2019-06

FREE SPACE OPTICS IMPLEMENTATION OF THE NETWORK STACK WITHIN AN RF-DENIED ENVIRONMENT

Naski, Timothy R.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FREE SPACE OPTICS IMPLEMENTATION OF THE NETWORK STACK WITHIN AN RF-DENIED ENVIRONMENT

by

Timothy R. Naski

June 2019

Thesis Advisor: Gurminder Singh
Co-Advisor: Peter R. Ateshian

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE FREE SPACE OPTICS IMPLEMENTATION OF THE NETWORK STACK WITHIN AN RF-DENIED ENVIRONMENT			**5. FUNDING NUMBERS**
6. AUTHOR(S) Timothy R. Naski			
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)

The objective of this research is to understand the abilities and limitations of communication in a radio frequencies (RF)-denied environment, especially with regard to the network stack. The next generation of warfare with another state actor will require non-traditional communication and extra security methods. RF and wired communications can be destroyed, jammed or not suitable. Free-space optics (FSO) provides the potential for high-speed communication between networks in an RF-denied environment. A visual link of an array of lasers can send data by oscillating visual patterns at high frequencies and cannot be captured without the enemy being directly between transmitter and receiver. This research explores the usage of FSO with traditional network-based protocols. The results show that it is possible to achieve two-way visual communication using FSO and traditional network protocols. Hardware currently limits the visual link capacity, preventing acceptable data rates for normal network operations. This thesis recommends hardware updates that can advance this system to acceptable network speeds. With the implementation of specialized hardware and software, FSO visual communication can support high internet bandwidths with integrated physical security.

14. SUBJECT TERMS line of sight communication, QR code, RF-denied environment			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

FREE SPACE OPTICS IMPLEMENTATION OF THE NETWORK STACK WITHIN AN RF-DENIED ENVIRONMENT

Timothy R. Naski
Ensign, United States Navy
BSE, U.S. Naval Academy, 2018

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2019

Approved by: Gurminder Singh
Advisor

Peter R. Ateshian
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The objective of this research is to understand the abilities and limitations of communication in a radio frequencies (RF)-denied environment, especially with regard to the network stack. The next generation of warfare with another state actor will require non-traditional communication and extra security methods. RF and wired communications can be destroyed, jammed or not suitable. Free-space optics (FSO) provides the potential for high-speed communication between networks in an RF-denied environment. A visual link of an array of lasers can send data by oscillating visual patterns at high frequencies and cannot be captured without the enemy being directly between transmitter and receiver. This research explores the usage of FSO with traditional network-based protocols. The results show that it is possible to achieve two-way visual communication using FSO and traditional network protocols. Hardware currently limits the visual link capacity, preventing acceptable data rates for normal network operations. This thesis recommends hardware updates that can advance this system to acceptable network speeds. With the implementation of specialized hardware and software, FSO visual communication can support high internet bandwidths with integrated physical security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

5G	Fifth Generation
AI	Artificial Intelligence
API	Application programing Interface
ASIC	Application-Specific Integrated Circuits
ASK	Amplitude-Shift Keying
BPPM	Binary Pulse Position Modulation
CPU	Central Processing Unit
CRC	Cyclical Redundancy Checking
ECC	Error Correction Capabilities
FCS	Frame Check Sequence
FPGA	Field Programmable Gate Arrays
FPS	Frames Per Second
FSK	Frequency- shift Keying
FSO	Free Space Optics
FSPL	Free Space Propagation Loss
GPU	Graphical Processing Unit
ICMP	Internet Control Message Protocol
LED	Light Emitting Diode
LFSR	Linear-Feedback Shift Register
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
NIC	Network Interface Controller
PSK	Phase- Shift Keying
QR	Quick Response
OSI	Open Systems Interconnection
PV	Photovoltaics
RF	Radio Frequencies
SISO	Single Input Singe Output

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus

EXECUTIVE SUMMARY

The next generation of warfare is expected to be characterized by a loss of traditional communications and tactics. Radio frequency (RF) and wired communications will be destroyed, jammed, or not suitable in mobile environments. Nevertheless, forces require secure and fast methods of communication to maintain capabilities. Requiring a technology capable of achieving high data rates and security but maintaining the status quo of military tactics. Free space optics (FSO) has the capability to achieve Gigabit/sec data rates, similar to modern high speed wired internet connections, with physical security. A visual link, of an array of lasers, can send data by oscillating patters at high frequencies. This data cannot be captured or decoded unless the enemy moves between the receiver and transmitter, providing a level of physical security. Creating a fast secure method of transmitting data between points without changing network protocols.

The objective of this research is to understand the abilities and limitations of communication within an RF-denied environment, especially with regard to the network stack. The next generation of warfare with another state actor, will require non-traditional communication and extra security methods. FSO provides these capabilities, and has the potential to provide high-speed communication between networks. This research looks at the limitations of this system, and how it is used with traditional network based protocols. The goal is to determine the viability of this system, without recreating internet protocols.

The results show that it is capable of achieving two-way visual communication using a FSO system. This is essential as two way communication is required with traditional internet protocols in any network link. This ensured that new protocols will not need to be developed for an FSO system. Hardware currently limited the system and preventing acceptable data rates for normal network operation. This thesis recommends hardware updates which, with over the counter equipment, will advance this system to network speeds. With the implementation of specialized hardware and software, FSO visual communication can create a network link with the desired high internet bandwidths.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge all of the people who have helped me on this long journey through all of the ups and downs, getting me to the place where I have completed my master's thesis. After all of these years of education, I can safely say that this is the largest project I have ever completed.

I would like to thank my family for supporting me, helping me and pushing me to become the person who I am today. They pushed me for my own good, even if it was kicking and screaming.

I would like to thank all of my friends and girlfriend, Kylie Bradley, for dealing with me. She gave me a hand when things were tough and motivated me when necessary.

I would not be where I am without the individuals who have helped me along the way. These people helped me mature and develop, and even have some fun. Whether friends or family, thank you for the patience and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The use of free space optics (FSO) has become a more viable option compared to those that use radio frequency (RF) technologies such as cellular, radio, and satellite. Although fifth generation (5G) cellular technology seems to provide the capabilities of gigabit/sec data rates, there are significant range limitations and the required infrastructure is expensive and tough to build. 5G cellular technologies seems to provide the next generation of communication, but it may be years away from everyday usage. FSO has the capabilities to reach the same data rates as those of RF technologies with increased security and confidentiality. This is due to the directionality of these systems, making them useful for specific industrial and military applications.

In industry FSO is being tested in terms of the transmission of data though various types of mediums including air, space, and water. There is investigation into sending data between buildings in large cities, where infrastructure is expensive and difficult to implement. A FSO connection can act like a physical cable, capable of achieving very high data rates, but not requiring the direct wiring between stations. Currently, there is a large investment in communication with satellites. The thought is that it is possible to achieve high data rates with satellites by using long-range RF communications.

Domains all across the military would gain a great deal from the use of FSO for secure communication with drones, satellites, forward operating units, and submarines. FSO does not require the amount of traditional infrastructure of RF communication, but has the ability to transmit at higher data rates. FSO just requires the moveable infrastructure of a transmitter and receiver to connect to a network. These transmitters can be portable for less sophisticated usage and at shorter distances. This type of communication has the ability to transmit in domains that are currently unavailable, such as underwater.

A. PROBLEM STATEMENT

The purpose of this thesis is to identify and develop a method for using FSO in an RF-denied environment capable of two-way communication, and that connects with the network stack. This is done with commercially available equipment to prove that two-way communication between tactical and internet networks is possible via a FSO connection.

B. OBJECTIVES

The objective of this thesis is to create and understand the method of developing a FSO capable system of interconnecting networks. Networks are not natively capable of using other methods of connection, and hardware developed by companies is not developer friendly. The network connection via FSO must be developed from the ground up, allowing data to pass between the systems. The objective is to create a system that can hook into the network stack, allowing data to flow between two separate networks. Furthermore, this thesis will determine the capabilities of this proof-of-concept connection, and uncover possible bottlenecks when developing a field-implemented system.

C. SCOPE

The scope of this thesis is to look at the effects of the proof-of-concept, and how the ideas learned can be transferred to future generations. This limits the capabilities of the system and will not result in the use of true, expected traffic on the system. Furthermore, the equipment that is chosen will not be expected to establish the connections expected for real implementation.

D. ORGANIZATION

The origination of this thesis is into five different chapters, including this chapter. Chapter II discusses prior work within academia on the use of FSO and network capabilities. The next chapter, Chapter III, lays out the proposed experiments and equipment used. Chapter IV will discuss the results of the two-way communication system and conclusions based upon those results. The final chapter, Chapter V, will give overarching conclusions for this thesis including future work.

II. BACKGROUND

This chapter describes the basics of networking. Networking is used to properly and efficiently transmit data across an optical link. There are currently multiple methods that solve the challenge of passing network packets, and this thesis will leverage the positives of each. To understand what this thesis attempts to leverage, adequate background information on prior work in this area is provided. The chapter sets a foundation by covering the basics of FSO and the comparison of FSO to traditional methods of sending data. Data encoding methods within the signal, the effects of the environment, and possible solutions to these problems are discussed.

A. FSO BASICS

FSO has the ability to leverage large ranges of technological advancements to develop new versions of data transfer. Visual data transfer has been around for years, but there has been minimal advancement due to low data rates. Currently, FSO has an essential niche within data communication for warfighting, providing capabilities that would be impossible with traditional wireless data transfer.

1. Warfare Relation to FSO

Modern warfare relies on sophisticated autonomous systems and instantaneous communication. These systems require constant data input from systems such as GPS, satellite communications, RF communications, and visual imagery. The constant input of data allows the systems to become more accurate, precise, and keep the warfighter informed. The individual warfighter has become reliant on this constant presence of information and communication. This data could be used to send or receive data from a drone, an aircraft flying overhead, or a ship in the ocean, providing situational awareness and knowledge of threats over the horizon [1].

2. Data Modulation

Data is transferred between entities in multiple ways, but the most common is via radio frequencies. Data is transmitted via a model called frequency modulation or wavelength modulation. Wavelength modulation is the oldest version of the modulation schemes, used in AM radio, and can only hold a limited data rate. This is where the wavelength is modified to encode ones and zeros. The frequency modulation, used in FM radio, has the ability to hold much higher data rates. In this scheme, the data is combined with the carrier signal by adjusting the carries frequency [2]. Visually, this is displayed in Figure 1, where the data signal and carrier are combined to create the modulated signal. The data signal can be visualized in a graph shown by the red line. The carrier can be any frequency depending on the needs of the signal and is demonstrated in the brown wave. Radio waves and light waves can also be this baseline carrier frequency. The modulated signal, shown in the blue, orange, and gray lines, is the combination of the data signal and the carrier signal. When a one is sent, the modulated signal is set to a high frequency, while when a zero is sent, the modulated signal is set to a lower frequency for the frequency-shift keying (FSK) scheme [3]. Alternative schemes include amplitude-shift keying (ASK) which changes wavelength and phase-shift keying (PSK) which shifts the phase. This is the most common way of encapsulating data and at higher frequencies more data can be encoded.

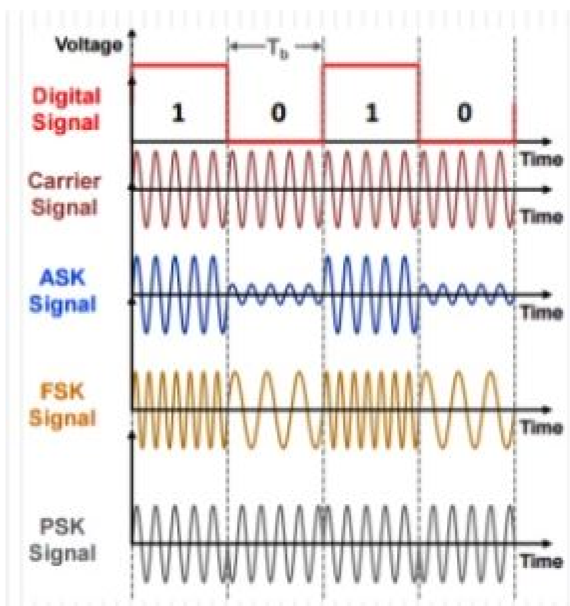

Figure 1. Data Modulation. Source: [3].

3. Frequency Spectrum

Different frequencies have different benefits based upon attenuation and range. Table 1 suggests that radio waves may provide the greatest range because of the large wavelengths that are possible; however, radio waves are not able to encode as much data as other methods, such as mobile frequencies. The mobile and satellite frequencies, which are between 300 MHz and 300 GHz, have the ability to encode much more information, but suffer from large losses from attenuation [4]. Depending on the usage, specific frequencies must be selected to best maximize the system. This may be to either increase data rates, or decrease losses due to attenuation.

Table 1. Waves and Their Characteristics. Source: [4].

Waves	Wavelength	Frequency	Period	Characteristics
Radio waves	100 km–1 m	10 kHz– 300 MHz	100 ns–0.1 ms	Radio FM, AM, and TV
Microwaves	1 m–1 mm	300 MHz–300 GHz	3 ps–100 ns	Mobile, satellite, radar
Infrared	1 mm– 0.8 μm	300 GHz–300 THz	3 fs–3 ps	Laser, night sight, telemeter
Visible light	400–800 nm	Energy in electron-volts (eV) –1 to 5 eV	1–3 fs	Laser, Sun, lamps
Ultraviolet	400–0.5 nm	5–1 keV	1.7as to 1 fs	Laser, lamps
X-rays	50–0.1 pm	1–100 keV	0.0003–1.7 as	X-ray tubes
Gamma-rays	<0.1 pm	>100 keV	< 0.0003 as	Radiation of energetic particles, synchrotrons

4. Loss Based on Propagation

The free space propagation loss (FSPL) equation,

$$FSPL = \left(\frac{4\pi d}{\lambda}\right)^2 \qquad (1)$$

, shows that loss is directly related to the distance (d) between systems and inversely related to wavelength (λ). This means that over the same distance the system which emits the smaller wavelength, thus higher frequency, will have a higher propagation loss. This equation could also be used to infer that if a system requires a minimal amount of propagation loss (FSPL kept constant), Equation 1 can be manipulated to look like

$$\boldsymbol{d} = \frac{\lambda\sqrt{FSPL}}{4\pi} \tag{2}$$

. This shows that the distance which data could be received is directly proportional to the wavelength. This means that radio waves, with the highest wavelength, would have the greatest distance of usable data transmission [5].

5. Real-World Wireless Technology Requirements

High-frequency data transmissions continue to have an increasing influence in civilian and military life. Cellular data has been on the forefront of modern wireless technology, as 5G poses to present the next generation of wireless data transfer. This technology presents a wave with a frequency of 20 GHz, data transfers of up to 1Gbps, minimal latency, and little user limitations. With such promised abilities, society has become complacent with modern methods of data transfer. However, in the military, the warfighter must be able to complete the mission no matter the situation. How will the warfighter react in an RF-denied environment if they are no longer are able to access traditional methods of communication and data transfer?

When looking at the problem of the best way to transfer data in an RF-denied environment, the warfighter must look at alternative methods of transmitting data. The second most prevalent method of data transfer behind RF is through the use of visual signals. Transferring data via visual signals has been around for thousands of years. Cities used to communicate via signal fires to determine if danger is eminent. Ships use signal flags and lights to communicate. Modern technology has opened possibilities to overcome past methods of data transfer; these provide the potential for high data rates to the horizon [6].

a. *Comparison of Wireless and Optical Links*

When comparing the merits of wireless infrared and wireless optic methods, both have beneficial features. Table 2 includes a small number of the possible attributes that should be compared when looking at the differences between infrared and optics. Although this table may give the impression that wireless optics has many of the abilities of infrared technology, it is very unlikely that wireless optics will become widespread in modern society [4]. This is due to the directionality of wireless optics. The transmitter must be pointed in the direction of the receiver for successful communication, making it challenging to market for the common consumer. This directionality is actually a significant advantage for military applications, keeping unnecessary data, even if it is encrypted, out of enemy's hands.

Table 2. Wireless and Optical Links Comparison. Source: [4].

Features	Radio 60 GHz	Wireless Optic
Spectrum availability	Reduced	Abundant
Spectrum regulation	Restricted	Free
Spectrum fee	Important to free	Free
Multipath fading	Very important	None
Data security	Encryption	Intrinsically secure by the walls
Intersymbol interference	Low	Potentially significant at high speed
Created or suffered electromagnetic interference	Possible if similar frequency or harmonic	None
Dominant noise	Other users	Artificial light and daylight
Human safety	Epidemiological study ongoing	Safety (Class 1) Internationally accepted standards

RF wireless data transfer has significant advantages over optical wireless data transfer. Companies with technologies approaching 5G capability boast potential 1 Gbps peak and 100 Mbps sustained data rates, while current optical methods cannot match these data rates. This is because data must be transferred with Morris code type data transfer, using fast switching of the light source to encode data. To maximize the effectiveness of these systems, some of the signal is used for error correction. The United States Marine Corps has developed a system (TALON) that uses free space optical technology to send a high-power laser between ground-to-ground equipment. This system has the potential to be used in an RF-denied environment, but supports a limited data rate of 880 Mbps.

6. Single Input Single Output versus Multiple Input Multiple Output

The FSO system used by the Marine Corps. (TALON) has a low data rate because the only way to send data is through turning the laser on and off. Although at maximum frequency the system can be oscillated at several thousand Hz, this data rate is low compared to other wireless data transfer techniques. The obvious solution would be to have multiple FSO systems, running in parallel to increase the data rate. This provides a good comparison between single input single output systems and multiple input multiple output systems, where there are pros and cons to both systems [7].

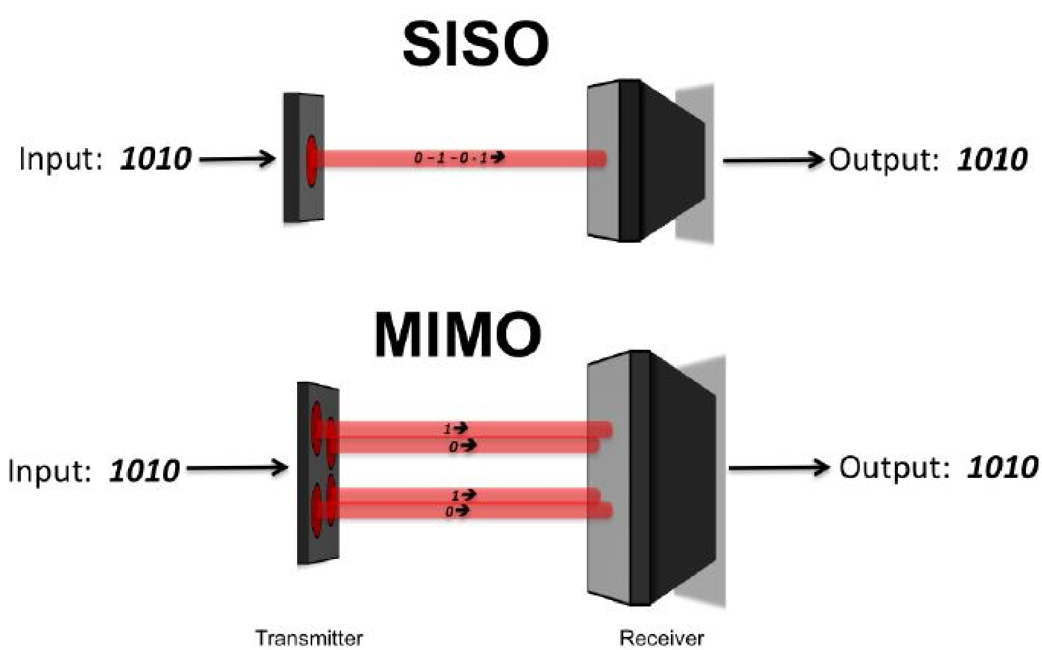

Figure 2. MIMO versus SISO. Source: [7].

a. Single Input Single Output

Many FSO operations are inherently a single input single output (SISO) system, in which there is one transmitter and the system has the ability to receive a single data stream. This means that these systems are only able to handle a single bit at a time. These systems can be very efficient depending on the data stream, as shown in modern cellular technology. The data rates depend on the transfer method, as demonstrated with frequency modulation, or the limits on the receiver.

Physical light waves, such as those found in FSO systems, have limitations in their modulation because the light wave will be the carrier signal and cannot be easily frequency modulated. Instead, light waves will be modulated by actuating the light wave on and off. This creates a signal of flashes for the data wave. Modern technology allows lasers to be actuated at frequencies of hundreds to thousands of hertz, requiring that the receiver be able to distinguish these oscillations or lack thereof [7].

b. Multiple Input Multiple Output

Multiple input multiple output (MIMO) systems have the ability to send and receive multiple signals at the same time. This results in much higher data rates as the system has the ability to inherently input and output multiple SISO systems. The receiver must have the ability to distinguish between multiple different input signals. These signals must be decoded independently, and then stitched back together to create the data signal. When transmitting a MIMO signal, the system must be able to divide and independently send the data signal.

