NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MODELING AND ANALYSIS OF MASKED CARRIER CHANNEL ACOUSTIC COMMUNICATION

by

Carlos F. Hargett

June 2021

Thesis Advisor: Justin P. Rohrer
Co-Advisor: Charles D. Prince

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE MODELING AND ANALYSIS OF MASKED CARRIER CHANNEL ACOUSTIC COMMUNICATION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Carlos F. Hargett	
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)

Legacy Navy communication systems are used for command and control in underwater fighting environments. Adversaries will seek to deny these communication mediums. Additionally, the use of these communication systems may reveal the tactical location of blue forces, creating an inherent need for innovative methods of communication. Using sonar systems in the underwater channel between vessels to transmit a desired signal disguised as ambient ocean noises or biologics is a possible way to communicate with a low probability of interception or detection. The purpose of this research is to examine the feasibility of transmitting data covertly in a multi-user scheme, using underwater acoustic means over program-of-record U.S. Navy technology, and to determine a model for doing so with associated physical and technical requirements. Future research should include novel approaches to steganography.

14. SUBJECT TERMS steganography, acoustic, Passerieux, underwater	**15. NUMBER OF PAGES** 83
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MODELING AND ANALYSIS OF MASKED CARRIER CHANNEL ACOUSTIC COMMUNICATION

Carlos F. Hargett
Lieutenant, United States Navy
BS, U.S. Naval Academy, 2014

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Justin P. Rohrer
Advisor

Charles D. Prince
Co-Advisor

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Legacy Navy communication systems are used for command and control in underwater fighting environments. Adversaries will seek to deny these communication mediums. Additionally, the use of these communication systems may reveal the tactical location of blue forces, creating an inherent need for innovative methods of communication. Using sonar systems in the underwater channel between vessels to transmit a desired signal disguised as ambient ocean noises or biologics is a possible way to communicate with a low probability of interception or detection. The purpose of this research is to examine the feasibility of transmitting data covertly in a multi-user scheme, using underwater acoustic means over program-of-record U.S. Navy technology, and to determine a model for doing so with associated physical and technical requirements. Future research should include novel approaches to steganography.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

CDMA code division multiple access

CSMA carrier sense multiple access

CSMA/CA carrier sense multiple access / collision avoidance

CTS clear to send

DSSS direct sequence spread spectrum

HF high frequency

MAC media access control

MMPE Monterey-Miami Parabolic Equation

OFDM orthogonal frequency division multiplexing

RTS ready to send

SNR signal to noise ratio

SSP sound speed profile

UDP User Datagram Protocol

VLF very low frequency

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I would like to thank Justin Rohrer and Charles Prince as my advisors for guiding me along the way.

I would also like to thank Ryan Ferrao, of whose work this is a continuation. You have helped in many tangible and intangible ways.

Additionally, I would like to thank all those at NPS for contributing to my learning and research even if only tangentially.

Finally, thank you Lauren, and everyone who helped at home while I completed this endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Vulnerabilities of legacy Navy communications systems create a need for innovative communication methods. Threats to these systems, which are used for command and control in warfighting environments, include denial by adversaries and situations in which the available use of these systems may reveal the tactical location of blue forces [1]. The use of underwater acoustic communication systems to transmit a desired signal disguised as ambient ocean noises or biologics is a possible way to communicate with a low probability of interception or detection.

This research has two thrusts: measuring the performance of collision mitigation via the application of carrier sense multiple access (CSMA), media access control (MAC), and Collision Avoidance to novel Passerieux implementations of masked underwater accoustic communication and multi-user communication via the application of code division multiple access (CDMA) schemes to auditory steganography in an underwater medium.

In this introductory chapter we cover the benefit to the Navy and Department of Defense, research questions, the scope of the thesis, methodology and organization.

1.1 Benefits of Study

Underwater communications is a challenging field. The submarine force has adapted a passive approach due to the ease of recognition and locating methodologies [1]. Similar challenges apply to any operations conducted below the surface of the ocean. Masked underwater communications will allow for the freedom to communicate in the underwater environment. Command and control as well as datalinks are vital to operations. This research intends to expand on the topic by allowing for multiple users or nodes in the network, allowing for undetected command and control, and information sharing amongst multiple users in a sub-surface environment.

Masked underwater communications are an important capability in that the masking or hiding of underwater communications mitigates or outright removes the vulnerabilities pre-

sented above. The current iteration of Passerieux's method for underwater communcation does not account for multi-user, multi-node implementations; however, a framework that allows for multiple nodes or users to communicate is both more useful and in many scenarios, a practical requirement. One could argue that in a free flowing environment such as in underwater military operations, multi-user communication is a necessity.

Along with multiple users communicating comes the need to resolve conflicts and collisions. Communications in the electromagnetic spectrum have been facing, resolving, and optimizing these issues for decades at this point. The underwater acoustic environment has its own idiosyncrasies which need to be addressed and measured against the solutions that have already been developed.

1.2 Research Questions

- How does CDMA affect the transmission rate and symbol resolution of Passerieux embedding and extraction?
- How do different CSMA and MAC schemes perform given the environment?
- Can masked underwater acoustic communications be achieved at practical speeds using Passerieux's method?
- Can multi-user communication be achieved at practical speeds using Passerieux's method of masked underwater acoustic communications?

Secondary research questions include the following:

- Which bit rates, as a result of steganographic schemes, are viable in a multi-user, non-linear network environment?
- Which bit rates, as a result of multiple access coding schemes, are viable in a multi-user, non-linear network environment?

