berkeley.edu/~sylvia/cs268-2019/papers/darpa-internet.pdf

[38] V. Cerf and R. Kahn, "A protocol for packet network intercommunication," *IEEE Transactions on Communications*, vol. 22, no. 5, pp. 637–648, 1974.

[39] M. Decina and V. Trecordi, "Convergence of telecommunications and computing to networking models for integrated services and applications," *Proceedings of the IEEE*, vol. 85, no. 12, pp. 1887–1914, 1997.

[40] K. Hewage, "Towards secure synchronous communication architectures for wireless networks," *Proceedings of the IEEE*, 2023. Available: https://uu.diva-portal.org/smash/get/diva2:1776132/FULLTEXT01.pdf

[41] B. Villain, "New generation of network access controller : An SDN approach," Theses, Université Pierre et Marie Curie - Paris VI, Oct. 2015. Available: https://theses.hal.science/tel-01368098

[42] "What is Transmission Control Protocol (TCP)?" [Accessed Online 2023]. Available: https://webhostinggeeks.com/blog/what-is-transmission-control-protocol-tcp/

[43] "User Datagram Protocol," RFC 768, Aug. 1980. Available: https://www.rfc-editor.org/info/rfc768

[44] "Networking Knowledge Base: UDP." [Accessed Online 2023]. Available: https://community.cisco.com/t5/networking-knowledge-base/udp/ta-p/3114870

[45] A. Gabrielson and H. Levkowitz, "Integrating network cryptography into the operating system," in *2012 IEEE Sixth International Conference on Software Security and Reliability Companion*, 2012, pp. 7–11.

[46] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, Jan. 2012. Available: https://www.rfc-editor.org/info/rfc6347

[47] Cadence Design Systems, "RF Interference: Types and Effects." [Accessed Online 2023]. Available: https://resources.pcb.cadence.com/blog/2022-rf-interference-types-and-effects

[48] "Signal Hound's Spike Spectrum Analyzer Software." [Accessed Online 2023]. Available: https://signalhound.com/spike/

[49] "Wireshark." [Accessed Online 2023]. Available: https://www.wireshark.org/

[50] Python, "The official home of the Python Programming Language." [Accessed Online 2023]. Available: https://www.python.org/

[51] Python, *ssl — TLS/SSL wrapper for socket objects.*, [Accessed Online 2023]. Available: https://docs.python.org/3/library/ssl.html#ssl.PROTOCOL_TLS

[52] "Rust Programming Language." [Accessed Online 2023]. Available: https://www.rust-lang.org/

[53] "Secpubsub," [Created 2023]. Available: https://gitlab.nps.edu/jwl/secpubsub

[54] OpenMLS, "An open-source implementation of the Messaging Layer Security protocol," [Accessed Online 2023]. Available: https://openmls.tech/

[55] "TLS code on Gitlab," [Created 2023]. Available: https://gitlab.nps.edu/chingting.yuan/thesis

[56] Broadcom, "How to create a self-signed SSL certificate." [Accessed online 2023]. Available: https://knowledge.broadcom.com/external/article/166370/how-to-create-a-selfsigned-ssl-certifica.html

[57] Federal Communications Commission, "Title 47 CFR Part 15 - Radio Frequency Devices." [Accessed online 2023]. Available: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15

[58] A. Jablonski and K. Dziedziech, "Intelligent spectrogram – A tool for analysis of complex non-stationary signals," *Mechanical Systems and Signal Processing*, vol. 167, p. 108554, 2022. Available: https://www.sciencedirect.com/science/article/pii/S0888327021008931

[59] Signal Hound, *Spike User Manual*, [Accessed Online 2023]. Available: https://signalhound.com/sigdownloads/Spike/Spike-User-Manual.pdf

[60] Keysight Technologies, "Understanding the fundamental principles of vector network analysis," [Accessed Online 2023]. Available: https://www.keysight.com/us/en/assets/7018-06714/application-notes/5952-0292.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California