The process of sending and receiving data in a MIMO system has many different problems, which makes the system more complex. The most basic process of receiving multiple signals can be a difficult problem, as these signals can interfere with each other or the environment, making it difficult to properly distinguish the multiple signals. The system also requires significant amounts of overhead to break the data signal, stich the data signal together, and deal with errors in transmission. Many of these problems are inherently difficult like specifically combining data signals. Combining multiple data signals may require advanced timing techniques or protocol schemes. Small errors or deviations can lead to failure of the entire system because data is no longer arriving properly at the end of the system [7].

c. Use of MIMO/SISO in FSO

Since a MIMO system is difficult to use and create, a SISO system may be more desirable in many situations. To increase the data rate for a system, it is easier to increase the frequency rather than adding multiple signals. This is demonstrated in cellular devices, as increases in data rates come from higher data modulation SISO schemes rather than from a MIMO system.

7. QR Codes

As discussed previously, FSO systems are limited by their SISO data rates, and it is impossible to increase data rates via traditional techniques. The best-case scenario is to use a MIMO system, but keep the simplicity of SISO systems. This could be possible using wireless optical systems by sending more than one laser in specific patterns to encode data, such as bar codes or QR (quick response) codes. Each of these systems has the ability to encode more data than individual lasers and have certain amounts of error correction. While sending a QR code, the encoding or decoding data problem of MIMO systems will be solved, as these systems provide an efficient method to synchronize the data [8]. This means that a QR code has the ability to receive/send multiple inputs/outputs as if they are a single input/output, while including necessary amounts of error corrections.

a. Possible Data Encoding Methods

Table 3 presents the amount of data in which different types of codes can encode, as well as other features. The QR code has become the best of all codes, allowing for large capacity, small size, and high-speed scanning.

Table 3. Comparison of Encoding Methods. Source: [9].

		QR Code	PDF417	DataMatrix	MaxiCode
Developer		DENSO Wave	Symbol Technologies	RVSI Acuity CiMatrix	UPS
Type		Matrix	Stacked barcode	Matrix	Matrix
Data capacity	Numeric	7,089	2,710	3,116	138
	Alphanumeric	4,296	1,850	2,355	93
	Binary	2,953	1,018	1,556	-
	Japanese, Chinese or Korean characters	1,817	554	778	-
Main features		Large capacity, small size, high-speed scanning	Large capacity	Small size	High-speed scanning
Main applications		All categories	Office automation	Factory automation	Logistics
Standards		AIM, JIS, ISO	AIM, ISO	AIM, ISO	AIM, ISO

b. Data Capabilities of QR Codes

With the implementation of QR codes, it is feasible to transfer larger amounts of data via wireless optical links. The amount of data which is sent, can also be limited by the size of the code or the level of error correction capabilities (ECC) shown in Table 4. In this case, ECC level L provides approximately seven percent correction, while level H can correct approximately 30%. The amount of error correction is inversely proportional to the amount of data which can be sent via the QR code.

Table 4. QR Code and Data Encoded. Source: [10].

Version	Modules	ECC Level	Data bits (mixed)	Numeric	Alphanu-meric	Binary	Kanji
1	21×21	L	152	41	25	17	10
		M	128	34	20	14	8
		Q	104	27	16	11	7
		H	72	17	10	7	4
2	25×25	L	272	77	47	32	20
		M	224	63	38	26	16
		Q	176	48	29	20	12
		H	128	34	20	14	8
3	29×29	L	440	127	77	53	32
		M	352	101	61	42	26
		Q	272	77	47	32	20
		H	208	58	35	24	15

If a wireless link has the ability to send, encode, receive, and decode QR codes at a high refresh rate, then this system could provide basic link functions. Lasers, which are oriented into a matrix to display QR codes, have this potential for high refresh rates and therefore high data rates. Receivers, such as high-speed cameras, have the ability to take images at multiple times greater than this, making it possible to transfer data.

8. Losses in a FSO Environment

A FSO system is feasibly possible as long as modern technology allows for data to be transferred at a high enough data rate. This system would work within ideal conditions, but these are not the conditions which it will need to work within. The atmosphere and environment can cause significant losses when trying to transfer data. To minimize these effects, there are ideal bands in which to send data.

a. Effects of Atmospheric Particles

The atmosphere is made up of molecules including water, oxygen, carbon dioxide, and nitrogen. Although these particles are necessary for us to survive, they limit the transmission of waves within in an environment. This process of restricting wave transmission is called attenuation, and is made up of absorption, scattering, refraction, and reflection. Waves moving through the atmosphere can be absorbed by these elemental particles. They could be scattered or refracted as waves interact with atmosphere particles, no longer reaching the desired source. Waves could also be reflected by particles within an environment. Light and infrared waves suffer from large amounts of attenuation at different wavelengths in the atmosphere [11]. This difference is due to the makeup of the atmosphere, as demonstrated in Figure 3.

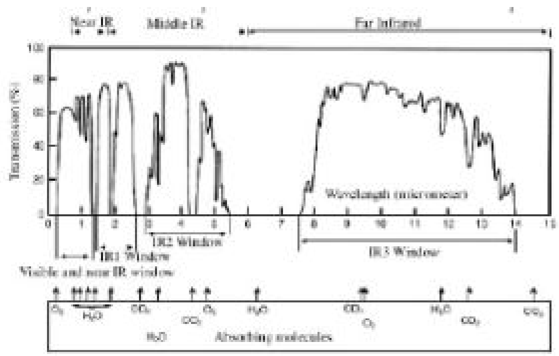

Figure 3. Losses as a Result of the Atmosphere. Source: [4].

b. Effects of Fog and Haze on FSO

FSO systems require good operating environments in order to best transfer their data. The signal has to constantly deal with atmospheric attenuation based upon the makeup of the atmosphere. This is independent of other weather effects within that environment. FSO systems are impossible to use within an environment with heavy haze or fog. This is because the molecules in the air absorb or reflect all of the signal.

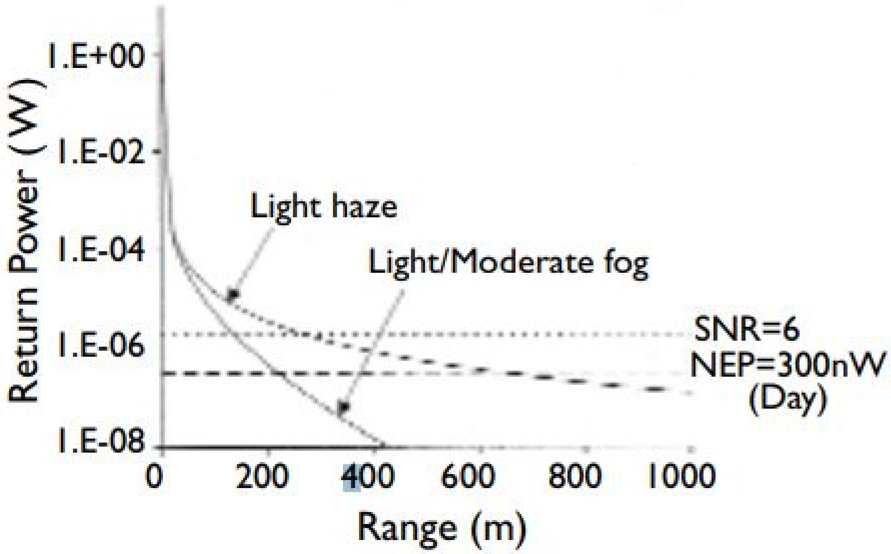

Figure 4. Effect of Fog and Haze on FSO. Source: [12].

Figure 4 shows the effect of a light haze or light/moderate fog when the signal is being sent for a typical 0.85-μm LED (light emitting diode) FSO system, which has 40-mW power [12]. The system shows that it cannot be read at any distance over 300 m. The only solution to this problem is to send more power to overcome losses, or use a wavelength that is less effected by the haze or fog. Nevertheless, the effects of environmental factors must be considered when evaluating the effectiveness of a FSO system.

c. Desirable Wavelengths due to Atmosphere

It will be essential for a FSO system to work within a warfighting system, especially where there could be large amounts of loss. In a naval environment, it can be expected that the system must perform where there is water vapor in the air. The limitations of the system must be considered and understood to best to create an effective system.

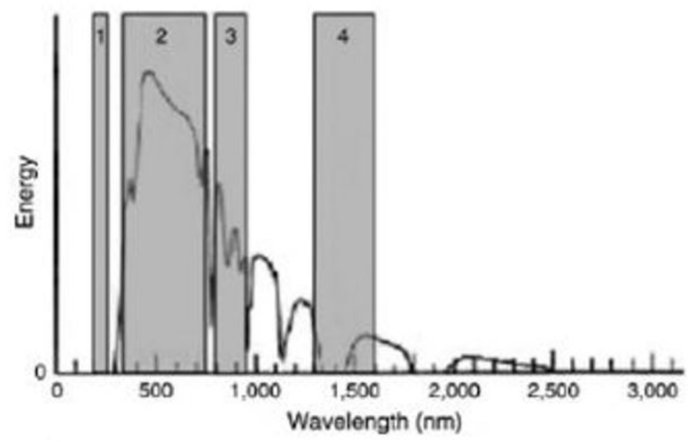

Figure 5. Desired Wavelength Bands for FSO. Source: [4].

Four separate bands can be chosen to transfer data within the environment, as shown in Figure 5. Each offers advantageous features within the parameters of eye safety, optical disrupting, optical link budget, complexity, transmission power, and sensitivity. Each of the bands is outlined in the diagram with the gray rectangular sections. Most optical wireless communications are found in the last three bands, incorporating visible light in lasers and infrared radiation. Depending on the requirements for the system and the resources for the project, there could be limits on which bands should be used.

9. Physical System for FSO

This thesis is focused on physical lasers as they give us the ability to easily establish an acceptable bandwidth data link within the budget for the project. Lasers provide the ability to send data via an optical link, but do not require exceptionally expensive equipment to create or receive the system. This type of system is not a new process, as data has been transferred via light since the early 1900s when FSO used light to transfer data for a telephone call. Modern data systems have the ability to have extremely high bandwidths, 0.1 to 1 Gbit/s, and at very low prices, approximately $1000 [12].

Most of the modern FSO systems use lasers between 0.8-µm and 1.5-µm diodes, operating at power levels on the order of 0.01 to 0.1 W up to 10 mW. New technology has allowed for modulation rates up to 100 MHz. Modern technologies have increased the prevalence of these systems, as lower power levels with higher modulation rates allow for higher data rates between multiple nodes.

B. WIRELESS AND WIRED PROTOCOLS

As discussed, before modern FSO systems can be adapted with the use QR codes, adequate data rates must be reached in a place between MIMO and SISO systems. In order to reach this situation, protocols must be created to best transfer data across a visual wireless link. The link will be inherently filled with loss, based on attenuation and the environment, so the 802.11 Wi-Fi protocol must be investigated. The link also must be simple and create a direct connection between nodes, just as the 802.3 Ethernet protocol. Therefore, the protocol created must be a combination of 802.11 and 802.3 to leverage their benefits.

1. Wireless Protocol

The 802.11 IEEE protocol standard enumerates the way in which wireless systems transfer data via the media access control (MAC) layer. This standard has created a process for properly and efficiently communicating within a network. By looking at a very specific portion of the protocol, fragmentation, much can be learned as to why this system has been created. Many times when there is not enough bandwidth to send an entire full packet or the system is operating in a heavy loss environment, fragmentation can be used to improve the overall throughput of the medium. Further improvements could be high efficiency, next generation high-speed WLANS or increased energy efficiency of the network.

a. Fragmentation

When looking at the basic fragmentation model proposed by the 802.11 protocol, the original packet is divided into multiple equal sized fragments, except for the last fragment which will contain less of the original packet. Each fragment contains its own MAC header and cyclical redundancy checking (CRC), as displayed in Figure 6. The header allows the system to correctly send the packet to the desired location and enable defragmentation, while the CRC aids in error checking of the fragment [13].

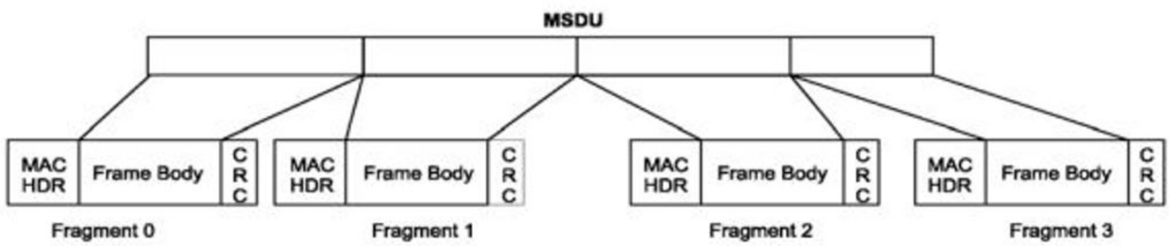

Figure 6. Fragmentation of MAC [13]

b. MAC Layer Protocol

The MAC header at the beginning of each fragment can contain information necessary for proper transmission of the packet seen in Figure 7. With traditional MAC headers, the first three (frame control, duration, address) and last three (height control, frame body, frame check sequence (FCS)) fields comprise the minimal MAC frame format. In this study, the use the sequence control frame is essential to assist in the fragmentation and defragmentation of a packet.

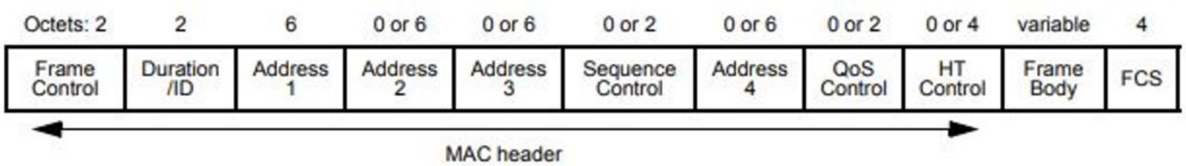

Figure 7. Mac Frame Header. Source: [14].

To develop the most dynamic and error resistant network, the system uses feedback to ensure delivery with more complex headers. This is especially beneficial if there are multiple users on a system, requiring de-confliction of multiple inputs. When considering the FSO with a single user and minimal loss, feedback is much less useful as it simply provides delivery. If there are multiple users on a system or errors in transmission, feedback is essential. This feedback is useful when errors on the network are larger than the ingrained error correction and if multiple users are connected with a single base node. For simplification, this study is only focused on a singular FSO, but will include the possibility of using a multiple FSO system in the future.

c. *Effects of Feedback*

Although feedback is not necessary, as shown in user datagram protocol (UDP), it helps to establish reliable packet delivery. Especially in FSO, where there can be loss due to attenuation or other atmospheric affects. Most traffic in the modern internet is encapsulated in transmission control protocol (TCP), demonstrating the need for reliable delivery. This feedback is also found within wireless networks, where feedback occurs when fragmented packets will arrive at the desired location.

2. Wired Protocol

The use of the 802.3 Ethernet protocol provides a good comparison to the 802.11 protocols, especially since the systems are created to solve different problems. The overhead in the Ethernet protocols is significantly smaller than those in Wi-Fi protocols as shown in Figure 8, as a result of wire reliability and efficiency. When sending data across a physical wire, the system deals with a single input, less noise, and an increased connection speed. The system does not need to process multiple signal inputs or deal with a link filled with loss [15].

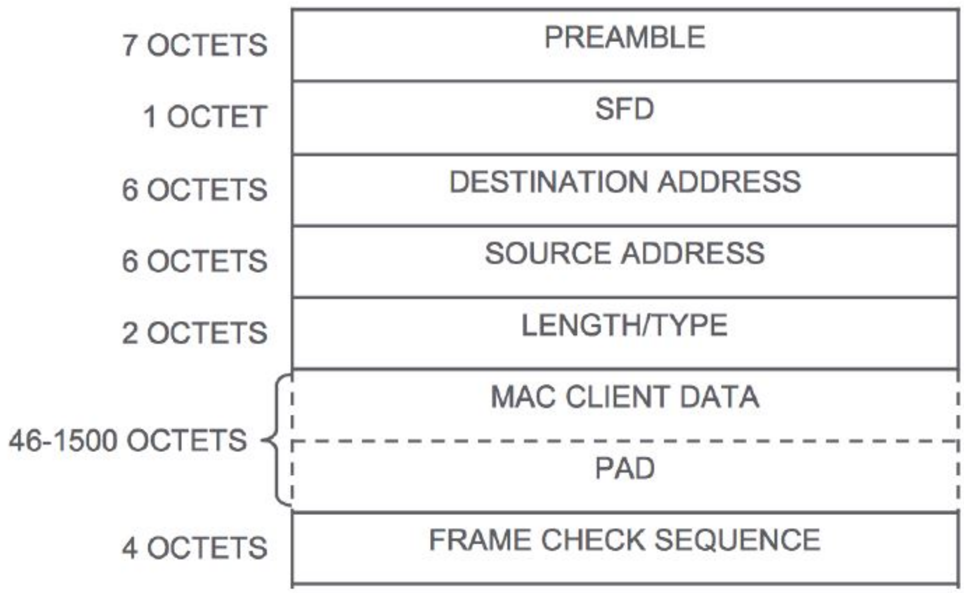

Figure 8. Ethernet Header. Source: [15].

The biggest drawback that comes from the use of the 802.3 protocol, with regard to FSO systems, is its inability to detect errors. When a packet has become corrupted on transmission, the packet will be dropped on arrival. This fault requires that higher layers must overcome these packet losses, and solve the retransmission. This comes as a result of the high reliability of wired networks, where the minimal packet loss makes the need for retransmission protocols unnecessary. The overhead for the retransmission protocols would create an excessive draw on the system compared with the occasional loss of packets.

3. Comparison between Wired and Wireless Protocols

When compared to Wi-Fi, which includes error correction and packet retransmission, Ethernet is built and developed for an entirely different environment. MAC level sequence numbers and headers, 802.11 ACKs, and retransmission fields allow for Wi-Fi to work within a high loss environment. Wi-Fi will detect errors within the system itself, allowing for more efficient retransmission, instead of having to rely on higher levels of the network stack.

Both of these protocols are created for their own individual type of network and help to make that specific network efficient and effective. In comparison, the 802.11 would not be an efficient protocol for a wired network, and the 802.3 protocol would not be an effective protocol in a wireless system. A FSO system can be characterized by a combination of both a wired and wireless network. For these reasons, it will be effective to include portions of each protocol, to maximize the ability for a FSO to realistically run application layer programs.

C. SUMMARY

Wireless optical data transfer has the ability to fill new design constraints given by the military, with the innovation ability in the physical layer. Instead of using traditional wireless radio communication, which can be intercepted or jammed, directed optical energy can be encoded with desired information. This creates data links with minimal to no chance of being intercepted and impervious to traditional methods of jamming. This system, based upon design constrains of the network model, innovates at the physical layer, allowing for minimal need to change other portions of the network.

When encoding the data which will be sent, each QR code can encapsulate only a certain amount of information based upon the size of the code. It is infeasible that a single QR code could encapsulate the entire network packet, especially if the packet contains the maximum 1500 bytes. Instead, QR codes must do what the network already does, and break the packet into manageable packets which can be reasonably encoded into QR codes. On the back end, the receiver will need to reassemble the original network packet before sending it to its destination.

The goals are to determine how the system will respond to different application layer programs and resolve whether this type of system could be suitable for military applications. The system has the inherent ability to send data across the link, but will the system be able to combine the technology of FSO with link layer protocols to best transfer data at suitable rates? Will the system be able to run within the most basic application layer programs?

III. SYSTEM DESIGN

This chapter discusses the design and implementation of the free space optics physical system. It addresses how the proof-of-concept design was built with over-the-counter equipment, the decision process for next generation hardware, and future considerations for a deployed hardware system. The purpose of this proof-of-concept design is to show how networking with FSO in the open systems interconnection (OSI) stack is achievable. That it is possible even without the demonstration of full operational capabilities. This chapter points out equipment or techniques which would help to achieve full operational capabilities, and give reasons for why it is not included within the current system.

A. HARDWARE

The developed experimental hardware system is significantly different from what would be expected in a deployed hardware solution. The proof-of-concept nature entails that the system does not meet the engineering requirements, high data rates, and lower latencies of operational equipment. To make comparisons between the two, the proof-of-concept's results must be extrapolated to identify capabilities and possible limitations of operational equipment. Furthermore, the use of over-the-counter equipment is designed to demonstrate functionality, but not to meet deployment capabilities. The field implemented system would include application-specific integrated circuits (ASICs), a specifically tuned transmitter, and powerful receivers, all developed to maximize efficiency and effectiveness.

To maximize the efficiency and effectiveness results in meeting the desired bandwidths and latencies. Increasing the capabilities of any single piece of the system (processing equipment, receiving equipment, and projection equipment) requires an equivalent increase in all other areas. For example, if the application needs to receive data at a higher frame rate, requires an equivalent increase in processing equipment and transmission equipment to transmit, decode, and encode this data.