1.3 Scope

This research was primarily conducted using a model. As such, the next logical step would be to verify the findings here with real, at-sea tests. The model uses both shallow and deep water environmental parameters, but additional environments that capture variables such as temperature, salinity and extreme noise levels would be worthwhile additions that

were simply beyond the scope of this research. In Chapter 3, we use four MAC schemes, however there is a plethora of commercial, proprietary and custom implementations that could be tested. This research focuses on common and simple implementations to explore the performance of widely used schemes and of stripped down implementations which reduce the overhead transmission costs.

1.4 Literature Review

There are three areas of literature that are particularly useful for reviewing the material: Passerieux's patent [2], Ryan Ferrao's thesis [3] and Reed-Solomon's error code [4]. Passerieux's patent is the foundational concept that this work is built upon. In the paper, Passerieux describes the titular Passerieux method for inserting data into a cover signal. Ryan Ferrao's thesis is a specific implementation of Passerieux's method. Ferrao wrote his transfer, embedding and extraction functions in MATLAB using natural whale sounds as the cover. He used the Monterey-Miami Parabolic Equation (MMPE) model to simulate the transmission in a simulated maritime environment. Finally we use Reed-Solomon forward error correction in Chapter 4 to describe and shape our performance envelope. Reed-Solomon's error code is the initial paper describing the addition of parity bits in a transmission frame to recover a matrix of data.

1.5 Approach and Significant Findings

This thesis builds upon the work of Ryan Ferrao, who managed to successfully model covert communications using the Passerieux method at BPSK speeds (2, 4, 10 b/s). Research focuses on applying multi-user algorithms to the novel approach by Ferrao and then to using schemes of higher speeds than BPSK [3]. We simulate multiple underwater environments to test the Passerieux method, then mathematically evaluate MAC schemes and develop performance envelopes to discover suitable schemes, parameters, and implementation variables. CDMA walsh codes are attempted as modifications to an implementation of Passerieux's method, but are ultimately unsuitable due to the predicatable distortion shown in Section 4.3.

1.6 Organization

The structure of the thesis follows:

Chapter 2: Background

Chapter 2 describes underwater acoustics research, steganography, and terms. We describe underwater steganography in the acoustic channel, with special attention to the Passerieux technique. Then we discuss the common multiple access schemes and their applicability to the research topic. Finally, we discuss media access protocols within the context of this research.

Chapter 3: Methodology

In Chapter 3 we discuss our overall methodology including specific programs, models and parameters used in our exploration of MAC protocols. We generate mean bit error rates, data frames, and calculate transmission delay to serve as a base for the theoretical maximum throughput that can be achieved after we apply common MAC schemes to our steganographic method.

Chapter 4: Results and Analysis

Chapter 4 describes the simulation, our reasonings, and findings for the application of forward error correction as well as the effect of MAC schemes. Finally, we end by showing the unsuitability of CDMA on the Passerieux technique.

Chapter 5: Conclusions and Future Work

Chapter 5 presents the final conclusions and future work of the thesis.

CHAPTER 2:
Background

Masked underwater communications and their optimization are a relatively unexplored research area. Chapter 2 discusses steganography, biological mimicry in the environment, binomial distributions, multiple access schemes, and CDMA.

2.1 Steganography in Masked Underwater Channels

Steganography is the process of hiding a message within another source. In this case we will be embedding data into a sound file, then transmitting that sound underwater.

2.1.1 Steganography Principles

Steganography is the embedding of a message into an object. The detectability of the modified object is typically of no consequence. When correctly implemented, the message is undetectable despite being in plain sight. This allows for covert and/or low probability of detection in environments or situations where secrecy would not be possible. Steganography has old roots but conceptually, it has become especially powerful in recent times due to the complexity of digital signal communications.

2.1.2 The Steganographic Channel

The five basic elements of a steganographic channel are a source of cover, algorithms, keys, message source and communication channel.

2.1.3 Cover Source

The cover source is the audio channel that will be embedded with the hidden message. The cover source must be overt and relative to the message with quantifiable properties.

2.1.4 Embedding and Extraction Algorithms

The embedding and extraction algorithms are the processes by which we insert information into a cover source, transmit the transformed signal, and recover that original information

from the signal at the receiving end after transmission.

2.1.5 Steganography Key

The steganography key is a randomly created value used during the embedding algorithm for the Passerieux technique.

2.1.6 Message Source

The message source, or message, is the hidden value that is to be inserted. Modern analysis has rendered plain messages to be vulnerable based on metrics and statistics even after embedment in the cover source. Variables like size or frequency of characters can reveal enough information for a forced decoding. The message should be transformed prior to embedment.

2.1.7 Communication Channel

The communication channel is the media by which the embedded message and cover will be transmitted. This channel is considered insecure and subject to monitoring, denial, or manipulation by outside actors. Tampering is beyond the scope of this research.

2.1.8 Audio Steganography

Audio steganography has greatly expanded with the rise of digital signal technologies. Parameters of interest are the ability to insert large amounts of data, the ability to accurately recover that data, the degree to which the acoustic source is able to be transformed, and the resistance of the transmitted signal to attenuation.

2.1.9 Masked Underwater Acoustic Communications

Masked underwater acoustic communications are more difficult than transmission through air due to the inherent properties of the environment and the unique costs imposed by the desire for covert or clandestine communication to begin with. The underwater acoustic environment is especially susceptible to attenuation from the effects of pressure, temperature, and salinity. Natural background noise is present in the environment due to sound travelling long distances from biological and non-biological sources. An underwater acoustic scheme

must take extra measures to account for these difficulties, usually in the form of slower bit rates due to longer wavelengths being more resilient. When balanced with the aforementioned desire for imperceptibility in steganography, the underwater environment can be a very challenging medium.

2.1.10 Biological Mimicry

Underwater channels carry acoustic signals long distances. It is entirely feasible for biological acoustic signals to be present in many environments. Something as simple or obscure as dolphin communication clicks would be an appropriate sound source. Generating a fake biological signal and embedding a message via a steganographic scheme then broadcasting this newly generated artificial, biological signal is possible and promising [5].

Table 2.1 is taken from the Discovery of Sound in the Sea website and is populated by the University of Rhode Island, NOAA, and other partners [6]. The source levels for some sounds generated by marine life and man-made sources are given in Table 2.1. The source levels of sound producers are given in underwater dB at 1m. Source levels are defined as if the receiver was one meter from the sound source. The sound levels given in the table are ambient noise levels in a 1Hz wide bandwidth meaning that the acoustic energy was only summed over 1Hz.

Table 2.1. Deep Source Sound Levels (dB)

Source	**Source Level (dB)**
Sperm Whale Clicks	163 - 223
Spinner Dolphin Pulse Bursts	108 - 115
Bottlenose Dolphin Whistles	125 - 173
Fin Whale Moans	155 - 186
Blue Whale Moans	155 - 188
Gray Whale Moans	142 - 185
Bowhead Whale Tonals, Moans and Song	128 - 189
Humpback Whale Song	144 - 174
Humpback Whale Fluke and Flipper Slap	183 - 192
Southern Right Whale Pulsive Call	172 - 187
Tug and Barge (18km/hour)	171
Supply Ship	181
Large Tanker	186
Ice breaking	193
U.S. Navy sonar	235
U.S. Navy sonar	223
SURTASS-LFA	215

Table 2.2 references sound levels from multiple studies measuring specific biologics and ambient noise sources [7], [8], [9].

Table 2.2. Shallow Source Sound Levels (dB)

Source	**Broadband Source Level (dB)**
Marbled Male Goby Fish (Mating)	130
Sand Goby Fish	121 - 138
Padogobius Bonelli	91 - 101
Mulloway Argyrosomus Japonicus	160
Oyster Toadfish (Mating)	125
Alpheus Glaber Snapping Shrimp	200
Harbor Porpoise	170
Surface Wave	55 - 160
Wind (2 - 37 knots)	30 - 75
Shipping	35 - 95

2.1.11 Masking

Liu et al. discuss biological mimicry in an underwater channel using direct sequence spread spectrum (DSSS) signals masked by a whale signal [10]. Whale biologic signals tend to be an inherently lower frequency, the DSSS signal is at a higher frequency and a lower power which exploits a phenomena wherein the high power, lower frequency signal masks the higher frequency signal. Biological mimicry and masking are natural progressions of this research.

2.1.12 Recorded Noise

Recorded noises appear to be a viable and feasible form of steganography. Passerieux lists such challenges as the inherent patterns of DSSS and orthogonal signals, as well as the relatively high complexity of artificially generated biologic signals [2], [11]. While DSSS and orthogonal frequency division multiplexing (OFDM) schemes have a low probability of detection, skilled sonar operators may be able to detect such signals. Recording a biologic signal, then using that signal, accomplishes the benefits of a biological signal's ability to be an overt communication channel without the complexity of generating a genuine signal artificially. Furthermore, if the signal can be recorded either from the environment or in-situ, the level of validity increases. A genuine-looking signal reduces the chance of further

scrutiny, achieving the desired covert effect.

2.1.13 Passerieux's Technique

J.M. Passerieux published a new steganography technique. This technique depends on manipulation of a continuous sound sample of a pre-recorded sound [2], [11]. Passerieux recorded a sound clip of dynamic length as a cover signal. The signal itself is split up and modified to represent the coded message, which is then reinserted into the cover via standard steganography practice. This cover signal is modified by dividing said signal into milliseconds-long intervals that total the number of symbols in the message. Each segment has an operator applied to its demodulated form this pre-manipulation ensures that SNR is reduced at the received end which is a property desired in covert operations and communication. A steganographic key is also applied in this process in order to express the desired symbol or character to represent the message. Passerieux's method in particular is resistant to Doppler effects, a desired attribute in a challenged underwater environment. The value generated by the above operation is added to each interval of the cover channel and recombined to form the new steganographic signal, which should be minimally altered due to minimization of the modulation schemes. On the receiving end, because Passerieux's scheme does not afford the receiver to know the original signal, the cover signal's message extraction is performed by creating a new steganographic signal. This new signal approximates the original by searching for peaks in the gain for each interval. This new signal, due to the data embedded in phases, will display periodic peaks at intervals equal to the originally chosen interval size, with amplitudes and phases proportional to the transmitted symbol. The symbols can then be extracted. This concept may be a valuable addition to the steganographic literature with regards to expected robustness and is the subject of past research by this department. This study seeks to expand upon this past research by applying this novel approach in a multi-node and multi-user configuration as well as increasing the throughput and speed. Passerieux's new steganography technique manipulates a recorder sound sample [2], [3]. The scheme records a cover signal from the environment, a new unique signal is generated and combined into the cover signal, producing the complete, transformed signal for transmission.