1. Processing Equipment

Processing equipment is required for FSO to capture, transport, or inject packets in multiple locations in the system. In modern everyday equipment, this occurs in devices such as the network card, router, or switch. These pieces of equipment do not natively support the use of FSO, and are normally not friendly for development. For these reasons, the processing must occur on a laptop or other programmable equipment.

The speed of processing is limited with a laptop-grade computer, as it is not efficient enough to natively meet the desired Gigabit/sec data rates. The future is to develop Field Programmable Gate Arrays (FPGAs) or ASICs, significantly increasing the speed of processing. In any networking equipment, it is essential that it has the ability to quickly process and send data. Large processing delays can result in increased latency and data in buffers. This leads to negative effect on the effectiveness of a system, especially with data waiting in buffers that needs processing or transmission.

ASICs and FPGAs can complete the same tasks as a computer processor in a fraction of the computing power and energy. This is because a Central Processing Unit (CPU) is designed for high dexterity in the tasks while ASICs and FPGAs are designed for a small number of dedicated tasks. CPUs can never compete with the effectiveness of a designed processor, but due to cost and skill required to design, this proof-of-concept uses a general purpose CPU for processing.

2. Receiving Equipment

The receiving equipment, i.e., the cameras, used for a FSO system must be capable of achieving high frame rates to capture changes in the oscillation equipment. The cameras used in the developmental proof-of-concept do not have high enough frame rates to minimize latency and support the desired bandwidth. Furthermore, it is only possible for any system to use half of the maximum frame rates of the camera, to ensure the camera receives the desired frame. This means that if the camera can sample at a maximum of 60hz, in the best case scenario the system uses 30 different frames. This means that each frame must hold 33 Megabits to reach one gigabit per second, which is unrealistic for any real system. This is only a small fraction of the frame rates, for reasonable frame sizes, required to meet the desired bandwidth and latencies.

The system which could meet the desired requirements should have the capability to sample twice as fast as the projection equipment is able to oscillate its output. This sampling rate is essential so that the system can reach its full potential; however, there may be many other limits on the system. Most of these limits arise in the computer vision processes, since the system must process increased frames per second.

3. Projection Equipment

The projection equipment used in this proof-of-concept system is a limiting factor as a traditional computer monitor can only maintain a low frame rate. Most modern computer monitors are only rated to display data between 30–120 times per second. The use of laser arrays can provide significantly higher framerates than modern monitor technology. This is because monitors must encode millions of pixels which requires advanced graphical processing units (GPU). Monitors can only achieve a fraction of the frame rate compared to 9 lasers as the GPU only needs to display 9 nodes. It is obvious that controlling 9 nodes versus millions will be significantly faster as long as the projection equipment can turn on and off fast enough.

The operationally deployed system should include an array of lasers, as proposed a minimum of 9 lasers; 8 which encode data and 1 which encodes state. With the capability for more lasers resulting in an increase in data rates, but any increase in the quantity of lasers has its own drawbacks. More data can be transferred using more lasers, but these lasers must be properly collated and aligned. This can be difficult, especially at long distances, when there are imperfections in the beam or housing. The receiver expects all beams to arrive with the same separation. This can be a difficult task without well-made, expensive lasers and low tolerance housings since small errors will propagate throughout the system.

B. SOFTWARE

The software used in the proof-of-concept is a combination of C and C++ libraries. This design provides ease of use, but has the potential for optimization and increases in data rates. Custom built software results in efficient operation without the implementation of overhead found within a large programing library. The libraries used provide more capabilities than required resulting in slowdowns and loss of efficiency. The software must be capable of capturing, encoding, and decoding information at Gigabit data rates; any unnecessary overhead or bloating must be eliminated.

1. C libraries

The C and C++ libraries are essential for allowing this system to capture, inject, identify, and transmit Ethernet frames across a visual link. The libraries allow for easy use, fast prototyping, and a unified language understood by most programmers. In software, it is important to maximize the effectiveness of programs by limiting latencies and buffers. The C and C++ programing languages can provide orders of magnitude speed-ups compared to python, java, and many other languages. The C and C++ libraries, libpcap and OpenCV, allow for the capture, manipulation, and transmission of data packets.

a. Libpcap

Libpcap is a basic C and C++ library which allows for the capture and analysis of layer two and three network packets. This software library provides the basic networking functionalities to create a new physical layer link via FSO. Libpcap provides an easy-to-use Application Programing Interface (API) for capturing and injecting data packets as they interact with a device.

The first capability of libpcap used is the creation of a network connection between the Network Interface Controller (NIC) and the program. This connection is the hook that allows for the capture or injection of data. Libpcap has the built-in capabilities to determine the number of captured packets and natively store them into memory. This provides a pointer to an array of characters with a length of the packet. This allows for packet filtering or conversion before being transferred or injected.

The libpcap library has ingrained tools for the analysis of incoming packets, allowing for filtering based upon specifications including host, protocol, or ports. This is used to identify useful and eliminating unnecessary data, acting as a simple firewall for desirable packets. Filtering can properly identify which packets must be sent or captured on the link, and those which must be injected onto the internet.

The capture and injection of the libpcap library allows for the injection of data into a network device. Injecting data as it's received on the opposite end of the data transfer, as the entire packet has reached its end state. The packet injection requires inputs of the NIC hook, pointer to the packet header, and packet size. There is no error checking of injected data, but blindly injects the packet size of data from memory onto the NIC.

b. OpenCV

OpenCV is an open source computer vision library which allows for the application of computer vision and machine learning into a basic API. This includes libraries which allow for the use of facial recognition, object identification, tracking, image stitching, image identification, and other computer vision applications. The system has the capabilities to identify and track images within the camera's view.

The OpenCV has two significant applications on the receiver, but does not affect the transmitter. First to identify the grid location based upon a basic checkerboard. Second is to identify the transmitted data. This is done as data is sent via changing the output grid. OpenCV takes the new image and identifying on and off nodes using the location of the basic checkerboard. A binary matrix is created correlating to the pattern displayed by the transmitter. The matrix can be decoded using the binary matrix and correlating this matrix to a byte of data.

This system is inherently inefficient but does not require significant timing synchronization, as the program must use OpenCV's computer vision library to determine new information. The identification and pattern recognition, even at a basic level, requires significant computing power. Using modern processors there are bottlenecks at higher frame rates. The current system, although crude to determine changes in output, prevents messy timing synchronization between sender and receiver. In a more advanced system, timing may be a significant consideration which may require minimal usage of OpenCV or other computer vision software.

The OpenCV libraries are exceptionally user friendly and powerful, but have the inherent burden of having too many capabilities. The optical link does not require software which has the ability to classify images or recognize an individual's face. In an ideal system, the identification software would have fewer, focused capabilities, optimized towards the speed of operation instead of flexibility. This is an inherent progression as the system moves from open source resources to a well-designed engineering machine, which matches hardware capabilities with the software.

2. Architecture

The architecture of optical link is designed to maintain stability into future generations with minimal changes. This is essential because the equipment described in Chapter III, Hardware, needs to be upgraded to meet operational needs. The next step is a hardware upgrade, as because it is a bottleneck for the system.

a. Overview

The visual optical link is broken into two distinct and separate systems, a transmitter and receiver, which have minimal interaction with one another. A SISO system has a single transmitter and receiver, as data only needs to be transferred in one direction. The transmitter and receiver for a SISO system each requires different hardware. On the other hand, a MIMO system (necessary for TCP) requires that the system have at least two inputs and two outputs. This is displayed in the Figure 9. The desired methodology would have the receiver and transmitter on the same piece of hardware to share network capabilities. Like typical networking, it is not essential to have data flowing in both directions at the same point in time, if the system is capable of achieving the desired data rates. The difference is that this FSO system does have the capability of transmitting and receiving at the same point in time. This is because of the directional nature of FSO, opposed to the beacon nature of wireless data transfer (Wi-Fi). Furthermore, FSO does not have to account for beam interference, as the signals never overlap. Multidirectional data transfer can double data transmissions, as data can be flowing both directions simultaneously.

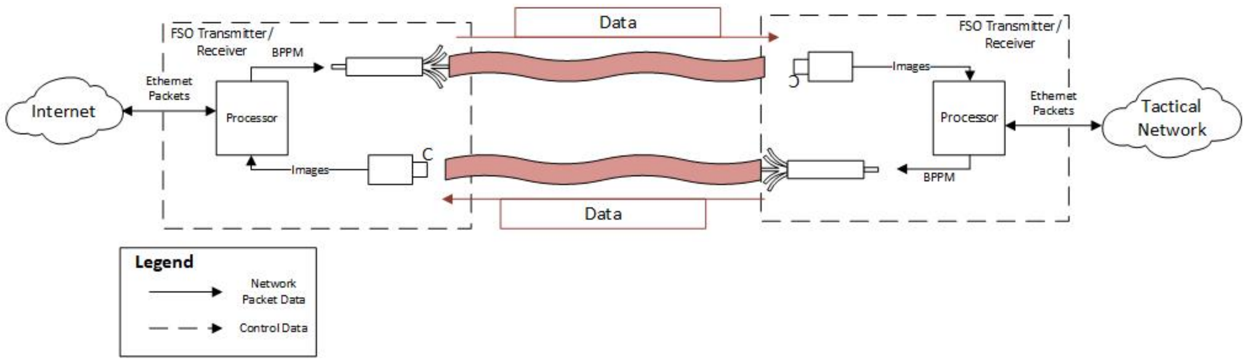

Figure 9. Transmission Overview

Figure 9 demonstrates the connection between an internet-connected network and a tactical network. This is essential for useful and effective military FSO system. The system must be able to transmit data between two different networks. Requiring a processor to control and identify the data as it is sent or received. The internals of this processor are displayed in Figure 10, which combines the transmitter and receiver. This is the physical hardware used to take data off or put it on a wire. This is achieved using the libpcap library and the shared network interface. Then either sending data with a binary pulse position modulation scheme or receiving images.

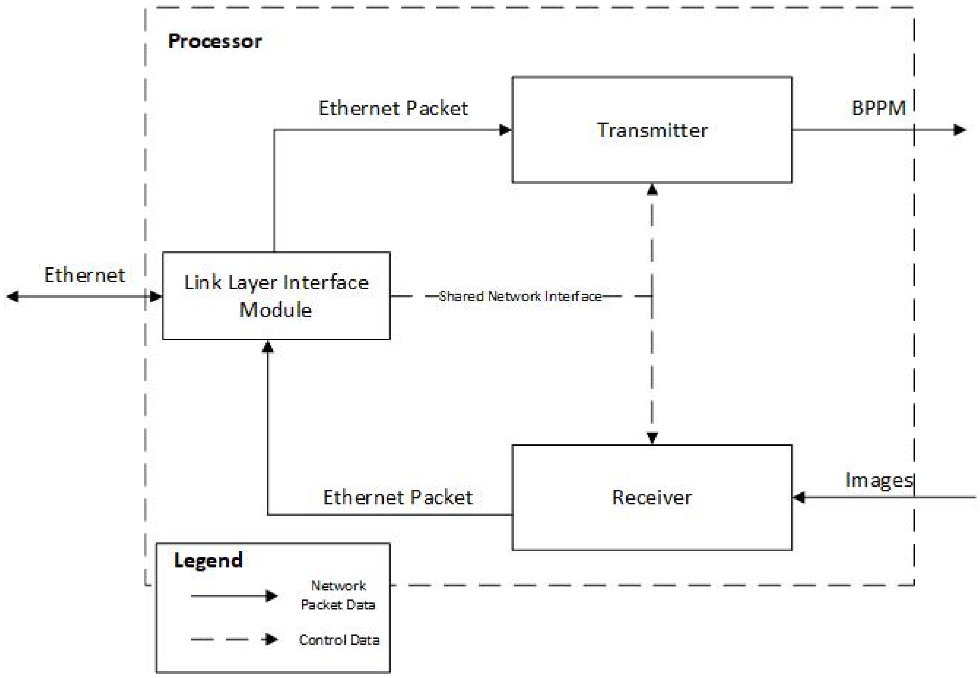

Figure 10. FSO Internal Processor

The link layer network interface module is responsible for interfacing with the local network stack. The logical location within the processor can be seen in Figure 10, and the method used by this module is seen in Figure 11. This mainly includes using the libpcap library to establish a network handle and grab local network traffic. The network handle is an essential component of the system, allowing for the use of further libpcap capabilities. There may be multiple network interfaces (NIC) on a specific device and this allows the user to select the desired NIC to be monitored. Information can be displayed about the NIC, including IP address, MAC address, and subnet mask.

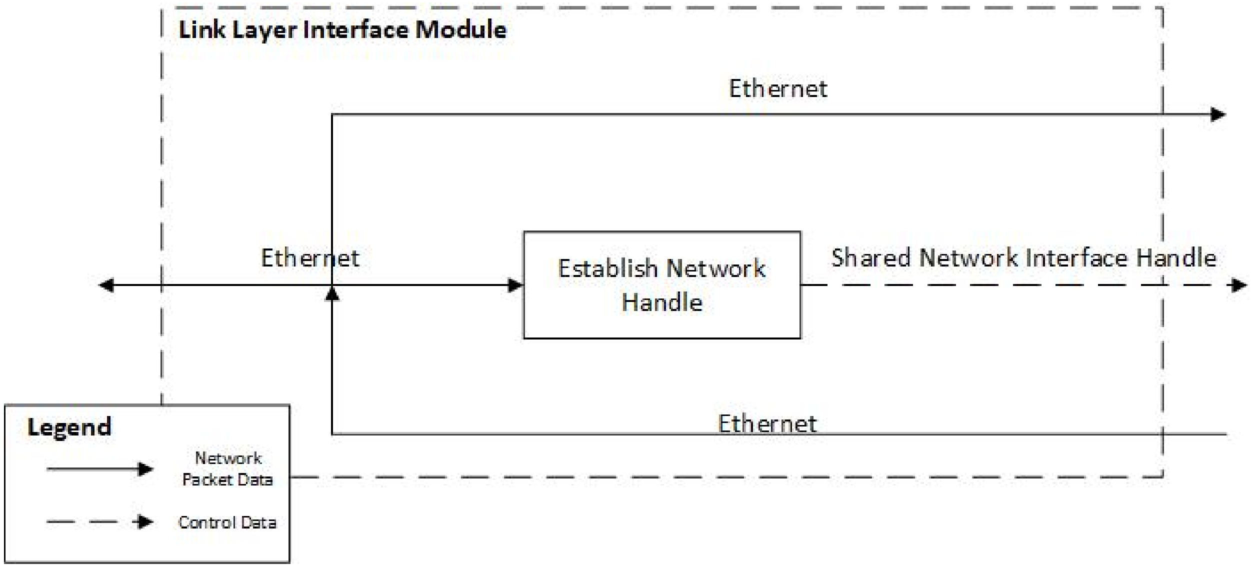

Figure 11. Link Layer Interface Module

b. Transmitter

The transmitter is responsible for sending data across the system. This means that it must be able to capture network data, encode this data, and properly output this data. The transmitter module is found within Figure 10, and is illustrated more thoroughly in Figure 12. The transmitting process requires several steps to capture data on the network and properly visually transmit it. This is done with the link layer network interface, link layer packet capture, error correction, and the transmission module.

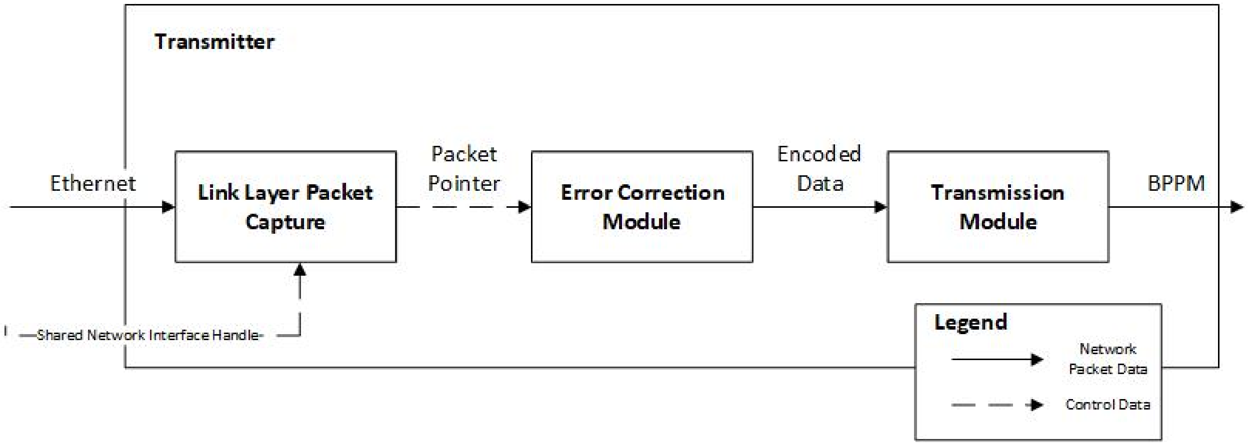

Figure 12. Transmitter Module

(1) Link Layer Packet Capture Module

The link layer packet capture module is responsible for capturing and storing network data seen in Figure 13. The packet capture module is found within the overarching transmitter module in Figure 12. The module uses the network handle established in the link layer network interface module and the packet capture function from the libpcap library. Depending on the desired settings, this can capture a number of packets on a network device and then store them in memory. The capture gives the user the ability to filter and transform the raw bits of a packet.

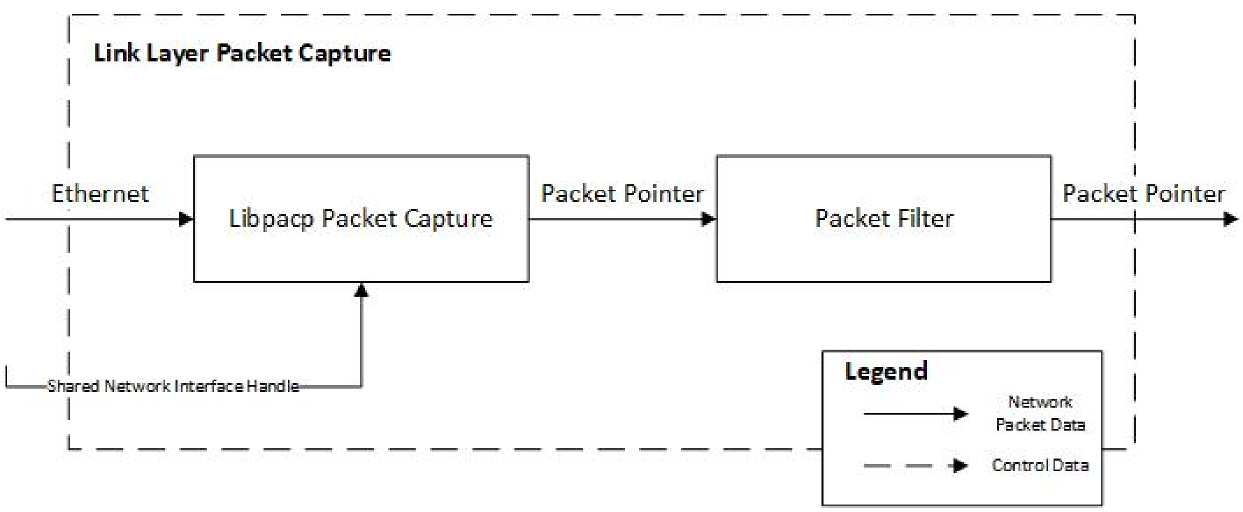

Figure 13. Packet Capture Module

(2) Error Correction Module

The error correction module provides error correction as the data is being transferred, seen within the transmitter module in Figure 12. This includes three steps of encoding and encryption, before an array of data is visually transmitted. These steps are further described in the Error Correction and Encryption section. The system modules are displayed in Figure 14. This includes an encryption step, Reed Solomon encoder, and Reed Muller encoder [16]. Each step takes the data captured in the link layer packet capture module and modifies it to provide extra security or error correction. The output from this module is a binary string, which has the capability to correct for multiple errors and has increased security.

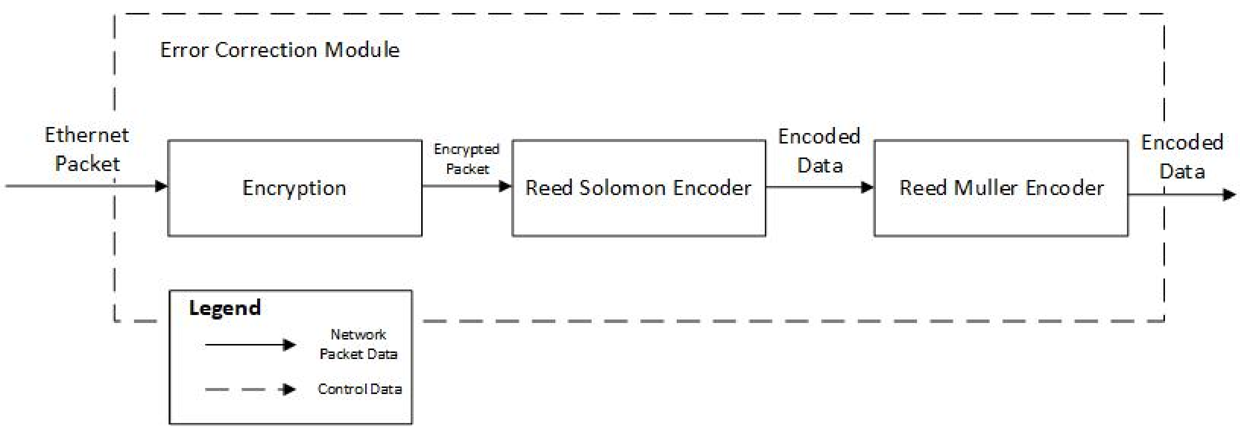

Figure 14. Error Correction Module

(3) Transmission Module

The final module, the transmission module, is seen in Figure 15 and is responsible for sending data via FSO in an array of lasers. Its context within the entire transmitter module is seen in Figure 12. The transmission module provides the capability to display encoded data via a monitor. The input for this module is a data string which has been encoded and encrypted. The system uses binary pulse position modulation to take this data, convert it, and allocate it to desired nodes. The module then displays a frame correlating to the desired data. Further explanation of the transmission frames, and their overhead is described in the Transmission Frame section.

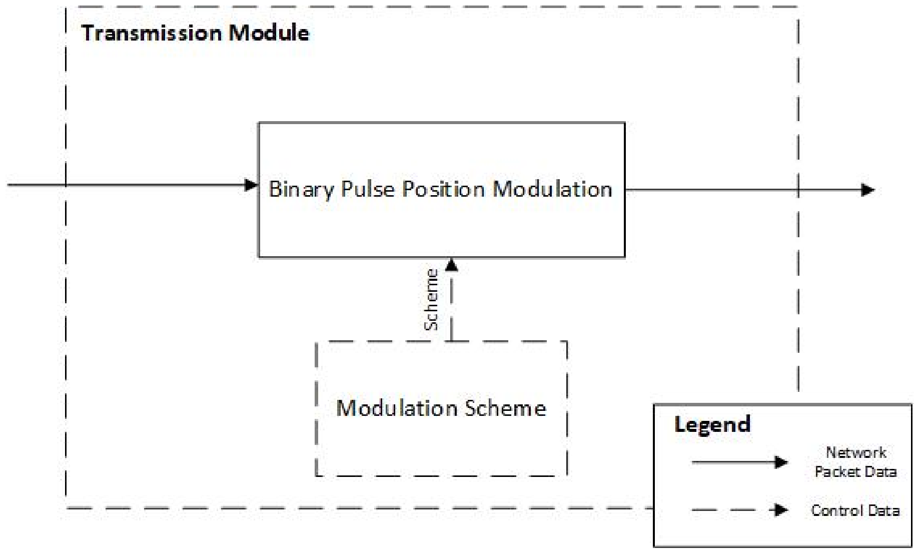

Figure 15. Transmission Module

c. Receiver

The receiver, seen in Figure 16, acts very similarly to that of the transmitter, seen in 12, but completes the system in reverse by decoding and injecting the received packet. The receiver is found within the processor seen in Figure 10. The biggest difference between the two systems is the need for computer vision to properly identify and decode packets. The receiver system must have the capability to take light, in the form of a laser or projection, and convert it into a binary string. Once the system has passed through the computer vision module, it is sent to the error correction decoding module converting the data into network packets. The same link layer network interface module as used in the transmission module, creates a handle which can be used by the link layer network injection module to inject data back into the new network.

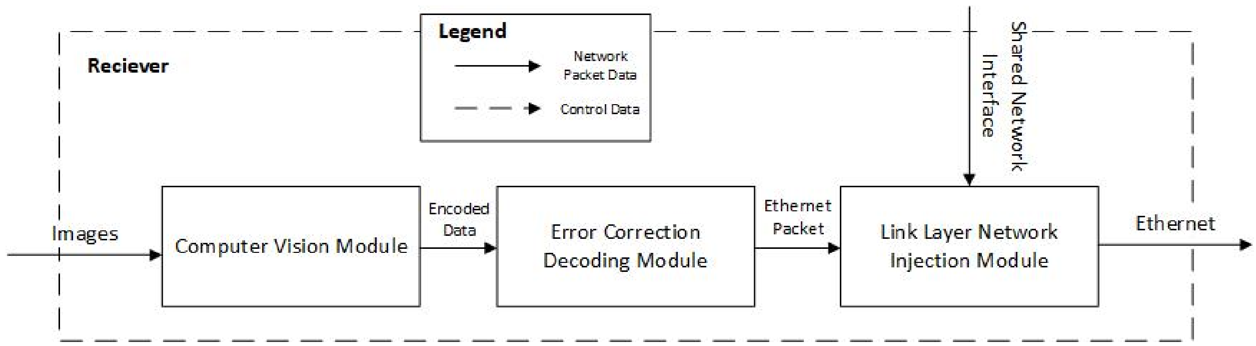

Figure 16. Receiver Module

(1) Computer Vision Module

The computer vision module is designed to identify the location of the three by three array, created by the transmitter. Its context within the entire receiver is seen within Figure 16. Computer vision converts this image back into the byte of data which is originally encoded by the transmitter. This method is logically described in Figure 17. The computer vision module uses the OpenCV library to identify the location of the data, and to determine the pattern created by the transmitter. With future generations of this system, hardware may be used to identify laser locations, and could result in the removal of this module. Hardware can physically determine the encoded pattern without the requirement of heavy software.

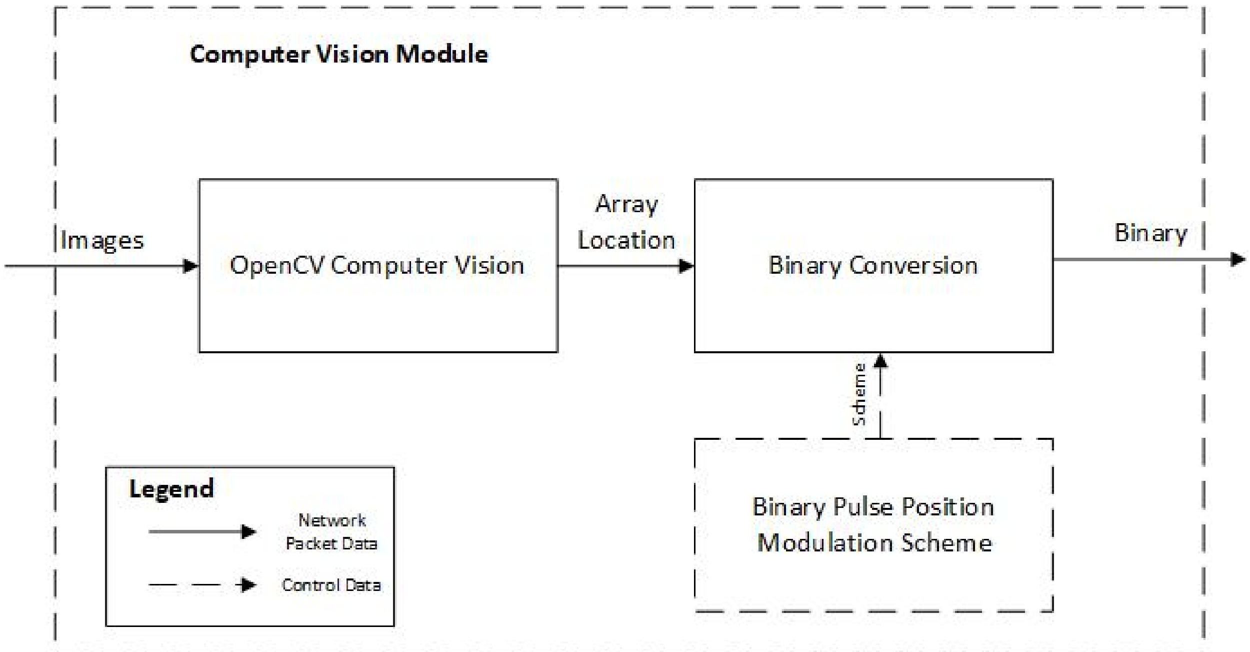

Figure 17. Computer Vision Module

(2) Error Correction Decoding Module

The error correction decoding module, Figure 18, uses the opposite of the error correction module, Figure 14, and outputs network capable packets. The decoding module can be found in the receiver architecture, Figure 16. Taking the bytes of data from the computer vision module and decoding the Reed Muller encoder, then the Reed Solomon encoder, and finally decrypting the data. This decoding and decryption results in packets reaching the receiver without errors, regardless of expected atmospheric interference. The decoders identify transmission errors and fix up to a level to ensure complete transmission.

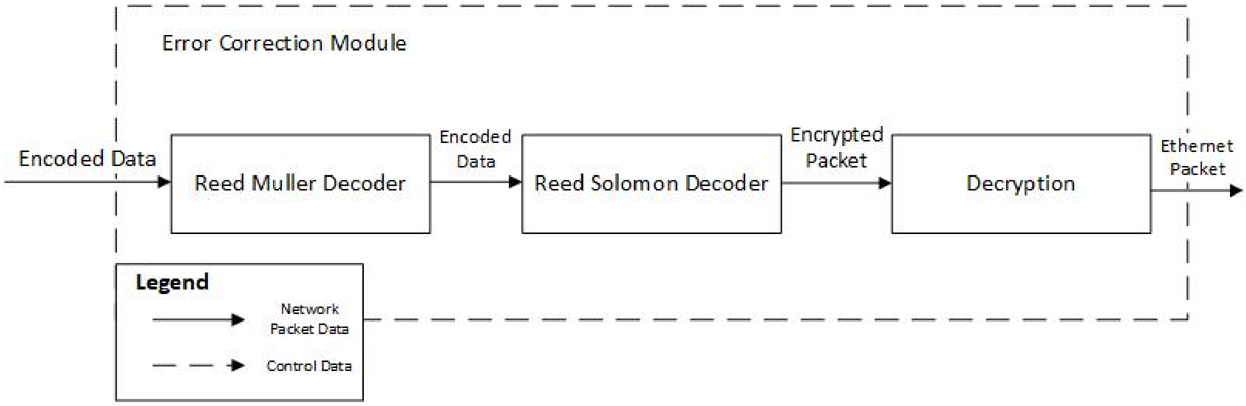

Figure 18. Error Correction Decoding Module

(3) Link Layer Network Injection Module

The link layer network injection module completes the end state of the system, putting the captured packets into the network, as seen in Figure 19. The packet injection takes the data, which was originally images, and injects it into the internet. This is the end state of the receiver, found in Figure 16.

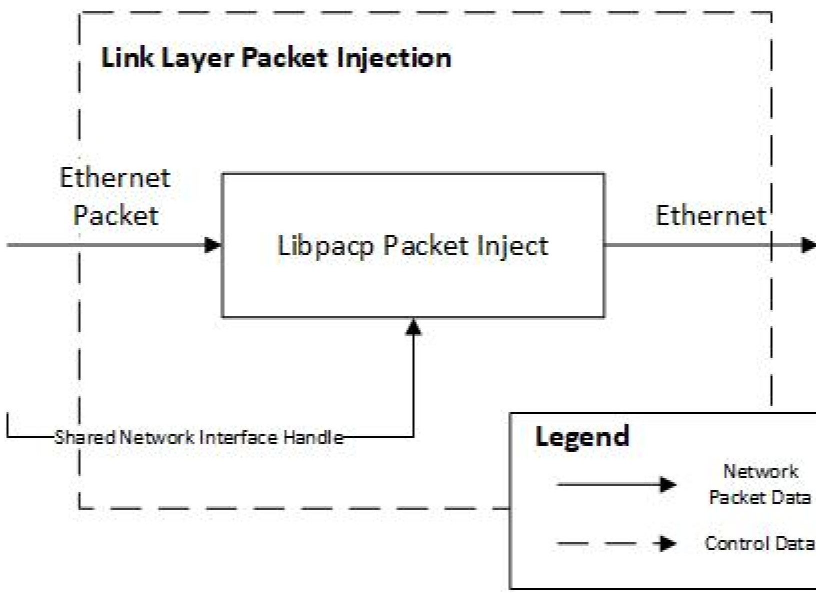

Figure 19. Link Layer Packet Injection Module

3. Error Correction and Encryption

To send data across a visual link at distance requires significant amounts of error correction and encryption to ensure integrity and confidentiality. In a FSO environment, it is expected that data is lost or damaged in transit. Error correction allows for corrupted data to be decoded and corrected in the end state. In this particular application, two different methods of error correction were employed: Reed Solomon and Reed Muller. The pipeline of the system takes the input data, encrypts then employs error correction to result in an error resistant system, as seen in Figure 14. The encrypted data enters a Reed Solomon encoder providing the first layer of error correction. This data is then inserted in a Reed Muller encoder for the second layer of encryption. Finally, this data is outputted by binary pulse position modulation (BPPM) in the transmission module. The methodology of this configuration, encrypt and then two layers of error correction, is under study to determine its effectiveness in a FSO environment. The end goal of any error correction is to add redundancies to recover the data.

The industry standard for error correction is the repetition of data to ensure that the complete set will reach the receiver. This standard fails to overcome physical obstacles inherent within FSO environments. Including laser fade which describes the effect of environmental factors, scintillation or attenuation, on a laser beam resulting incorrect data reception. The biggest problem with a fade, unlike traditional errors, is that it can last for hundreds to thousands of frames, especially in systems with high data rates. This means that in an array of lasers, a node could be lost for large portions of the transmission. Repetition of data, as described by the industry standard of error correction, cannot account for errors such as fades. The goal of the proposed error correction pipelines is to minimize the effects of fades, while still accounting for traditional Gaussian loss and noise.

a. Encryption

An essential portion of any data transfer, especially those in the military is to ensure confidentiality of data. Encryption can provide this by ensuring that if an enemy captures the transmission they cannot reading or understanding the data. The specific type of encryption that was used in this case is a linear-feedback shift register (LFSR). This type of encryption is used to efficiently make the data look random. Providing another level of security over the directionality of FSO.

b. Reed Solomon Encoder

The first level of error correction uses the Reed Solomon encoder, which is found within modern technology including CD's, DVDs, and data transmission technologies. This specific instance of the Reed Solomon encoder uses up to 223 bytes of data and then output 255 bytes. This error correction model creates 255 frames, each with 8 bits. The system can completely recover from errors in up to 16 frames. This means that the link can recover from a minimum of 16 bits of error, if each error is within a different frame. The significant difference is that if a whole frame, eight bits, is lost, the decoder can recover similarly as losing one bit in a frame. This means that there is a recoverable range of errors, 16 to 128 bits, depending upon location. This method of decoding by the receiver, using erasure code, allows for the error recovery. The Reed Solomon encoder has included 32 bytes of overhead, but now has the ability to correct up to 16 bytes of errors.

c. Reed Muller Encoder

The second level of error correction is the Reed Muller encoder which is found within data transmission, particularly in deep-space communication or the proposed 5G standard. The encoder takes a single frame from the Reed Solomon encoder, eight bits, and divide them into two four-bit segments. These four-bit segments are inserted into the Reed Muller encoder, which outputs two eight-bit segments. The benefit of this error correction scheme is that it can recover data if there are up to three errors of every eight bits. This is significant when trying to overcome fades, because laser nodes can be out of fade for numerous frames but the entire set of data can be recovered. The Reed Muller encoder has effectively doubled the size of the data, but has drastically increased error correction abilities.

d. Binary Pulse Position Modulation

The BPPM is the method of sending data across the visual link. BPPM is the method of encoding data into a matrix, show in Figure 20. In this case, the matrix has dimensions of three by three. A typical byte has the layout of B1 B2 B3 B4 B5 B6 B7 B8, where each bit corresponds to a specific position in Figure 20. When looking at the different transmission frames, found in Figure 23, the data is encapsulated within nine different lasers. Each character is made up of one byte, or eight bits. In Figure 20, the bottom right bit is left blank, but a true laser system, this bit is used to transmit state and other control information.

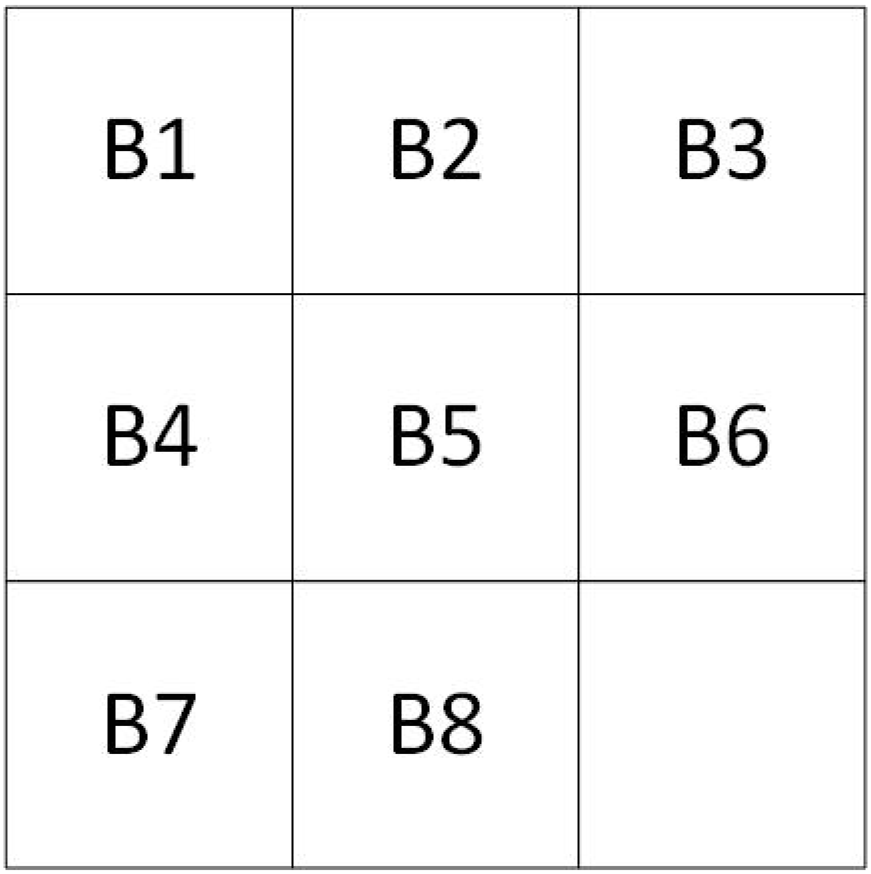

Figure 20. Binary Pulse Position Modulation

4. Transmission Frames

For FSO to work, data must be sent across the link via light, and in most cases for high data rates this must be done using a pattern. In this thesis, patterns are created by the system's transmitter to communicate location of data, start of data, the data itself, and when the communication has ended. These patterns, or transmission frames, are a pre-agreed procedures to properly send data to the receiver, ensuring data transfer is efficient and effective.

a. Calibration Frame

The initial frame, the calibration frame, is used by OpenCV to identify location for subsequent data transfer. In this proof-of-concept the calibration frame is a checkerboard seen in Figure 21. This gives OpenCV the location and size for subsequent transmission frames within the overarching image. This can drastically increase the efficiency computer vision, as the program does not have to search the entire image for the data pattern. This assumes that the receiver and sender are stationary, as designed in this basic prototype. The calibration frame can be any pattern designated before transmission, but checkerboards are a traditional calibration frame. The checkerboard can give the receiver an idea of distance and orientation of the transmitter. More advanced tactics for orientation and calibration are not used in our system, and in future models, this could be used.

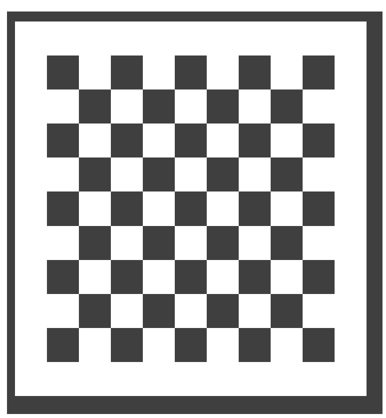

Figure 21. Calibration Frame

b. Start Frame

The start frame, seen in Figure 22, signals to the receiver that the transmission is about to begin sending data and is essential for efficient transmission. This is especially useful with computer vision, so the receiver knows when to start recording data. This frame is displayed longer than each of the subsequent transmission frames, except for the end frame, to ensure proper reception. This pattern is different from any other possible output frames, but does not include any information. Within all FSO systems, the start frame is a necessary frame.

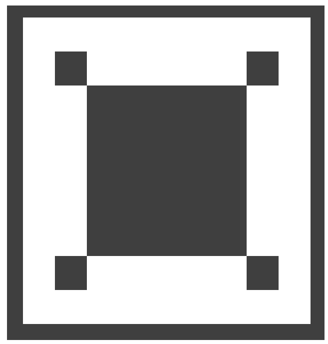

Figure 22. Start Frame

c. Data Frames

The data frames, as seen in Figure 23, encode the data being sent by the transmitter to the receiver. These frames include error correction, as they are the bulk of transmission frames and time. As indicated, these frames are sent between the initial start frame and the end frame. The desired FSO design has nine lasers which encode all of the required data, while the proof-of-concept has significantly more oscillating pixels. These extra pixels make the proof-of-concept design easier to use and identify data.