Ferrao explains the theory behind the Passerieux equation as follows [3]: Passerieux's algorithm is performed in the time domain on the complex baseband signal representation

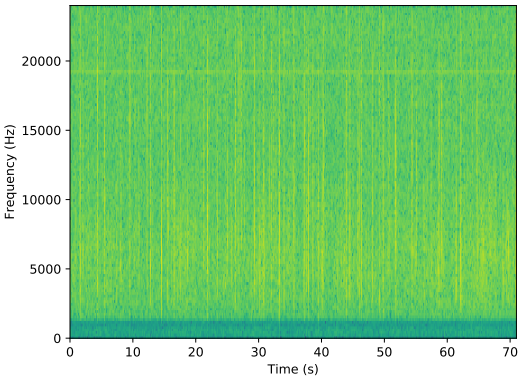
of an original signal obtained after demodulation around a chosen carrier frequency and bandwidth [2], [11]. Passerieux calculates an auxiliary signal, $\Psi_x(t)$ from a noise signal, $x(t)$. $\Psi_x(t)$ is calculated in a manner known to both the transmitter and receiver, with a series of phase terms β_p acting as the stego key. The stego signal to be transmitted, $y(t)$, can then be obtained as

$$y(t) = x(t) + \alpha \cdot a_m \cdot \Psi_x(t), \tag{2.1}$$

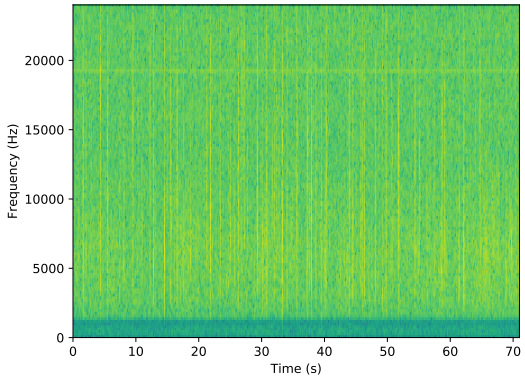
where α is a gain term acting as the relative amplitude of the auxiliary signal to the original signal and a_m is the symbol to be embedded ($\pm$ 1 in a BPSK scheme) in the m^{th} symbol period. With knowledge of the scheme, as well as the pre-shared stego key, the receiver can perform a complementary operation to estimate $\Psi_x(t)$ as $\Psi_y(t)$ and thereafter cross-correlate $\Psi_y(t)$ with the received signal in order to extract the embedded symbols.

The Ψ operator is critical to this scheme. To create the auxiliary signal, $x(t)$ is first divided into small segments of period, T, normally several hundred milliseconds, depending on the desired bitrate. Next, each period, T, is divided into $2p$ sub-intervals of decreasing and subsequently increasing lengths, indexed from $-p, \ldots, -2, -1, -1, -2, \ldots, p$. The sub-intervals are separated by guard intervals, both of whose lengths are heuristically chosen. The length of both the sub-intervals and the guard intervals are symmetric around the midpoint of the period segment. The data points in the segment are switched and then time-reversed such that data in the p^{th} sub-interval, $x_p(t)$, would then become $x'_p(t) = x_{-p}(\tau_p - t)$ when switched and time-reversed, where τ_p is the time delay between sub-interval $-p$ and p. At the time of research, start and end times will be manually synchronized so as to simplify execution of the algorithm that will allow for testing of multi-user/multi-access schemes.

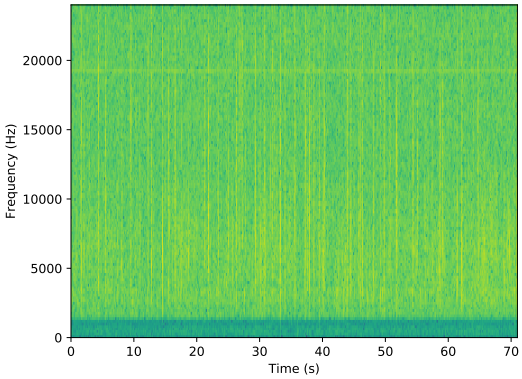
Figure 2.1 show what one can expect from a successful use of Passerieux's algorithm [3]. Figure 2.1 (a) shows the unaltered cover signal we start with. Figure 2.1 (b) is the fully transformed signal that is the cover signal embedded with our steganographic code. The gain of the new signal has an α value of 0.32. Figure 2.1 (c) has an α of 0.89. All of these spectrographs are virtually indiscernible from each other which shows that even at high gain values, we are able to achieve effective masking.



(a) Spectrum of Cover Audio



(b) Spectrum with Embedded Bits, $\alpha = 0.32$



(c) Spectrum with Embedded Bits, $\alpha = 0.89$

Figure 2.1. Spectrograph Comparison between Cover Signals and Embedded Signals

2.2 Channel Modeling

In order to model our symbols and frames across the environment, we rely on binomial distributions and Reed-Solomon forward error correction.

2.2.1 Binomial Distribution

Binomial distributions are a series of equations that model discrete events as failures or successes. In our case, we use the inverse of the bit error to model the chance that a byte, or 8 bits, is transmitted correctly - 8 out of 8 events. Our intuition shows us that we will need a low bit error rate to make it through 8 iterations in a row with no room for failure as

a single dropped bit corrupts the entire byte. Similarly, we use binomial distribution again to model that every transmitted byte in a given frame is transmitted correctly. For larger frame sizes, the need for an extremely low bit error rate is exacerbated. In Chapter 3, we review Equation 3.1 in its entirety [12].

2.2.2 Reed-Solomon Forward Error Correction

Reed-Solomon codes are a group of codes developed by I.S. Reed and G. Solomon in their 1960 paper [4]. This code scheme uses correcting bits for the purpose of correcting errors in a data block upon decoding. Essentially, they use orthogonal codes to transform a data block in such a way that it can be recovered from itself as the adjacent rows in a given block checksum each other. The extent that symbols can be corrected is a function of the total size of the data block and the total size of the transmitted block that is used up as "parity bits" [4].

In our experiment we do not implement a form of Reed-Solomon forward error correction programmatically, but we do model our symbol error rates, overhead costs, and resultant goodput analysis with the inclusion of realistic, "optimal" forward error correction.

2.2.3 SNR Selection

The Monterey-Miami Parabolic Equation model simulates the attenuation associated with spherical spreading as determined by our parameters shown in Table 4.1 and Table 4.2. This simulation continues the parametric values used in the Masked Underwater Acoustic Channel group at Naval Postgraduate School [3]. The default values for the Monterey-Miami Parabolic Equation model simulates the sound speed profile resembling Monterey Bay. This sound speed profile accounts for an expected transmission loss up to 60dB. A SNR of 60dB then, is used for the transmission signal to offset attenuation caused by spherical spreading or range in order to simulate a received SNR value of zero at the receiving node. An SNR of 40dB is used to represent a situation or environment where one could expect more noise in the environment at the receiving node. Further, one should be deliberate in their selection of SNR and what story they are trying to tell. The goal of covert communications is to pass data undetected. Our method is to hide in plain sight, but one should not take for granted that a sound will be covert just because it is natural. Natural whale sounds can be seen as high as 230dB [13]. While 230dB is a naturally occurring sound level, one must take

into account how likely it is that a whale would be present in close enough proximity to an adversary to generate 230dB. If an adversary sonar operator suddenly observed sound at that level, it may cause more harm than good as it would draw a large amount of attention to a very large sound source that is not easily explained since it does not actually exist.

2.3 Multiple Access Schemes

Channel access schemes generally fall into the following categories. FDMA, TDMA and CDMA.

2.3.1 Code Division Multiple Access (CDMA)

Code Division Multiple Access is an access scheme whereby distinct channels are assigned a "code" or a key. Mathematically, this code, a walsh code, is used to transform the data such that it can be transmitted intermittently through a channel with other orthogonal data streams without interfering with one another. Due to the orthogonal nature of the codes they can be safely transmitted and decoded into their distinct data messages with minimal interference if any.

2.4 Media Access Protocols and Applicability

ALOHA and Slotted ALOHA are access control protocols defined by users randomly transmitting whenever they have a packet to transmit. If the receiver node receives an error free packet, it responds to the sender node with an ACK. The random nature of transmission allows for collisions to take place. If two packets are sent at the same time, or one packet is sent while another packet is being processed, the second packet will be "dropped" and the receiver node will not ACK it. After a randomly determined time of not receiving an ACK, the sender node will retransmit its packet. The random retransmit time is determined independently of other nodes and reduces the possibility of repeated collisions. Slotted ALOHA is a variant that assigns blocks of time for a transmission to start. This reduces collisions by reducing the possibility for transmission to occur in the middle of another packet or node's transmit time because there are transmission "slots." ALOHA and Slotted ALOHA do not perform well in bursty traffic scenarios as there will be a high rate of transmissions and thus collisions all at the same time. Masked underwater

acoustic communications are likely to be bursty and thus make ALOHA and its variants ill-suited at first glance. Maximum achievable throughput is 18% for ALOHA and 36% for Slotted ALOHA. [14]

Carrier Sense Media Access (CSMA) attempts to reduce collisions by monitoring the broadcast channel and delaying transmission if another node is transmitting. CSMA is not suitable for underwater communication due to the fact that nodes must be able to sense each other in order for the protocol to function effectively. In an underwater environment, propagation delay is significant and can cause CSMA to not accurately detect when a channel is in use because of the slow nature of transmission and receipt. This delay compounds significantly and exacerbates the slow transmission times already present in underwater communications. CSMA does not appear to be feasible in networks with long "lines" of nodes but could be efficient in parts of the network where nodes are nebulously grouped together and able to detect one another. CSMA is not inherently efficient but it is meant to be reliable.

Multiple Access with Collision Avoidance (MACA) is promising for underwater environments due to its ability to operate independently at the receiver. Transmitting nodes send Request-to-Send (ready to send (RTS)) to the receiving node. The receiving node then sends back a Clear-to-Send (clear to send (CTS)). When the sending node receives a CTS with an appropriate message length, it sends the message. In this way, collisions are avoided before they begin. Furthermore, nodes can learn the minimum required power level for reliable transmission. By incorporating power minimization, nodes can reach a point where they do not interfere with each other, allowing for a clear communication path. Additionally, power reduction could be a concern for some transmitters in the underwater environment. Finally, the reduction of noise in the environment is a positive when one considers the inherently high noise and lossy traits of underwater communications. MACA has a higher overhead cost however and masked underwater communications are likely to be bursty and the impact of overhead should be minimal compared to the gain in throughput from collision avoidance.

2.5 Widespread CDMA Protocols

Cellular technologies that have been used in CDMA encoding are EDGE, CDMAONE, CDMA2000 and UMTS. Currently ranging from 2G to 4G these protocols are proven and

widespread in the commercial sector.