The timing and identification must be considered when correctly identifying data as it is received. A problem case is when the transmitter sends two identical frames one after the other. The receiver must be able to distinguish the two. This could be done with timing that after a specific time threshold the system recognizes the second duplicate frame. Creating timing between the receiver and transmitter results in new problems including initialization. To provide an easy solution for this proof-of-concept, oscillates the frames after each transmission so no two sequential frames looks at the same to the receiver. This is shown between row one and row two in Figure 23. The outside seven pixel evenly spaced pattern consistently changes.

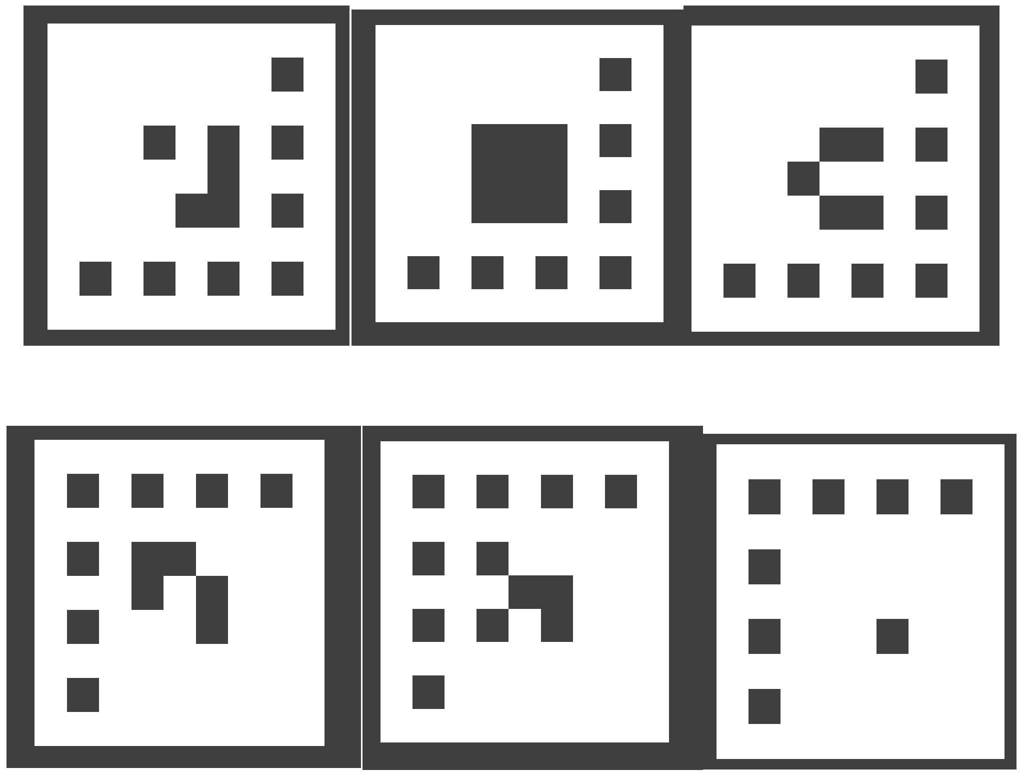

Figure 23. Transmission Frames

The nine center pixels in Figure 23 is where all of the data is encoded. Each containing a character using binary pulse position modulation. This means that the transmission frame has the ability to encode $\mathbf{2^8 = 256}$ different characters. Several different patterns are displayed in Figure 23 and result in binary characters, and eventually the encoded packets.

The proof-of-concept has key differences between the true desired system including the number of pixels and layout. A more efficient system, as opposed to this test system, contains a larger number of nodes. These nodes must transfer data and state, as the proposed system has an array of nine lasers (eight data and one state). More nodes allows for more data to be encoded per frame. Using a monitor does not require node spacing considerations in the calibration, start, or end frames. A true laser system requires significant spacing between nodes. This allows for differentiation at the receiver and accounting for spreading at distance.

d. End Frames

The end frame has its own unique sequence, seen in Figure 24, to signify that the entire transmission has been sent. This frame is almost as important as the start frame, helping to push the system into the next steps of the architecture. This frame is sent for more time than other transmission frames to ensure reception and allow for post transmission decryption. In future generations, significantly more levels of error tolerance could be included. For example, if the end frame is not received, but another start frame is received, the system can infer that the last transmission has completed. This solution is not without complications, requiring threading to avoid blocking on subsequent transmissions.

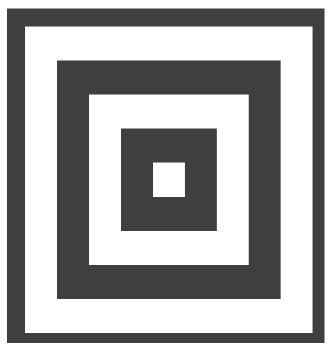

Figure 24. End Frame

C. TESTING OF OPTICAL SYSTEM

Testing of the optical system is done to identify the basic characteristics and limitations for future generations. With the intention of identifying possible shortcomings and bottlenecks of the system. There are obvious limitations of the currently design before running tests, most notably the data rate and latency. Keeping these limitations in mind, insight can be gained on future generations determining expected problems and shortcomings. It is also possible to use simulation to learn about expected results of the environment or hardware. For example, the proof-of-concept is not expected to be tested at far distances, and therefore minimal environmental errors. These errors could be simulated via software to understand how the system responds in normal environmental conditions.

1. Setup of the System

The proof-of-concept system has been constructed to achieve basic one way and two-way traffic between two networks. The initial goal of the system is to use the ping network software utility to test basic connectivity. Ping provides many desired capabilities, sending packets at variable sizes and frequencies. With a small bandwidth, it is desired to have a test which can send small number of minimal packets. In future tests, which are used to test the limitations of the system, the packet size and quantity may be increased.

The physical system acts as a real tactical network, but within a laboratory. The system is set up with tactical and internet networks. Each network has its own computer, with one of them having connectivity to the internet. Both networks have a transmitter and receiver as demonstrated in Figure 8. The method of sending data is through a computer screen, updating the screen where the camera takes images. The receiver uses these images, and computer vision to process, identify, and classify data.

The test system setup is within the lab and has no safety concerns as no lasers are used. With the upgraded next generation system, safety of personnel must be considered when shining lasers at long distances. This requires significant oversight and planning as lasers can cause permanent bodily damage.

2. Desired Experimental Characteristics

The goal of this proof-of-concept system is to determine the possible capabilities of a FSO system. Although this system has inherent equipment limitations for achievable data rates, it is interesting to see what can be extracted. The data can be interpolated to the fit future generation systems by understanding current limitations. Including bottlenecks of equipment, software, and the environment. Testing the effect of data loss, packet size, and framerate, when considering the factors of throughput, goodput, latency, and bytes received.

a. Throughput

The throughput of a system is an essential characteristic in understanding the rate at which a network runs. Determining bottlenecks, if the desired throughput is realistic, and current limitations. It is an interesting comparison between the amount of error correction and throughput to determine effectiveness. It is known that as increased error correction reduces the throughput of the system.

b. Goodput

The goodput, new data received per unit time, is important when considering a large percentage of loss. The goodput, when compared to throughput, can provide insight on the number of retransmissions required. Goodput requires the amount of useable data received at the endpoint divided by the time. There can be excessive latencies, losses, and retransmissions within a FSO system, requiring comparisons based on goodput.

c. Latency

With a system constantly overcoming losses and errors, latency is an essential consideration when considering viability. This is true, as many programs require a minimal latency, which could be a limiting factor. Latency is one of the most important characteristics, determining how the system responds to errors, losses, retransmissions, and buffers as a result of software or hardware slowdowns.

d. Effect of Loss

The level and effect of loss due to environmental conditions must be studied in a FSO system. Where and when can a FSO system be used must be considered carefully. Can it be used within a foggy, cloudy or hazy environment? How the system recovers, and what happens if there are too errors for error correction to resolve?

e. Packet Size

The packet size in a FSO system has another impact on the amount of data arriving at the end state receiver. The system must be optimized to maximize the goodput, as increases in the packet size can increase data reaching the receiver in low loss environments. While in high loss environments, smaller packet sizes could have a greater chance of arrival.

f. Time of Execution

The length of runtime can result in timeouts, data transfer, or other information about the system. Furthermore, it is interesting to look at execution time, as this is highly related to the latency and loss of the system. Determining if there are any bottlenecks resulting in longer execution times. Execution time can give indication on the rate of transmission and errors.

g. Framerate

An essential characteristic of the FSO system is the maximum capable framerate, as it drastically effects data rates. The problem comes, that framerates cannot exceed the capabilities of the physical equipment. The maximum framerate based on hardware can give an indication of bottlenecks and possible framerates of future generations.

h. Desired System

The desired next generation field implemented system is an arrayed FSO data transfer system. Requiring an array of high power lasers, in a three by three orientation, which can traverse a minimum of 1km through non-ideal conditions. These lasers encode data at a rate up to one Gbps and can compensate for the expected error rate. Error correction ensures that the whole data set arrives at the receiver. The first generation system uses cameras to capture the transferred data frames at a sufficient frame rate. The system has adequate computing power to recognize and extract data in real time. The next generation receiver uses a physical receiver to identify the pattern being sent. This arrayed FSO transfer system has the capability of being more secure than traditional RF methods, and meet modern data rates.

Like any communication system, larger viable distances are more desirable. The arrayed FSO system must be tested at long distances, to determine viability within a warfare environment. It is expected to have a sustainable range of 1km, but longer distances are desired. Environmental factors must be considered as distance increases because the environment drastically reduces transmission capabilities at distance.

D. EXPERIMENTATION

When conducting experiments for this proof-of-concept system the most important demonstration is of two-way communication capabilities. Focusing on demonstrating the connection between two separate networks. The proposed system must work with traditional IP protocols, so two way communication is essential for protocols such a TCP. This two-way capabilities are first demonstrated using single packets and the ping protocol. The next level of testing considers an array of different factors on the one way and two way interfaces. Including the testing of the effect of bit losses, packet size, and framerate, when considering the factors of throughput, goodput, latency, and bytes received. Helping to establish the limitations and effectiveness of the physical system, without considering environmental effects.

E. SUMMARY

This chapter discussed the methodology and process of creating a two-way visual communication system. The implementation in software and hardware which overviews the entirety of the system. Allowing for a two-way visual communication link which can pass packets and responses between different networks. This chapter identifies specific characteristics which need to be considered when testing a FSO communication system. Providing the link between prior work and experimentation with respect of two-way FSO communication.

IV. TESTING AND ANALYSIS

The testing of a FSO system is not an inherently easy task as changes in components and variables can change the results significantly. Depending on the desired outcomes, specific variables, and components must be selected. Many times simulation is chosen instead of experimentation to limit variables and isolate components. The negative is that developing a simulation can be more difficult than the results it achieves. In this case, the desired outcome is to identify and demonstrate network integration of a two-way FSO system. Requiring the ability to transfer packets and responses between different networks. The hardware used is not intended to demonstrate the full field operational capabilities of a next generation FSO system, but instead demonstrate the ability to capture, pass, update headers, and inject packets.

A. SIMULATION

To test variables in a system, simulation is the fastest and cheapest method, but requires a working simulation. Simulation of FSO visual communication does not have an established simulation model and can result in unexpected results. The overarching FSO environmental simulation was developed to study and identify satellite to ground station visual communication. More well-known NS-3 simulation methods are used to consider the packet size within a high loss environment.

1. FSO Environmental Simulation

The first simulation uses a premade environmental simulation to determine effects of software and hardware characteristics. This simulation is attempting to understand the overarching effects of a FSO system when connecting a ground station to satellite. This is significantly longer than the expected connection of this thesis FSO system

a. Methodology of FSO Environmental Simulation

When developing the simulation, we used a preexisting framework in the NS-3 simulation module developed of the SOCIS 2016 Optical Satellite Systems project [17]. This simulation was developed to analyze the effect of data being sent between ground stations and satellites. This module required separate downloading and installation as it was not a basic and integrated portion of NS-3. The module came with basic example codes allowing for sending of data between a node and sink. To determine how this system would work within a real environment, it had to implement into the IP stack. This included sending data using the UDP protocols.

The model allows for a significant number of variables and parameters to be adjusted and considered. These are adjusted based upon the parameters that one is attempting to simulate. The basic parameters regarding the transmitter of the system is the distance between node and sink, transmission power, packet size, beam width, gain, receiver gain, and aperture diameter, and wavelength. The model is set within an environment with specified parameters, adapting how the system will respond.

The experiment creates a geosynchronous satellite which would receive data from a ground station at distances between 400 km to 1500 km. The system would send UDP packets varying from sizes of 100 to 3600 bytes reaching 2MB of data. Data was collected and parsed to determine the number of packets received by the sink. This data was collected, condensed, and averaged to determine the packet success rate for the simulation. Multiple simulations were conducted to see how the system would perform at different packet sizes and distances. The results were consolidated and plotted to determine the validity of the model.

b. Results and Analysis of Environmental Simulation

Figure 25 is created to consider the effect of wavelength on a FSO system. In this simulation, we wanted to see how the effect of wavelength would affect the packet success rate of the system, and to make the simulation more understandable we chose the colors of the rainbow. We also chose 1000 km to determine the packet success rate as the red wavelength has a packet success rate of 0.5.

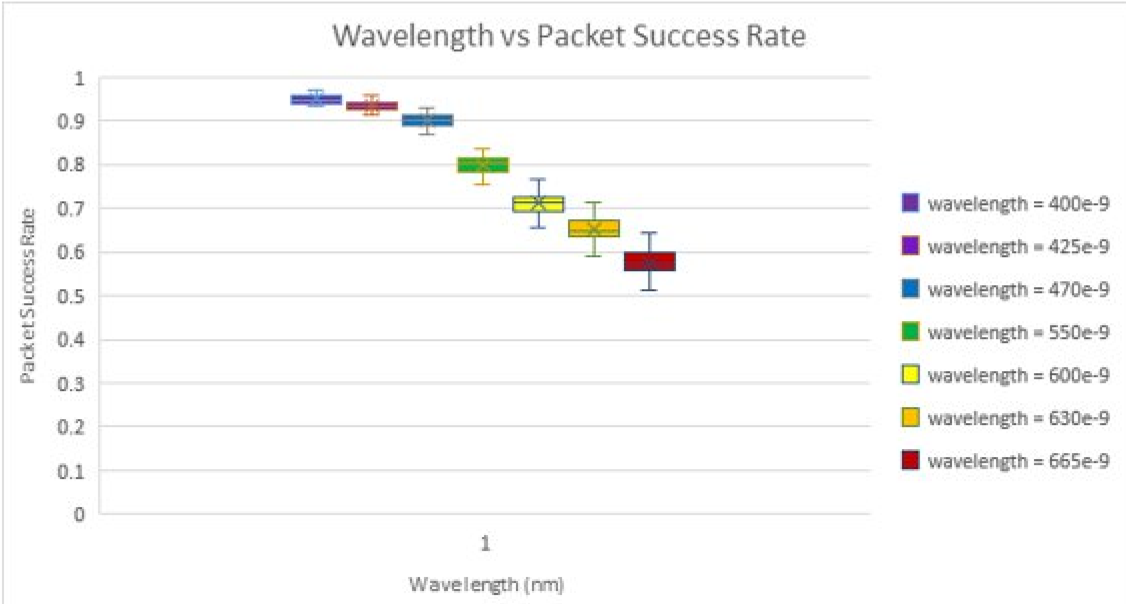

Figure 25. Wavelength versus Packet Success Rate

The simulation returned results of varying packet success rates for varying wavelengths. The red wavelength displayed the lowest packet success rate, with an average close to 0.58, and the purple wavelength had the highest with 0.95 packet success rate. The other colors of the rainbow, as indicated in the legend, fell in between the red and purple with respect to wavelength.

This result is not as expected, because attenuation is directly related to the wavelength. Small wavelengths correlate to high frequencies and thus higher loss based upon attenuation. While larger wavelengths result in smaller frequencies and result in lower losses. It is expected that the red wavelengths would experience the smallest losses because of low attenuation and thus have the highest packet success rate. While purple would experience the most loss from attenuation and thus the lowest packet success rate. The results were exactly opposite of what was expected, which either indicates that there are other factors resulting in the packet success rate or that the model does not match real life.

These possible factors which could affect the packet success rate is the spreading of the beam as it travels the 1000km from the ground station to the satellite. The longer the wavelength the greater the spreading of the wave, resulting in a lower packet success rate.

Meaning that red wavelengths could spread more than other colors. Attenuation has the largest effect wave propagation at short distances, and if this is constant at large distances, the model does not adequately model reality.

The next two graphs, Figure 26 and 27, show a comparison between the NS-3 FSO model and NS-3 802.11 UDP traffic simulations. The graphs show that both FSO and UDP traffic behaved similarly in that there is a precipitous drop off in the packet success rate at a certain distance. That distance for UDP was approximately 600 meters and approximately 6000 kilometers for the FSO simulation. As the distance continued to increase, the packet success rate did not recover.

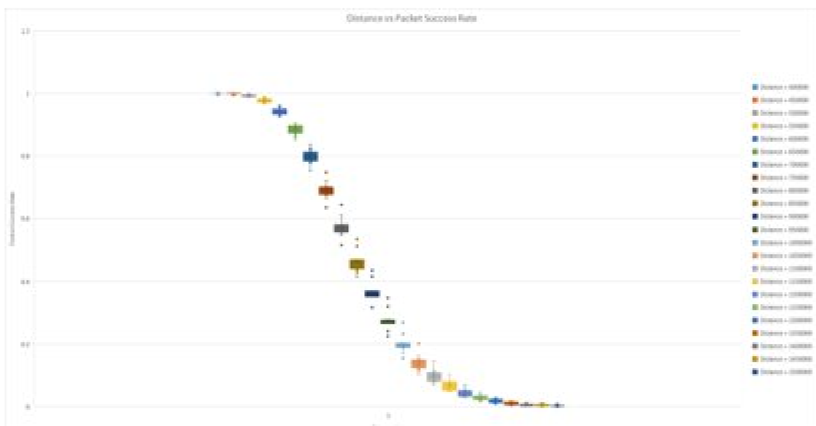

Figure 26. Distance versus Packet Success Rate

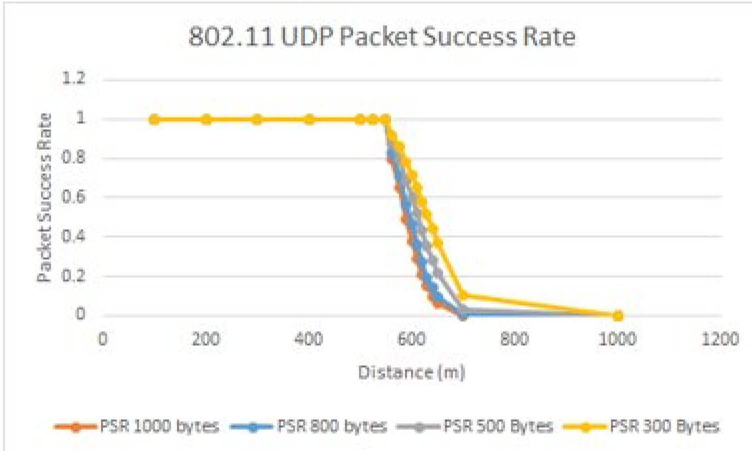

Figure 27. 802.11 UDP Distance versus Packet Success Rate

The comparison between the two simulations demonstrated the overarching effects of the NS-3 module. The decrease in the packet success rate shown in Figure 26 most adequately represents the correct shape. The S-curve with equal tails is as one would expect the system to react. The system in Figure 27 demonstrates the 802.11 UDP packet success rate over an increasing range. This system does not represent the idealized curve for UDP packets with the equal tail S-curve. This is because rarely does the system truly model the idealized curve but instead representing what would occur in real life. When looking at the general configuration of the curves, both systems have similarities. Including when distance increases the packet success rate decreases, tailing at the beginning and end. This similarity demonstrates some validity of the FSO model, and its ability to model real life.

Figure 28 is from true experiments considering the bit error rate (BER) versus the distance in a FSO system. This shows how the system will be reacting with respect to different wavelengths and at different distances. It demonstrates that larger distances has greater error rates and the smaller wavelengths have larger error rates.

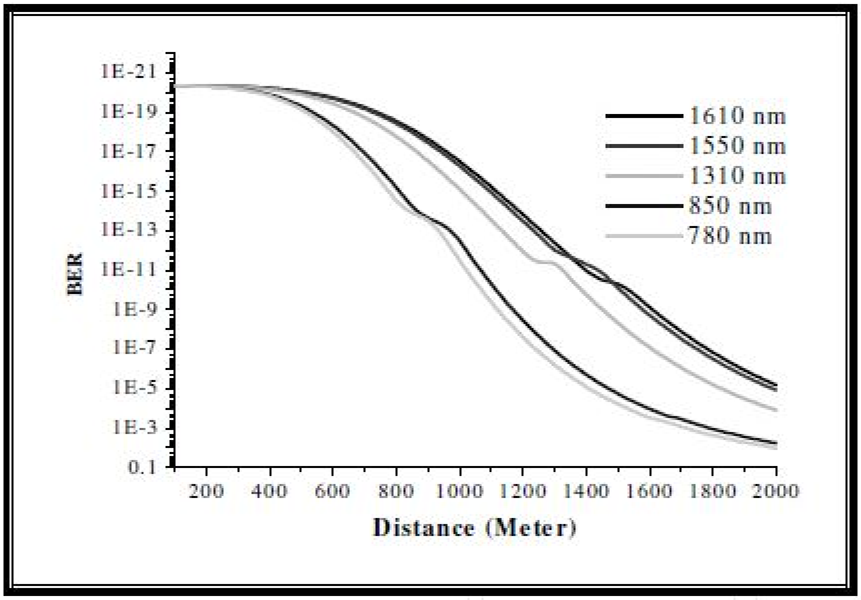

Figure 28. BER versus Distance in FSO. Source: [18].

Figure 28, backs up the ideas found in Figure 26 and 27 where the increased in distances will result in an increase in the error rate. In other words, the increase in distance results in a decrease in the packet success rate due to more errors. Figure 28 also demonstrates the tails of errors at close and far distances. The system in Figure 28 demonstrates the opposite of what was shown in Figure 25 with respect to wavelength. In Figure 28, the larger wavelengths have smaller bit error rate, and thus a higher packet success rate. This is opposite of what was shown in Figure 25, leading to the unreliability of the simulation.

Figure 29 shows the relationship between the packet success rate and packet size (in bytes). From left to right packet size increases by 100 bytes, but the packet success rate decreases and then levels off. This suggested two things: 1) Packet size had a direct effect of the initial success rates and 2) that there was a packet size threshold relative to decreases in the packet success rate. However, there was an unexplained spike in the packet success rate when the packet size increased to 2000 bytes. The rate then tapered back down as more simulations were conducted in the model.

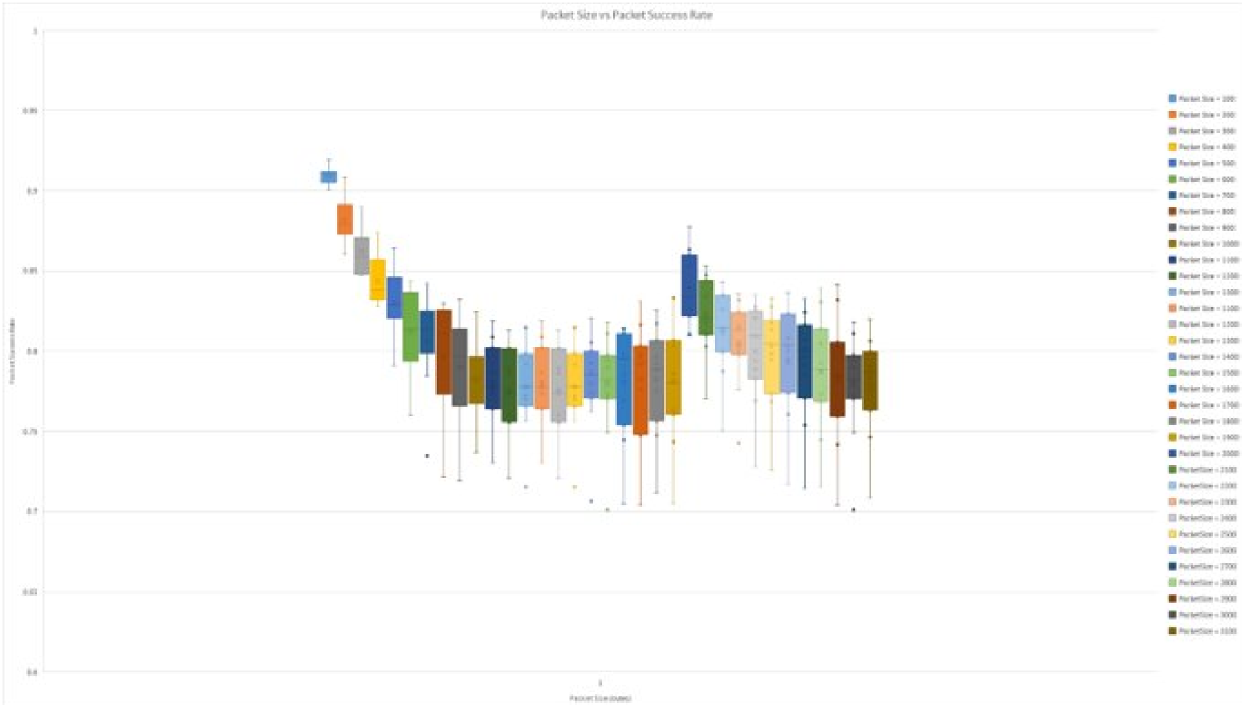

Figure 29. Packet Size versus Packet Success Rate

Figure 29 demonstrates several oddities found within the simulation of FSO. As expected, when increasing the packet size, while keeping the distance consistent, decreases the packet success rate. This seems to level off at a specific point, which does not make sense, as the large the packet size the larger of a chance that the packet will incur an error. The reason the steady state could make sense if the errors within a system are not randomly distributed. Resulting in the same section of packets receiving errors, and not changing the packet success rate.

The unexplained spike at 2000 bytes is the largest unexplained factor, as each test done explain this resulted in failure. The initial guess was that the system was undergoing fragmentation as the packet size grew beyond the maximum transmission unit of the link. When reviewing the systems outputs there was no indication of fragmentation, as there were 2000-byte packets being sent and 2000-byte packets being received. Furthermore, we investigated another simulated link which had the same properties. When the data was viewed in Wireshark, it was obvious that all packets being sent and received were 2000 bytes.

Another interesting note is that after the spike in packet success rate after 2000 bytes, the system begins to once again steady state at the same value of before. This steady state is an interesting phenomenon of the system, as it unlikely that the system would do this naturally without fragmentation or some problem with the simulation.

Figure 30 shows the effect of packet size and error rate in a real world FSO experiment over the Chesapeake Bay. The graph shows the comparison between error rate and packet size for three different output powers. The graph is on a logarithmic scale which demonstrates that there is an exponential increase in errors as the packet size increases.

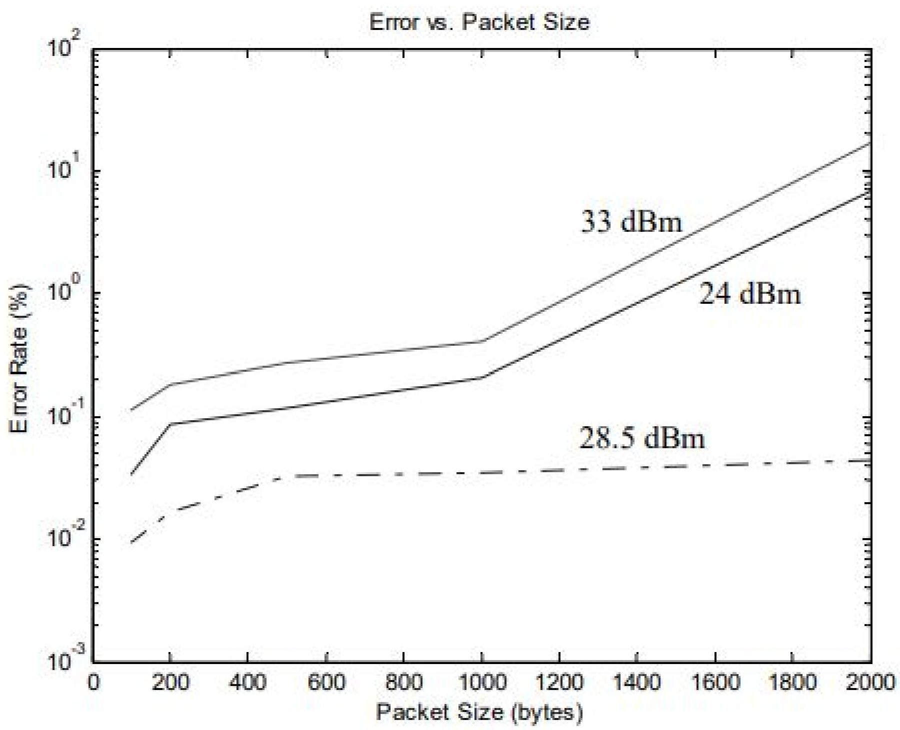

Figure 30. Error versus Packet Size in Chesapeake. Source: [19].

When comparing Figure 30, to the results in Figure 29, further demonstrates the inaccuracies of the FSO model. This experiment demonstrates that errors increase with packet size, so the stead state of Figure 29 is not realistic. Due to the logarithmic nature of the error rate in Figure 30, it demonstrates that there is an exponential increase in error as the packet size increases, which furthermore demonstrates the inaccuracies of the simulation.

Figure 31 illustrates a three-way comparison between packet success rate, packet size, and distance. This figure takes the average of different 10 simulations at each distances between 400km and 1500km and packet sizes between 100 and 2000 bytes. Distance appears to be the driving factor influencing the packet success rate. The uniform increase at the end of each line is the unexplained spike when the packet size reached 2000 bytes.

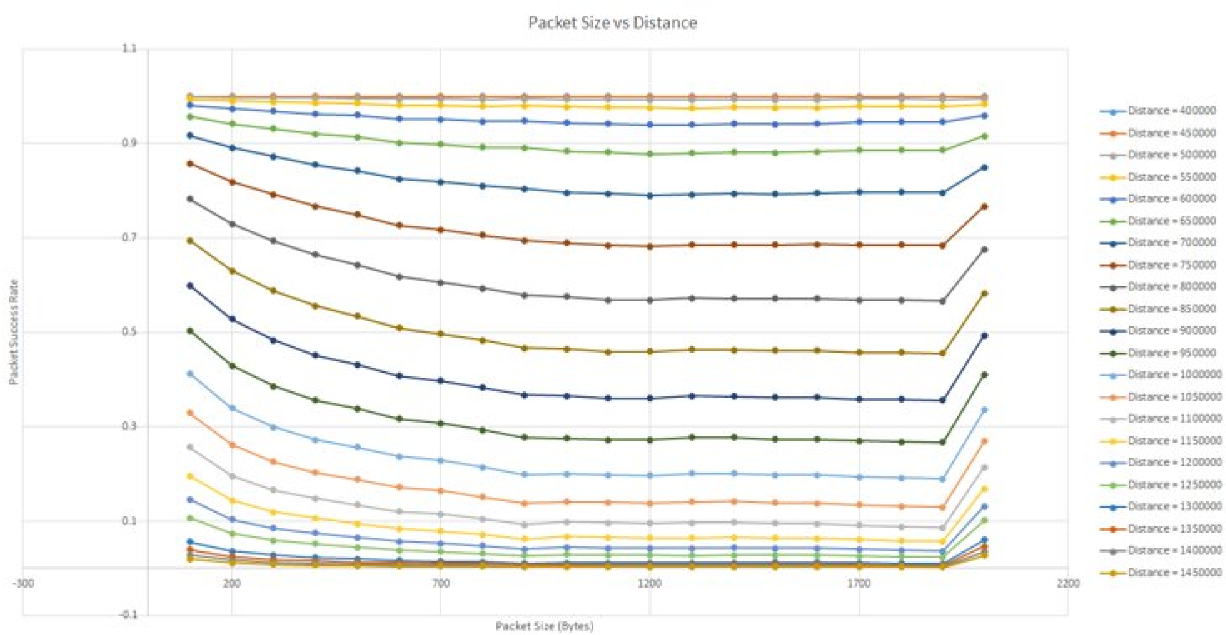

Figure 31. Combined Packet Size versus Distance

The system in Figure 31 demonstrates both the effect of packet size and distance on the packet success rate. The model shows a similar response due to different packet sizes at different distances in the packet success rate. At the high and low bounds of distance, there is minimal affect due to packet size in the packet success rate. This makes sense that at small distances, most packets reach the destination, so changing packet size will only minimally affect the system. While at large distances, only a small number of packets will arrive at the destination, making packet size minimally effective. Regardless, at all distances it is shown that small packet sizes result in higher packet success rate, and that there is a jump at 2000 bytes for every packet size. This graph confirms observations made in Figures 26–30 at a much larger section of data points and distances.

c. Conclusions of Environmental Simulation

The overarching question that this simulation is to answer is if the model adequately represents reality. We used the variables of packet size, distance, and wavelength to explore this question. It can be concluded that although the model does support how distance effects data transfer, the overarching validity of the model is questionable. It has no easy implementation of transmission power, free space path loss, and strange results at different packet sizes and wavelengths. Based upon these negativities, the model is unable to match reality, so it is difficult to consider results adequate representations of true FSO.

2. Testing of Packet Size in NS-3

Simulating in NS-3 is the easiest way to model and conduct many experiments within an environment. When considering the effect of packet size at in high loss environments, simulation is the best way to provide this answer.

a. Methodology of Packet Size in NS-3

NS-3 is an effective simulation software, with the ability to simulate an 802.11 wireless network with many variables. Including the number of nodes, distance between nodes, transmission loss in environment, transmission power, IP layer protocols, etc. To create the simplest simulation of transmission rate and packet size, the simulation looks at packets being exchanged between two nodes. These nodes are varied based upon distance to increase or decrease the amount of loss incurred in the network.

To see how different packet sizes would affect the throughput of the system, the simulation is set up using the UDP protocol, sending two Megabytes of data. UDP allows for a lightweight protocol that only sends packets and does not wait for the response. This best display the effect of packet size on a network as the receiving monitors the number of packets received. This identifies the effect of packet size rather than the IP layer protocol.

The experiment was run by changing the data size from 300 bytes to 1000 bytes to determine how many packets would be received by the second node. The simulation will create 3 different outputted files. The first file is a trace file, including all interactions and packet movement in the simulation. The next two files are pcap files, which view network traffic from the viewpoint of a specific node. This collection of files allows the user to view an overview of packets movement and the viewpoint of a single node. This allows for the determination of the number of packets which are received at the endpoint. Using Wireshark allows for the analysis of pcap files, and see the number of packets which have arrived at the desired node.

b. Data and Analysis of Packet Size Simulation

The simulation described in Figure 32 demonstrates the effects of sending different packet sizes from a single node to sink at different distances. The output demonstrates the number of bytes received by the end node, or the system's ability to transfer data to the desired location. The simulation runs for the amount of time required to send 2MB of data to the desired location.

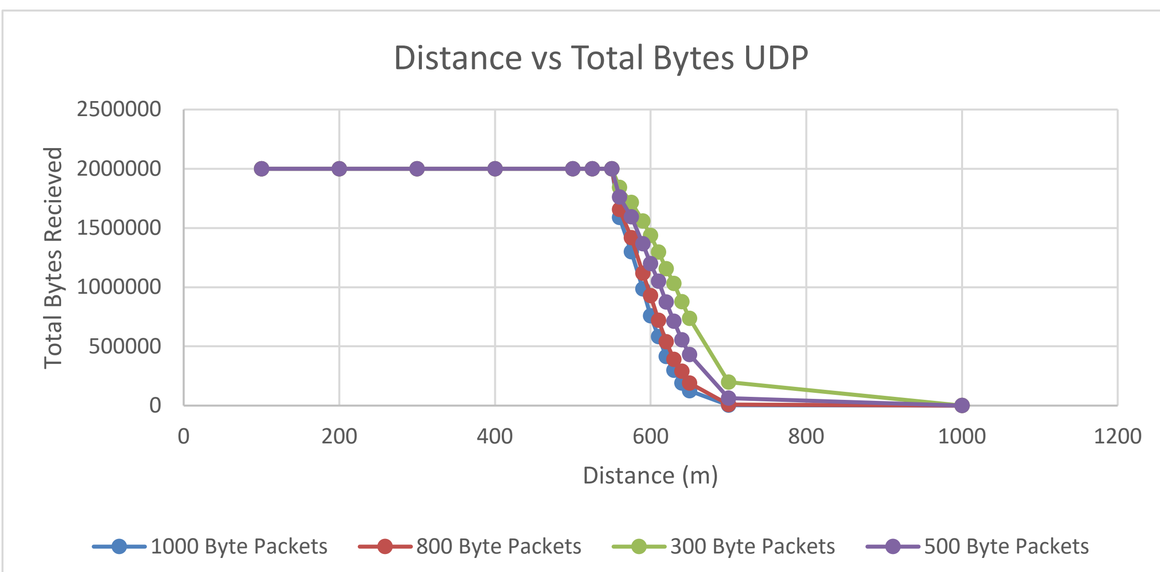

Figure 32. Distance versus Total Bytes Received for UDP

When considering Figure 32, the smaller packet size will deliver at least as many bytes to the destination, especially in areas where the system incurs losses. Found in areas between 575 and 600m. This demonstrates that using UDP in a heavy loss environment, the smaller the packet size the better chance that more data will arrive at the sink.

The simulation was duplicated for TCP having a sink and node at varying distances and packet sizes. This simulation may result in different conclusions for the same environment because of feedback is required for TCP. Due to TCPs feedback, we will consider packet size and distance versus three different variables: total bytes received, time, and goodput. The first being distance which results are displayed in Figure 33 and 34.

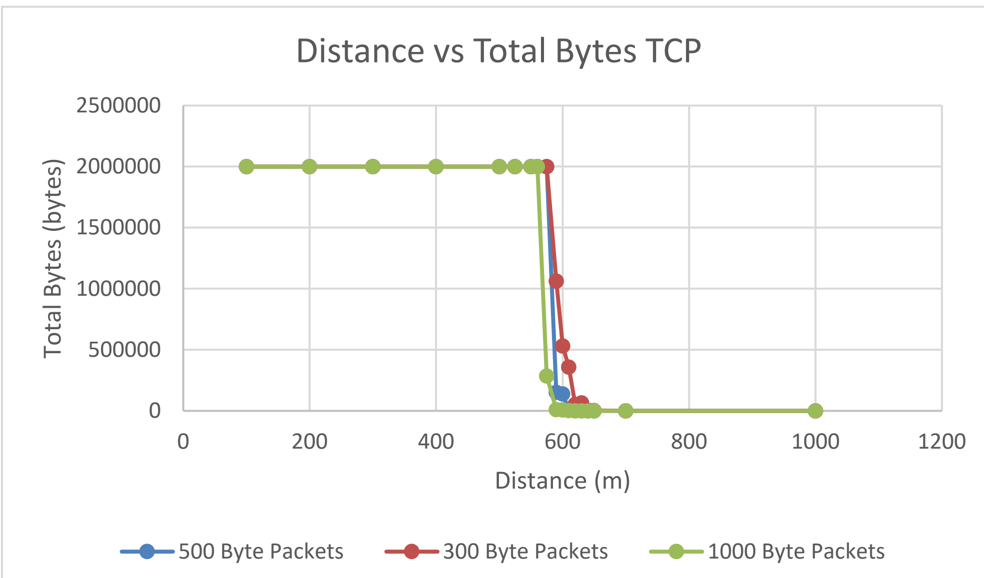

Figure 33. Distance versus Total Bytes Using TCP protocol

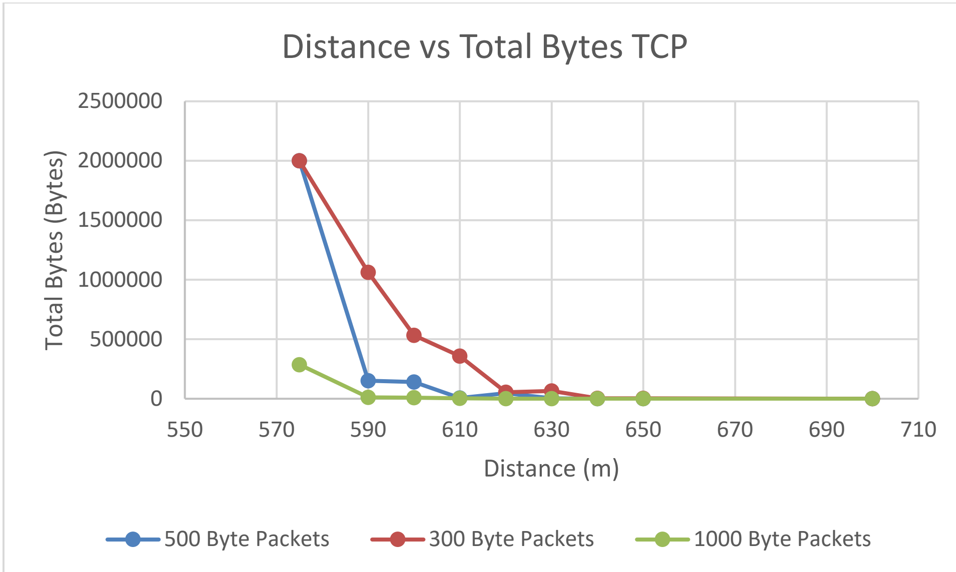

Figure 34. Zoomed In Distance versus Total Bytes Received

When considering the two graphs in Figure 33 and 3 demonstrate the same data, while Figure 34 is a more detailed view when it experiences loss. Once again when considering the total number of bytes, it is fairly obvious that smaller byte packets will deliver at least as many bytes. These points are exceptionally clear in Figure 34 as the 300 byte packets are always above the other packet sizes.