There is concern for the resolution of such channels in lossy environments. Specifically, will walsh code spreading and reformation or "de-spreading" maintain acceptable bit error rates or will the added complexity and attenuation have significant impacts in an underwater environment in relation to speed and/or fidelity. Possible solutions and future work could be put into the application of tailored walsh codes other than the standard IS-95 code that would work better in the underwater, acoustic environment. Chan et. al, discuss in their paper, "Local Decoding of Walsh Codes to Reduce CDMA Spreading Computation", techniques to reduce bit error rates [15].

CDMA2000 is attractive due to its robust forward error correction properties however at the current stage of underwater acoustic transmissions there is concern as to the usefulness of increased data rates. Additionally, the further spreading of the signal is especially unattractive due to the challenge of transmitting in the medium in general. Spreading is also not a particularly desired effect in clandestine communications due to the inherently high probability of detecting acoustic transmissions in an underwater environment. Additional testing is still worthwhile.

CHAPTER 3:
Methodology

In this Chapter we apply the concepts taken from underwater acoustic channels, Passerieux steganography, multiple user, multiple access and collision avoidance schemes. We evaluate Passerieux's method for underwater steganography in a multi-user environment by modeling single user performance in ideal conditions, then applying these upper bounds to ideal formulas and protocols in the multiple access control space. Specific implementation of Passerieux was based on previous work by Ryan Ferrao in MATLAB [3]. Modeling was performed in the Monterey-Miami Parabolic Equation. CDMA was attempted but was proven to be unsuitable in a Passerieux-based scheme. Reed-Solomon forward error correction and binomial distributions were used to analyze the effect data presented by our model and Passerieux functions. MAC protocols included were ALOHA, Slotted ALOHA, carrier sense multiple access / collision avoidance (CSMA/CA) and RTS/CTS.

3.1 Overview

Monterey-Miami Parabolic Equation

MMPE is used to model the performance of transmitting acoustic channels in an underwater environment. MMPE allows for manipulation and customization of many inputs and parameters. Specific parameters that are varied and evaluated include depth of model, range of model, depth of transmitter, total range and signal to noise ratio (SNR). Frequency and bandwidth are fixed, as evaluating the performance of this implementation of Passerieux's steganography scheme is outside the scope of this multi-user, multi-access experiment. MMPE generates a transfer function which we use later by our MATLAB implementation to model the effect of underwater transmission of our steganographic messages.

MATLAB

"Underwater Masked Carrier Acoustic Communication: Modeling and Analysis" [3] provides an implementation of Passerieux's steganographic method [2]. Passerieux's method is given a variation of inputs to include: The range between the receiver and sender, bitrate

and ratio of embedded signals in the cover channel. The MATLAB script generates a percentage of correctly received signals at a given bitrate. This generated percentage serves as the basis for our expected transmit performance such as packets and speed in the ideal case.

Reed-Solomon Forward Error Correction

Reed-Solomon forward error correction is a realistic scheme to stabilize transmission. The symbol rates allow for a realistic measure of performance while simultaneously presenting a realistic cost in overhead.

Binomial distribution

Binomial distributions are a set of mathematic equations used to model discrete events as successes and failures. In the context of this work, we are modeling the success-failure probability of the transmission of an entire frame of data.

ALOHA

As discussed in Chapter 2, ALOHA is an early implementation of a MAC scheme. ALOHA was an early iteration with a simplistic model that was prone to causing further collisions. The channel utilization, discussed below, is applied to our processed goodput.

Slotted ALOHA

Slotted ALOHA is an improvement upon the ALOHA protocol. Slotted ALOHA has a known channel utilization, this equation is applied to our generated ideal performance.

CSMA/CA

CSMA/CA is a more complex control scheme than earlier efforts such as ALOHA. Our assumptions are discussed further in Section 3.2.4. A range of Utilizations are generated based on the load and predicted delay, an ideal value is chosen to get an upper bound on CSMA/CA's channel utilization. This figure is then applied.

RTS/CTS

The 802.11 protocol is used as the specific implementation for CSMA/CA and CTS/RTS type collision avoidance protocols. The effects of CSMA/CA RTS/CTS utilization are modeled as discussed in "The Effect of Frame Length-Fragmentation and RTS-CTS Mechanism on IEEE 802.11 Mac Performance" [16]. Expected channel utilization is then applied.

3.2 Implementation

3.2.1 MMPE

Actual sea trials are outside of the scope of this research. Simple simulators such as NS-3 are not robust enough for underwater acoustic analysis. MMPE is a near accurate model to generate raw data. The MMPE source executable takes seven input files in order to generate three binaries which are further processed by two output files. The final output file is then used to generate a transfer function. The files are:

- mmpe2dbbv2_64, this file is the executable.
- pefiles.inp, this file is mandatory and contains range and depth information.
- pessp.inp, this file contains the sound speed profile data.
- pebath.inp, this file contains the bathymetry of the water/bottom interface.
- pebotprop.inp, this file contains the acoustic parameters of the medium just below the water/bottom interface.
- pedbath.inp, this file defines the deep layer bathymetry beneath the water/sediment interface.
- pedbotprop.inp, this file contains the acoustic properties of the deep layer.
- pesrc.inp, this file contains the source information.
- press.bin, this file is a generated binary containing calculation information.
- avr.bin, this file is a generated binary containing calculation information.
- avz.bin, this file is a generated binary containing calculation information.
- peout1.m, this file is generated and used for post processing.
- peout2.m, this file is generated and used for post processing.

For the experiment:

- mmpe2dbbv2_64 takes no arguments.

- pefiles.inp and pesrc.inp are the primary input files and are modified for range and SNR.
- peout2.m is used to process based on a single depth.
- The generated transfer function is the necessary output file that was used for follow on modeling in MATLAB.

Additional reading on the parameters can be found at the MMPEwebsite [17].

3.2.2 MATLAB

A singular script is used to coordinate multiple programs which implement Passerieux's embedding and extraction concepts [2]. The main inputs of the embedding operation are the cover audio for the secret message to be injected into and the period T, which controls our bitrate. We use bitrates of 2 b/s, 4 b/s and 10 b/s as the lower and upper bounds of Passerieux's method as implemented in Ferrao's research [3]. α is the ratio of encoded message to cover audio.

The extraction method largely reverses Passerieux's embedding scheme while evaluating the number of received symbols. The percent of correctly received symbols after the embedding, transfer and extracting process is used as a realistic measure of performance to be applied to MACs later in the process. The associated parameters are linked throughout evaluation.

The transfer function contains the range and SNR parameters. These were also varied to achieve a feasible bit error rate by which to evaluate our follow on MACs.

3.2.3 Follow-on Processing

An outer script runs our Passerieux script multiple times, which is then passed to another script that plots the results using a binomial distribution. We observe and evaluate the effect of multiple frame sizes for a given bit error rate on the final probability of success. An 8 byte header is added to the frame in order to model realistic overhead costs [18], [19].

Binomial probability function [12]:

$$P(X = x) = C_n^x p^x q^{n-x}, x = 0, 1, 2, ..., n. \tag{3.1}$$

A frame size is heuristically chosen to maximize overall goodput performance. The frame size is then chosen to include in Reed-Solomon forward error correction Equation 3.2. The equation is run multiple times for different parity symbol values. The resultant symbol error rate is then plotted.

Reed-Solomon forward error correction:

$$P_E \approx \frac{1}{2^m - 1} \sum_{j=t+1}^{2^m-1} j \binom{2m-1}{j} p^j (1-p)^{2^m-1-j} \tag{3.2}$$

where:
m is the number of bits, 8 in our case due to a byte [4], [20].
t = the number of correctable symbols. Note, there must be two parity symbols for every correctable symbol t.

The resultant symbol error rate is then fed through a binomial distribution reflecting the total frame and header size.

A parity symbol is then chosen heuristically to support a performance envelope over speed and distance. These values are then used in the above equations again to produce an "optimal" goodput and are plotted against distance, which again is an indicator of bit error in an acoustic underwater environment.

MAC schemes are applied to these final goodputs to show a performance ceiling based on our parameters and the MAC protocol used.

3.2.4 Media Access Control

Media access control channel utilization is computed for four separate MACs. This percentage is then applied to the calculated goodput based on our performance envelope. This approach seeks to generate useful data on the effect of MACs on underwater schemes in a simulated environment, as well as the qualitative feasibility of such schemes.

ALOHA

ALOHA's utilization is given by the following equation [14]:

$$S = Ge^{-2G} \tag{3.3}$$

where G is the load. A load of 0.5 is used to generate ALOHA's maximum theoretical efficiency of 0.184. This number is chosen to set an upper-bound.

Of note, ALOHA is a two channel protocol. Current implementations of our model do not include allowance for a second channel as acoustic environments would be crippled by multipath effects. Possible solutions to this would be to either use a completely separate base frequency such as high frequency (HF) and very low frequency (VLF) for the "control channel" or the protocol could accept the additional loss in a fire and forget type scheme such as User Datagram Protocol (UDP).

Slotted ALOHA

Slotted ALOHA is very similar to ALOHA. See Chapter 2 for the specific distinctions. For our purposes Slotted ALOHA achieves an ideal efficiency of 0.368 at a load of 1, given by the equation [14]:

$$S = Ge^{-G} \tag{3.4}$$

where G is the load. Our chosen load is 1.

Slotted ALOHA is also a two channel scheme like ALOHA. Thus the same consideration should be made as above in ALOHA.

CSMA/CA

We used the non-persistent form of CSMA/CA to calculate CSMA's efficiency. The equation used is [14]:

$$S = \frac{gTe^{-agT}}{gT(1+2a) + e^{-agt}} \tag{3.5}$$

where g is the offered load. T is maximum transmission delay and a is the normalized propagation delay.

Assumptions: a is 1, we are seeking an average bound therefore we do not account for micro deviations in path length in this model.

RTS/CTS

We choose the 802.11 implementation. RTS/CTS enabled CSMA/CA is a much more dynamic figure. We use the maximum throughput as presented in the paper "The Effect of Frame Length, Fragmentration and RTS/CTS Mechanism on IEEE 802.11 MAC Performance" [16]. RTS/CTS is determined by the following equations [21]:

$$TMT_{APP} = \frac{\beta}{\alpha + \beta} \times TMT_{802.11} \tag{3.6}$$

We assume no fragmentation. TMT refers to the maximum throughput, TMT_{APP} is the TMT of the application layer, α is the total overhead above MAC layer, β is the application datagram size and $TMT_{802.11}$ is the TMT of 802.11 MAC layer.

$$TMT_{802.11} = \frac{MSDUsize}{DelayperMSDU} \tag{3.7}$$

MSDU is the MAC Service Data Unit.

$$DelayperMSDU = (TDIFS + TSIFS + TBO + TRTS + TCTS + TACK + TDATA) \tag{3.8}$$

DIFS is the time delay for which the sender will wait after completing it's backoff, before sending the RTS package. SIFS is the time for which the receiver will wait before sending the CTS and acknowledgement package to the sender and the time the sender waits after receiving a CTS and before sending data to the receiver. TBO is the back off time. TRTS is time to send RTS. TCTS is time to send CTS. TACK is time to acknowledge. TDATA is time to send a frame of data.