The simulation was set to run for a maximum of 1000 seconds, and TCP's run time can vary drastically based upon the topology or latency of the links. In this case, when packets are dropped, completion times will increase drastically. When considering the Figure 33 and 34, the smaller packet sizes achieve better transmission rates, and thus lower transmission times. In Figure 35 and 36, demonstrates the time that each simulation took to reach completion.

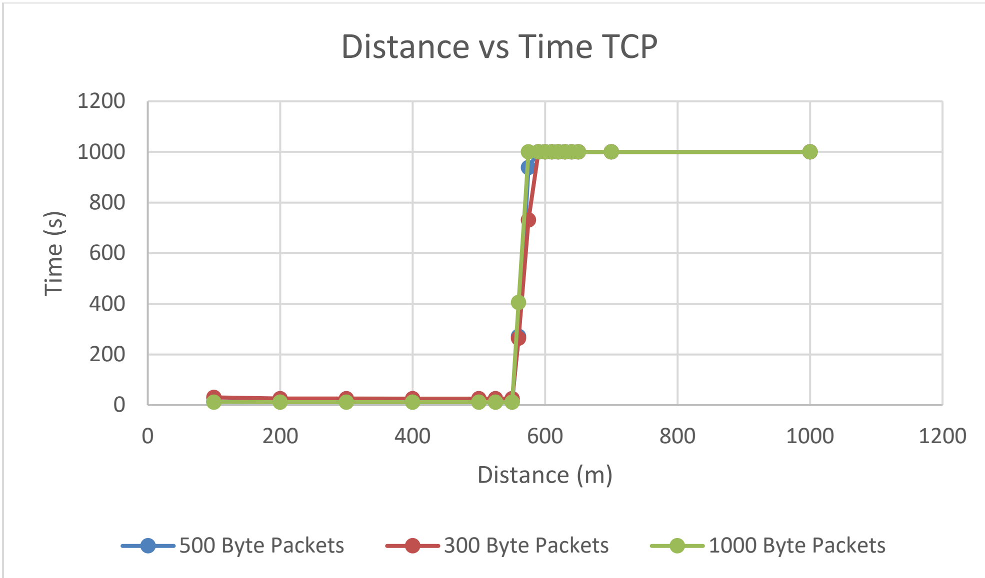

Figure 35. Distance versus Time Using TCP protocol

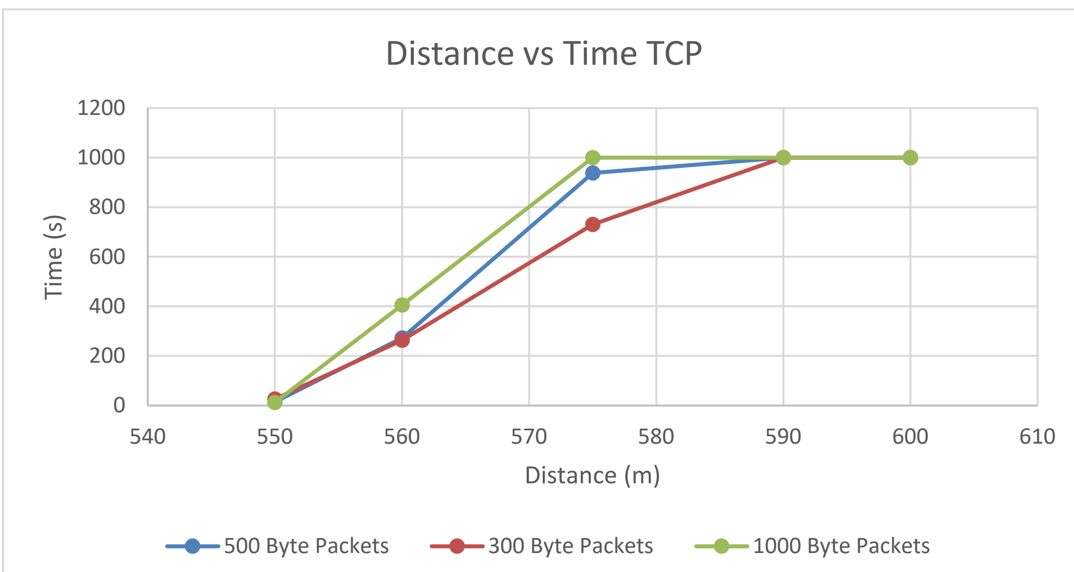

Figure 36. Zoomed in Distance versus Time for TCP

In Figure 35, when looking at large sections before 550m, the small byte packets have longer transmission times than the larger packet sizes. In Figure 36, the data in sections between 550m to 590m shows the smaller packets take less time. After 590m, all three packet sizes time out.

The reason for the observations made above, can be explained based upon features incorporated within TCP or the nature of smaller packet sizes. The smaller packet sizes taking longer up to 550m, makes sense, as the smaller packets will require more transmissions, compared to those of the larger packets. The 1000-byte packets will require three times less transmissions when compared to the 300-byte packets. TCP requires the proper arrival of ACKs before sending the next set of data. To send the same 1000 bytes the smaller packets must have six transmissions versus two. Therefore, the 300-byte packets requires a larger wait time to send the same amount of data. These results in Figure 34 and 35 make sense since the smaller packets require significantly more packets to send and receive all 2MB of data.

The benefits of smaller packet sizes are seen in distances between 550 to 590m as the smaller packet sizes took less time than the other packet sizes. This makes sense as smaller packet sizes results in less data being lost in transmission, and thus less retransmissions. Although it may take the 300-byte packets three times as many packets to transmit the same amount of data, more will arrive at the destination. Between 550 and 590m demonstrates the idea that TCP favors packet reliability because a triple duplicate ACKs forces TCP back into slow start. This failure to reliably send packets results in worse time performance than smaller packet sizes.

Finally all TCP packet sizes steady stated at 1000 seconds because the simulation timeouts. The 1000-second timeout does not indicate that no data has reached the end state. At distances of 590 to 650m the 300-byte packets timeout, but are having more data reaching the end state.

When comparing sending 2MB of data at different packet sizes and distances, bytes received and time taken can result in a confusing outcome. To compare all four variables (packet size, distance, time taken, and bytes received) the goodput is considered. Goodput is defined as the number of bytes received divided by the amount of time taken to receive this data. This data is demonstrated in Figures 37 and 38.

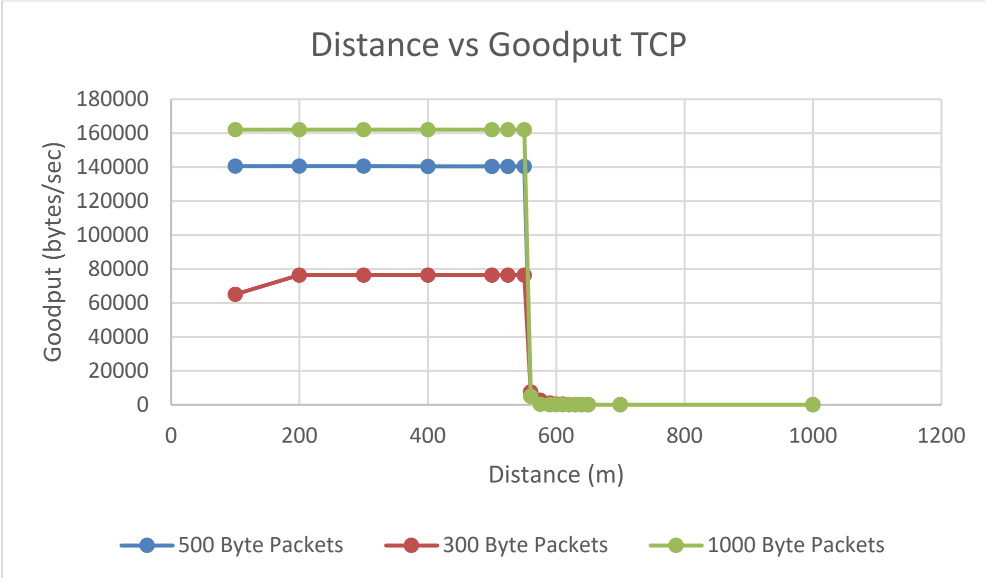

Figure 37. Distance versus Goodput for TCP Protocol

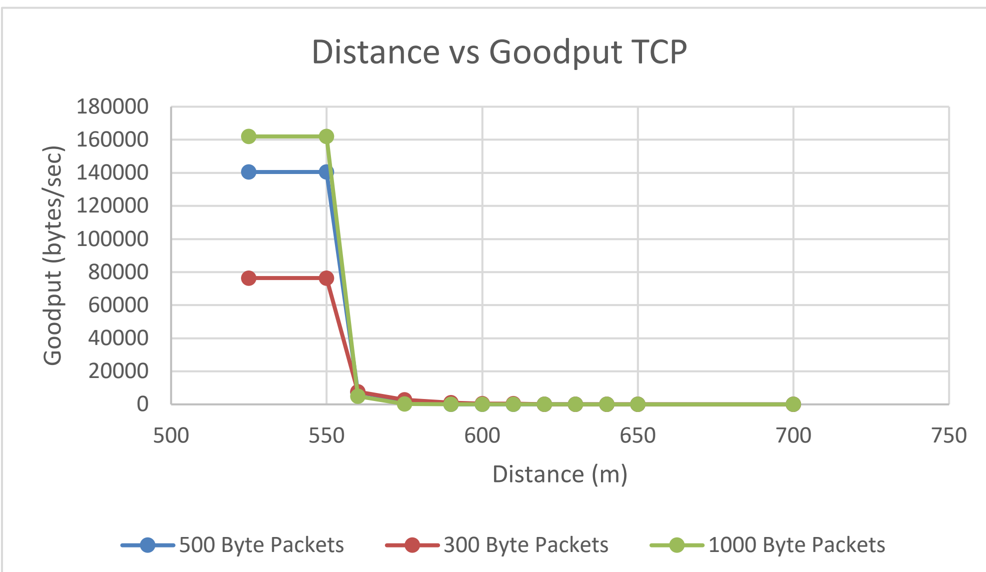

Figure 38. Zoomed in Distance versus Goodput

When looking at these results in Figure 37 and 38, there is a minimal argument to be made for smaller, 300-byte packets. The goodput benefits at distances less than 550m is significant for large packet sizes, while there are only minimal gains at distances greater than 575m for small packet sizes. Based on the goodput one would obviously choose larger packet sizes, unless they were sure that their system was at distances between 575 and 650m.

This conclusion of larger packet sizes makes sense, as goodput is a comparison between bytes received and time. Many networking systems rely on this type of ratio, because the user needs the most data available in a short amount of time. The difference occurs in systems, such as FSO, which cares about bytes received instead of the time taken. When considering a heavy loss environment, like those in distances between 575 and 650m, the smaller packet sizes can actually increase the systems goodput.

When comparing TCP with UDP systems both agree that smaller packets could result in more bytes being received. In TCP systems, the overall answer is a little more complicated, resulting in the best packet size depends upon the application. The next question is, which system, TCP or UDP, will deliver packets better. The simulation is considers and compares 300 bytes and 1000 bytes using TCP and UDP protocols. This is demonstrated in Figure 39 and 40.

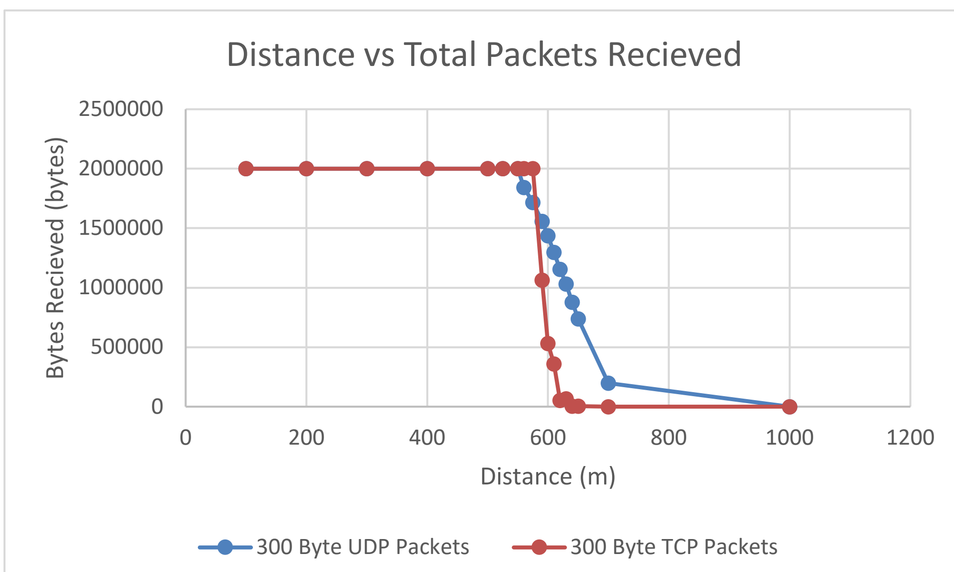

Figure 39. Distance versus Total Bytes Received for 300 Byte Packets

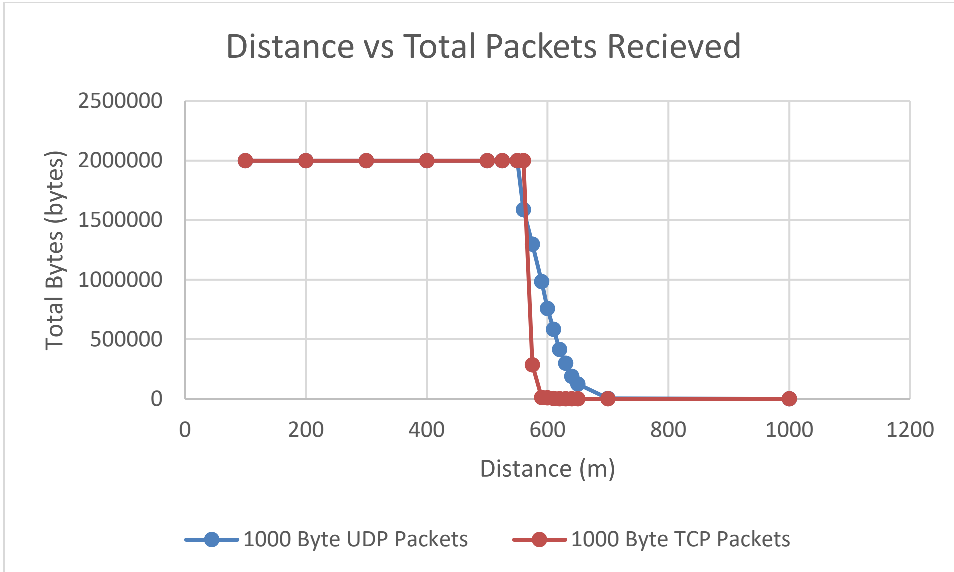

Figure 40. Distance versus Total Bytes Received for 1000 Byte Packets

When considering the above graphs, Figure 37 and 40, for packet sizes of 300 bytes and 1000 bytes, it is obvious that the UDP system is a more desirable system as more bytes are received at a majority of positions. Furthermore, when the system starts to lose reliability, the slope of the TCP system is much steeper.

The reasons for these results comes from the TCP and UDP protocols. TCP ensures that all data has reached the desired location. This results in feedback, ACKs, to ensure the delivery of the packet to the sink. This means that when a packet is lost, the system will respond and resend the packet to the destination. This can be seen at distances of 550m and 575m where the UDP system does not have the total 2MB data being received at the destination. The problem occurs when there is too much loss for TCP to be useful. The system will spend too much time resending packets, instead of focusing on sending new packets. This is demonstrated between distances of 600 to 650m where UDP was able to deliver more bytes successfully. In other words, TCP sends a packet multiple times making sure that all packets are delivered, leading to timeouts and less packets arriving at the sink.

c. *Conclusions of Packet Size Simulation*

The use in FSO is an excellent example where fragmentation and smaller data packets will be useful, especially if the links experience heavy losses. The end nodes must be able to handle the extra computation from fragmentation. The amount of computational power in each device can be increased to the desired values. Latency is still a concern, as in all networks, but a FSO network must be designed with expected losses.

The best situation would be to understand the type of operational environment to change and adapt the packet size depending upon the loss. This is, in some sense, what traditional 802.11 fragmentation does, but a more dynamic version of fragmentation could result in more data reaching the end state. Furthermore, in certain situations, it would be beneficial to oscillate between TCP and UDP packets as UDP can result in more data reaching the end state.

With regard to FSO, TCP small packet sizes would result the largest arrival rate for a two way system. If a one way system is needed a UDP type system would be beneficial. Furthermore, in all systems with no current time dependency, smaller packet sizes would be beneficial. They result in a larger packet success rate and thus more data reaching the end state.

B. EQUIPMENT SETUP

The goal of our proof-of-concept is to demonstrate network integration of a two-way FSO system, requiring the ability to transfer packets and responses between different networks. However, the equipment used in our proof-of-concept system is limited along many dimensions. To meet desired data rates, 1 Gigbit/sec, FSO visual communication link must have exceptionally high frame rates to transfer all of the desired data. In traditional engineering design, the hardware is over engineered to not limit or mask the desired results. In the case of this thesis, the primary goal is not to create a system which has the ability to achieve 1 Gigbit/sec data rates but to demonstrate its feasibility with our approach. Our secondary goal is to limit equipment calibration and continuity to isolate the networking considerations.

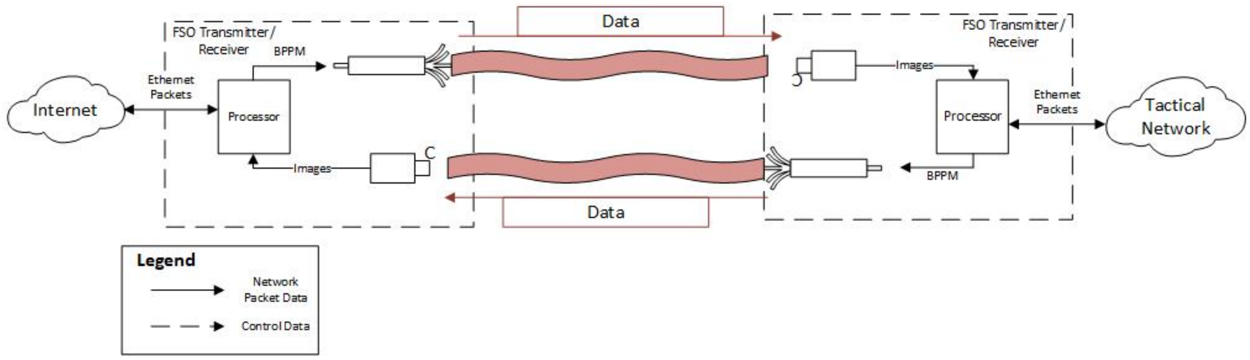

Figure 41. Overview of Physical FSO System

The proof-of-concept uses two cameras, two computer monitors, and two computers to process and transmit the desired images. The architecture is developed in Chapter III System Design, C Software, Architecture and in Figure 41. To demonstrate basic two-way communication one of the computers is the designated traffic source. This traffic source generates all of the network traffic and transmits this traffic to the first receiver. The receiver takes this traffic, modifies the header, and injects it into the internet. This packet injection results in a response from the internet, which is captured, and sent back to the original source. This response is then injected onto the network of the original traffic source. This methodology demonstrates that traffic originated on an off-internet network can receive an internet response via two-way visual communication.

The setup of the proof-of-concept has two monitors with 4 feet in-between and with cameras directed towards each. The cameras are positioned to the side of the monitor, and each monitor is angled to its corresponding camera. The positioning of the monitor square to the camera makes object identification easier. The computers, used for computation, are positioned close enough to connect to the monitors and cameras. The distance between transmitter and receiver is used to reduce possible losses due to distance.

1. Traffic Generation

The internet control message protocol (ICMP) Ping is used to generate basic network traffic between the transmitter and receiver. The ICMP protocol uses minimal Ethernet and IP headers, which allows easy header reconfiguration. Furthermore, Pings have the useful characteristics that they contain a single request and response to a known

IP address. As opposed to TCP communication, Ping does not require initial communication between the source and destination before transferring data; the request and response are the entire interaction.

The Ping request includes 52 bytes for the headers, packets characteristics, including source and destination MAC, source and destination IP, checksum, and length. These are used to properly route the packet to its destination, and determine if it has reached the proper destination.

The ICMP Ping protocol also provides the built-in ability of changing packet size to determine how the system will react with changes in packet size. The increase in packet size adds more data into the payload, resulting in longer transmissions along the visual link. The response to these requests will stop copying the payload (56 bytes) of the request to limit network traffic. The request and response can be characterized to determine if the packets have properly reached their destination.

The ICMP Ping protocol is easily recognizable on a network as there is minimal native ICMP interaction on a network. This prevents the packet capture from collecting unnecessary packets, although non-desired ICMP packets can be filtered out. Furthermore, the ICMP request and response pair can be easily identified on a network.

It is essential in the testing of a final state FSO link to consider the effects of different protocols and data draws on the visual link. For ease of use, the link must have all capabilities of a traditional link. Traditional traffic, both TCP and UDP, can be generated by a network traffic generator to test the systems operational limits. A link between an internet capable nodes can expect significant TCP traffic [20]. The generated traffic must correspond to expected network traffic. This is because some operational systems may need much less capability.

2. Transmitter

The transmitter in this test is a traditional computer monitor connected to the computation computer. Its job is to display the visually encoded data. This computer monitor connection is chosen for its ease of use, ease of troubleshooting and fewer errors than a higher refresh rate source.

The next generation of the system should use a LED board such as an Adafruit 32X32 LED board which has significantly higher refresh rate and display capabilities than a typical computer monitor. These boards are driven by microcontrollers, in this case an Arduino, resulting in either a pass-through or computation on the microcontroller. A pass-through will be required when achieving high data rates.

A future generation of transmitters which use lasers will support a significantly larger distances of transmission. The stronger the laser and different wavelengths based on the environment can reach longer distances. The first generation of lasers will be with a simple easy to use class III laser, such as a small 5mW 650 nm red 50 kHz laser. This will increase the transmission rates and distance over the led board.

The use of a computer monitor allows for demonstration and testing at extremely short ranges without excessive troubleshooting. The decision to use low-cost, off-the-shelf equipment is to support only the demonstration of the network capabilities. Basic two-way network communication does not require the significant data rates.

3. Receiver

The receiver is used to capture and process the data that is sent by the transmitter. This is most commonly done using cameras, but more advanced sensing techniques can be used to increase framerates beyond that of traditional receiving equipment. In this thesis, cameras are used and calibrated to receive data.

The current receiver is a high-resolution universal serial bus (USB) camera which is capable of receiving a maximum of 120 FPS at a resolution of 480p. The same system can receive at higher resolutions but lower framerates. When attempting to maximize data rates, resolution must be sacrificed for speed as long as the receiver has enough granularity to distinguish the separate nodes.

The higher the framerate of the camera the faster the system can identify and process new data. This is because the sampling rate has to be twice the speed of the transmitter to properly decode the data and prevent aliasing. There are consumer cameras which can capture hundreds of thousands of frames per second. These cameras do provide high sampling rates, but require difficult interface software.

The next generation of receivers could be diodes which will result in identification of lasers without the use of computer vision or high-speed cameras. Laser receiving diodes, photovoltaics (PV) cells, will drastically decrease the amount of computational power required to receive data, as computer vision can be a bottleneck at high framerates. Moving the receiver to hardware, such as PV cells, instead of software can increase the speed, but loses calibration flexibility. The transmitter or receiver must be manually calibrated for every change in location to properly receive the transmitted data.

The use of a plug-and-play type camera provides the ability to easily create a two-way communication link. These cameras do not require extra software, training, or special considerations to prevent their failure. This ease of use is desired over speed to demonstrate two communications, versus effort being used in camera calibration and interfacing.

C. OPTICAL LINK TESTING

The testing of the visual link is to determine the ability of the system to function as a network link within the desired test environment. To properly consider network capabilities, the setup as described in equipment setup with two transmitters and two receivers using the ICMP Ping Protocol to simulate network traffic.

1. Results

Our proof-of-concept FSO system demonstrates its ability to properly transmit data between two different networks and results in feedback between the two. There are multiple test iterations which implement different levels of packet filtering and header manipulation. Each level demonstrates the desired ability for two-way visual communication between different networks. Communication occurs between network one and network two. Network one indicates the tactical, non-internet, network which all requests originate. Network two indicates the network which is connected to the internet, and will always be receiving the requests form network one.

a. Test One

The first level of communication testing is between the two networks, network one and network two, with a pre-recorded Ping request packet. The recorded request, from network two, is manually transferred to the computer which is connected to network one. The computer injects this pre-recorded packet onto network one as if it had originated from a local Ping request. The same computer captures the packet and inserts it into a buffer to be sent to network two via visual data frames. These data frames are captured by the receiver on network two, converted into a network packet, and then injected into the internet without header modification. The internet response is captured and sent from network two to network one via visual communication. The captured internet response packet is then injected back into network one.

This system created in Test One demonstrates communication between two different networks. Furthermore, that a packet, sent with visual communication, can be injected and receive a response. The pre-recorded packet enabled the injection on network two without the requirement of header modification. This is not how a realistic system would work where requests originating on network one will be fulfilled by the response on network two. This does demonstrate that a response can be generated by a FSO system and create a two-way system.

b. Test Two

The second level of testing, considers two-way communication with a request originating on network one and response created on the internet. The ICMP Ping request is generated on network one, captured, and then stored in a buffer. This buffer is converted into visual frames and sent across the optical link to the receiver. The packet is received but is not natively capable of being injected onto the internet. This is because the Ethernet and IP headers are for the computer on network one. These headers must be removed and replaced with IP and Ethernet headers originating on network two. Once the new headers were applied, the injected packet (with new headers), will receive the proper response. This response is captured and visually transmitted to Network 1 and injected.

The system in Test Two also demonstrates the ability to create two-way communication. In this test, using visual communication the system is able to invoke and pass a response from a request originating on network one. This test truly demonstrates the abilities for visual communication to connect different entities.

c. Test Three

The final test is similar to that of Test Two, but must consider the effect of changing packet sizes. The visual system must be capable of dealing with packets which are requested using different protocols and sizes. This means that that the receiver and transmitter must be capable of dealing with these different sizes. The request begins on network one, which uses the ICMP Ping protocol with increasing size payloads. This request is captured and transmitted across the visual link. Due to the size of the payload the computation computer must replace the headers and calculate new checksums for this new header. Allowing for the injection of any sized payload, and receive a response from the desired source. This response is captured, sent, and injected back into network one.

The model found within Test Three demonstrates most capabilities found within traditional two-way communication but using a visual link. The FSO system must be capable of responding to requests found on network one, and manage different sized packets. The use of higher speed communications will result in communications within desired timeout periods.

2. Analysis

The solutions in each of the two-way packet communication tests demonstrates the ability to transmit data across a FSO system and then achieve a response. Each test has a progressive increase in capabilities, moving towards traditional communication between different networks. A FSO network must be able to consider changing packet sizes, which receive responses from an outside network.

The third network test models the characteristics of the desired connection between different networks, but its flaw is the bandwidth. The system meets desired specifications for a two-way communication, but is too slow for modern network communication. The receiver natively runs the cameras at five frames per second (FPS), resulting in a maximum sensing capability of 2.5 frames per second. This means that an average, ICMP Ping packet of 100 bytes, will take at least 320 seconds round trip time to receive a response. This is because this 100-byte packet, with error correction results in 400 bytes being transmitted. Each three by three frame contains one byte of data, so the system will need to transmit 400 frames. At 2.5 FPS, it will take 160 seconds to transmit the entire 400 bytes one way. Without considering any other delays, the visual system will take 320 seconds to deliver a response for a request.

This can be dramatically increased by using more capable system components. When pushing the receiver to its maximum of 120 FPS, the system can properly sample and identify a maximum of 60 FPS. For the same 100-byte packet, it will now take a minimum of 13.3 seconds round trip time for a request to receive its response. This is 24 times faster of a response than the system with 5 FPS camera sample rate.

The inclusion of more data per frame, by expanding the size of the array, such as increasing from a three by three matrix to a four by four matrix, will close to double the amount data capable of being encoded into a system. Doubling the amount of data which could be encoded, will also half the transmission time. Meaning that the 13.3 round trip response time will be shortened to 7.6 seconds with the inclusion of seven more lasers or data points. When comparing this type of system to a QR system, which has the ability to encode much more data per frame, can drastically decrease latency. Without considering computation times, a 29 by 29 arrayed system, with minimal error correction can encode 440 bits per frame. This means that there will be 55 bytes per frame at 60 fps, or 3300 bytes/sec. This larger array will be able to achieve a round trip time in 60 milliseconds. This is much closer to the desired latency, but computation of encoding/decoding QR frames will cause a bottleneck in the system. Limiting the framerate to undesirable rates.

This demonstrates how increases in the sampling and transmission rates can drastically increase the speed of transmission. This is even without changing the methodology of the system, but pushing the current equipment to its limits. Although there is a 24 multiplier increase in performance when running the cameras at their maximum FPS, this round-trip time of 13.3 seconds is still orders of magnitude too slow for normal networking operations. A normal ICMP protocol will expect to receive a response in 13 milliseconds. It is expected that the current setup would be unable to reach desired networking speeds, but did demonstrate basic two-way networking capabilities with FSO transmission.

3. Extrapolation

The interesting consideration of a two-way communication is with the extrapolation of the results into more suitable equipment. This equipment allows for high data rates and thus low latency, capable of gigabit/sec network speeds. With more capable equipment, receivers and transmitters, the data rate could be drastically increased.

Considering a more advanced transmitter such as the small 5mW class III 650 nm red 50 kHz laser, higher framerates can be achieved over the monitor displayed. The 60 Hz frequency of the monitor compared to the small class III laser, 50 kHz, there is a drastic increase in data rate. If a receiver can capture and process different frames at 50 kHz, the system is able to transmit 50,000 frames per second. If each frame contains a byte of data, the system will achieve 50 Kbytes/sec or 400Kbit/sec. Using an introductory laser results in low modern internet speeds, and drastically decrease latency of the system. Without using specialized, expensive lasers, and assuming that each frame can be captured and decoded at necessary rates, this system demonstrates next generation data rates.

When considering the receiver and framerates of cameras, there can be large increases in the FPS compared to the system developed in this thesis. Researchers have developed a trillion FPS camera which allows for the use of 500 billion frames per second [21]. This means that data can be sent at a rate of four trillion bits per second, but this camera is at the far limit of possible receivers. With an over the counter system, the phantom v2512 (currently costing approximately $125,000) has the ability to achieve 25,000 fps at one megapixel and up to one million fps at a resolution of 256x32. This minimal resolution may be adequate to recognize a three by three array of lasers. This over the counter receiver allows for a sample rate of 500,000 fps, and thus achieve a four Mbit/sec data rates.

Next generation transmission and receiving equipment provide high data rates and low latency because of high frequency and frame rate equipment. These pieces of equipment can be found and purchased by the user, but with specially designed equipment, these data rates can be increased even further. At these extremely high framerates, it has been assumed that the processing will keep up with the system. This is no easy task and will require significant computing power and optimization, or specifically designed equipment.

The use of computer vision, provides some necessary capabilities, but could be an unavoidable bottleneck. To overcome this bottleneck, the system may need to implement a new version of sensing without the use of computer vision and cameras. This results in more experimental hardware such as PV cells where the receiver measures the number of incoming photons. This type of measurement could be significantly faster than traditional computer vision and require significantly less processing.

D. SUMMARY

This chapter discusses the equipment, testing, results, analysis, and extrapolation of two-way communication within a FSO system. The chapter also looked at possible simulation of FSO systems. This showed the failures of a single basic FSO simulation, but the possibilities of limiting packet size. This thesis did demonstrate the ability to create two-way visual communication system by capturing, transferring, header modification, and injecting network-based packets. The FSO injection system developed in this thesis does not achieve useable data rates or latencies for modern network operations. Although this is negative, it is shown that with equipment improvements these data rates and latencies will rival slow internet connections. With professionally developed equipment, data rates can rival the fastest of wired internet speeds.

V. CONCLUSION

This chapter provides the conclusions for this work on creating a two-way network communication using visual links. It includes the pertinent observations made when testing the system. The chapter also discusses possibilities for this technology and the next generation of future work.

A. OBSERVATIONS

This thesis was successful in handling the initial research concern: the viability of two-way optical links between networks. This paves the way for further testing of FSO links using different application layer protocols. Most modern applications rely on a backbone of two-way internet communication, typically by using TCP. Two-way communication is the heart of a MIMO system, increasing complexity over a simple SISO system. This thesis demonstrates the plausibility of two-way communication using a visual channel at modern data rates.

1. Use of 3x3 Array Rather than Traditional QR Code

Although there are benefits to the use of QR codes, they can face challenges with the speed of encoding/decoding and environmental transmission losses. QR codes are known for their ability to transfer large amounts of data in a relatively small sized image with built-in error correction. They are suitable for high speed scanning. The QR code is primarily designed for single use scanning where latency is not an issue. Typical use includes scanning packages and other mobile applications in which orientation and data capacity are larger concerns. This means that the encoding/decoding of a QR system may be too slow for visual network communications for which encoding and decoding latencies must be very small.

The speed of encoding and decoding could be solved by using powerful computational hardware. This, however, does not account for environmental effects when transmitting images, including Gaussian noise and fades (laser wave is pushed out of fade due to attenuation). QR codes are designed to overcome the effect of physical damage, rather than that of the environment. These environmental effects can cause node failures, and sometimes, losses of entire frames. This causes a fade to be exceptionally important as a node can be lost for thousands of frames.

Simpler encoding schemes, such as binary pulse position modulation, provide the capabilities of reaching high frequencies with included error correction. This does result in the loss of many QR code benefits including ease of scanning or relatively small size. These benefits, although useful, are not essential for the functionality of high-speed visual communication. Furthermore, other methods of error correction can be used instead, such as Reed Solomon and Reed Muller encoders.

2. Error Correction Sequence

The use of Reed Solomon and Reed Muller encoders provide significant error correction capabilities without the use of traditional QR codes. These encoders allow for the correction of traditional Gaussian noise and fades. This allows for entire frame correction and recovery up to a threshold (three nodes) if lost, even for many contiguous frames. The negative of this error correction scheme is that it quadruples the data size, therefore quadrupling latency and quartering bandwidth. The benefit is that this scheme outperforms the industry standard (duplicate data) and traditional QR code's error correction.

3. Computer Vision Slows Down the Process

The use of computer vision provides ease of use and flexibility but does impose performance limitations. Computer vision allows for easy calibration and image recognition regardless of environmental conditions, but requires extra processing time. Similar to the QR code's encoding/decoding slowdown, computer vision is expected to bottleneck the system at high framerates. It is difficult to complete real-time post-reception image processing, especially when expecting thousands of frames per second. A hardware or streamlined method of sensing the transmitted data is required such as PV cells. PV cells have the capability of measuring the transmitted photons and determining the transmitted data.

4. Implementation of Two-Way Communication

The created proof-of-concept system met the desired requirements of two-way optical communication. This system demonstrates potential for carrying network traffic in future systems. Although a two-way optical communication system was created, it is explained that to reach desired data rates, significant upgrades must be completed. Furthermore, to reach full capabilities of Gigabit/sec data rate, specialized construction of software and hardware will be needed.

5. FSO in Tactical Environments

The use of FSO in a tactical environment enables capabilities not available in traditional communication methods. Not only can optical communication meet or exceed traditional RF data rates, but includes increased security, resistance to jamming, and increased portability. This provides warfighters the ability to communicate effectively within the next generation of warfare.

B. SUMMARY

The research described in this thesis shows the potential of two-way network communication within an RF-denied environment. This is essential for traditional internet protocols using an optical link when interfacing between separate networks. This thesis provides an important stepping stone in this process of linking networks visually without having to create a new packet standard. The visual link is created with over-the-counter equipment, but specialized software and hardware can increase data rates to useable speeds.

C. FUTURE WORK

Future research is needed to increase the efficiency and effectiveness of an arrayed optical network.

1. Implementation of an Arrayed Laser System with High-Speed Receiver

The most important future work is to create an operating model capable of achieving higher frequency framerates, which will result in acceptable data rates and latencies. This would entail using a receiver which can achieve higher framerates and a higher frequency transmission than used in this research. The first step will be a small arrayed laser transmitter and a high-speed camera receiver. Implementation of these two systems will require testing and experimentation to determine all bottlenecks and effective data rates.

2. Optimizing the System at Distances

All proposed and tested FSO links were created at short distances to demonstrate data links without loss. Increasing the distance between transmitter and receiver, as would be required in a tactical environment, results in environmental losses due to attenuation. Although the designed optical link includes error correction, error rates vary depending on link distances and environmental factors. Separate error correction models maximize the data rate within different environments. The class and color of lasers can affect data reception along with method of error correction. The software and hardware can be tuned and optimized to maximize effectiveness and efficiency when sending data at different distances.

3. Future Generation of Optical Links

Artificial intelligence (AI) or machine learning has the capability to optimize the visual link automatically. This proposed system can recognize environmental factors based on loss, and properly tune the system to achieve the highest data rate and minimize latency. AI and machine learning can automatically choose between error correction models, packet size, frame size, or laser color to suit the operational environment.

LIST OF REFERENCES

[1] C. Casey, "Free space optical communication in the military environment," M.S. thesis, Dept. of Computer Science, Monterey, California, USA, 2014. [Online]. Available: https://calhoun.nps.edu/handle/10945/43886

[2] S. S. D. Neo, "Free space optics communication for mobile military platforms," M.S. thesis, Dept. of Computer Science, NPS, Monterey, Ca, USA, 2003. [Online]. Available: https://calhoun.nps.edu/handle/10945/6160

[3] N. Baranwal, "Digital modulation techniques," Univ. of Allahabad, Prayagraj, India. Jan. 27, 2016. [Online]. Available: www.slideshare.net/nidhibaranwal/digital-modulation-techniques-57572540

[4] O. Bouchet, *Wireless Optical Telecommunication*s, 1st ed. Hoboken, NJ, USA: John Wiley & Sons, 2012.

[5] R, Johnson, *Antenna Engineering Handbook*. New York, NY, USA: McGraw-Hill, Inc, 1961.

[6] O. Timus, "Free space optic communication for Navy surface ship platforms," M.S. thesis, Dept. of Computer Science, NPS, Monterey, Ca, USA, 2004. [Online]. Available: https://calhoun.nps.edu/handle/10945/1623

[7] A. W. Felder, "Array based free space optic systems for tactical communications," M.S. thesis, Dept. of Computer Science, NPS, Monterey, Ca, USA, 2018. [Online]. Available: https://calhoun.nps.edu/handle/10945/59655

[8] A. R. Lucas, "Digital semaphore: Technical feasibility of QR code optical signaling for fleet communications," M.S. thesis, Dept. of Information Sciences, NPS, Monterey, Ca, 2013. [Online]. Available: https://calhoun.nps.edu/handle/10945/34699

[9] DENSO Wave Incorporated. "QR code essentials," October 23, 2018. [Online]. Available: http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D

[10] B. Badawi, T. Aris, N. Mustapha, and N. Manshor, " Fuzzy encoder for four layer color QR Code," in Proc. of IC-ITS, Selangor, Malaysia, Oct 30–31, 2018.

[11] J. W. Lai, "Free space optical communication for tactical operations," M.S. thesis, Dept. of Computer Science, NPS, Monterey, Ca, 2016. [Online]. Available: https://calhoun.nps.edu/handle/10945/50573

[12] D. Killinger, "Free space optics for laser communication through the air," *Optics and Photonics News*, vol. 13, no.10, pp 36–42, 2002.

[13] D. Bhaskar and M. Bhawna “Performance evaluation of MAC protocol for IEEE 802. 11, 802. 11Ext. WLAN and IEEE 802. 15. 4 WPAN Using NS-2,” *International Journal of Computer Applications*, vol. 119, no. 16, pp. 25–30.

[14] IEEE Standard for Information technology--Telecommunications and information exchange between systems local and metropolitan area networks: Standard 802.11, 2016, [Online]. Available: http://ieeexplore.ieee.org/ stamp /stamp.jsp?tp=&arnumber=7786995

[15] IEEE Standard for Ethernet: Standard 802.3, 2015, [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7428776

[16] P. Keeley, “Optimal FSO encoding scheme,” unpublished.

[17] M. D. Perna, “Fso Module,” NS-3 FSO Module - Model Library. March 2019. [Online]. Available: www.nsnam.org/reviews/2016/socis-midterm/fso.html

[18] M. J. Lok, I. E. Lee, Z. Ghassemlooy, G. C. Chung, “Investigation on the error performance of modulation formats in free-space optical communication links with turbulences,” presented at Communication Systems Networks and Digital ignal Processing (CSNDSP) 2016 10th International Symposium, Jul. 20–22, 2016, pp. 1–6.

[19] Suite, M R, and W J Scharpf. “Packet testing in free-space optical communication links over water.” *Proc. of SPIE,* vol. 6215, pp. 32–41, 2006. [Online]. Available: http://search.proquest.com/docview/28134763/

[20] D. Xu, X. Liu, and A. Vasilakos, “Traffic-Aware resource provisioning for distributed Clouds,” *IEEE Cloud Computing,* vol.2, no. 1 pp. 30 – 39, Jan 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7091770

[21] J. Lewis,”Lund university develops 5 trillion FPS film camera,” *Vision Systems Design*, vol. 22, no. 6, pp. 9–12, Jun 2017.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California