Efficiency used is 77% [16].

3.3 CDMA

CDMA is attempted to achieve higher bit rates and to combat multipath attenuation. Passerieux's algorithm appears to be an inappropriate steganographic approach for CDMA. Within the embedding and extraction function described above, a pseudo-random, orthogonal code is applied to the embedded data before and after Passerieux's transforms.

The resultant code is noticeably transformed. At first a MATLAB module is used to generate an orthogonal code. Next a symbol orthogonal code of "101010. . . ." is used. Both approaches when applied to the message before embedding, or when applied after embedding, utterly distort the signal and make the alteration noticeable and obvious. Period, T is altered from 1 to 10 with the results all being severely unsuitable.

Separate cover audio files of various lengths and frequencies are used, VLF and HF bands (whale, dolphin and rain) are applied. Cover audio ranging from 30 seconds to 6 second chirps is used. The unnatural distortion is apparent by the introduction of the pseudo random code to Passerieux's algorithm. A sonar operator would likely be able to detect this signal.

3.4 Summary

In this Chapter, we provide a general overview of our methodology. The MMPE model is used with a variety of inputs to generate acoustic data. This data is then embedded and extracted according to Passerieux's algorithm. We process this data in order to generate error rates. We calculate a realistic goodput performance envelope in an underwater environment based on heuristics, probability and Reed-Solomon forward error correction. Finally we apply the throughput efficiencies of multiple MAC protocols to our goodput to generate useful data pertaining to the effect of multiple implementations of MACs on Passerieux's steganographic approach. We also present our methodology for attempting and ultimately finding CDMA to be unsuitable for Passerieux-specific steganographic algorithms. We present our results in Chapter 4.

CHAPTER 4:
Results and Analysis

In this Chapter, we present the results of our experiment followed by the results of ideal parameters. We show our expected costs and finally we show the negative results of our implementation of CDMA.

Throughout our results we focus and center our discussion around four points: distance, bitrate, and throughput, the effects of water as a medium (including depth, salinity, temperature, bottom composition, and other uncategorized environmental effects) and whether or not a trained sonar operator would be able to detect our transformed signal. Increased distance will increase attenuation, lowering our throughput and possibly the effectiveness of our communication. Bitrate and throughput will slow our communications and impact the efficacy of communications. Efficacy of communication is as derived by communicating efficiency, and by no detection of signal as inspected by an advantaged adversarial sonar operator. The effects of the environment will also increase or decrease attenuation, impacting communications. Ultimately the first three effects lead to negative effects on communication. In order to combat these effects measures would need to be taken to lower attenuation or increase throughput. These combative measures would likely increase the probability of detection by a trained sonar operator. The more likely a sonar operator is able to detect a signal and recognize it as unnatural the less effective a steganographic scheme is, and the whole treason to use this form of communication is to avoid detection.

4.1 Acoustic Model Ideal Averages

The basis for this analysis relies on a series of trials utilizing MMPE to simulate multiple permutations of channel type, symbol embedding rate, auxiliary signal gain, range, and SNR. We keep cover audio, frequency, and bandwidth static throughout the trials.

The channel model is divided into two categories: deep and shallow. Deep channel depth is set to 1500m. With the range set from 0 to 3km. The emitter depth is 500m. The post processing source is set to 500m as well. Shallow Channel depth is set to 200m. With range set from 0 to 3km. The emitter depth is 60m. The post processing source is set to 60m as

well. Symbol embedding rate, T, was set to a period of 0.5, 0.25, or 0.10 to show a range of performance for this implementation of Passerieux. Auxiliary signal gain, α, is 0.11, 0.32, or 0.89 to show key performance variations as expected by the results from Ferrao 2018 [3]. SNR is either 40dB or 60dB. A SNR of 40dB is chosen to represent a noisy transmission environment, 60dB is chosen as a value that would offset attenuation due to spreading [3]. In Section 2.2.3 we further discuss that the distinction between 60 SNR and 40 SNR is to represent two environments at the receiving node where attenuation has reduced the gain of a transmitted signal because of interfering noise and distances in the underwater medium. Specifically, we offset the expected transmission loss of the Monterey Bay as modeled by the Monterey-Miami Parabolic Equation. The cover audio is a .wav audio file of sperm whales obtained from the National Oceanic and Atmospheric Administration (NOAA). Cover audio is an uncompressed 48KHz .wav. [22]. The frequency is a 2048Hz bandwidth with a center frequency of 2500Hz.

MMPE

Parameters presented in tabular format below:

Table 4.1. MMPE Model Parameters - Deep

Input File	**Parameter**	**Values**
`pefiles.inp`	nzout, depmin[m], depmax[m]	500, 0, 2000
	nrout, rngmin[km], rngmax[km]	500, 0, 3.0
	nz, dr[km], depcalc[m], c0[m/s]	0, 0.0, 0.0, 1500.0
`pesrc.inp`	Source depth[m]	500
	Array length[m]	0.0
	D/E angle [deg]	0.0
	Center frequency [Hz]	2500
	Frequency bandwidth [Hz]	2048
	Number of frequencies	4096
`pessp.inp`	Water volume attenuation	1
	Number of sound speed profile (SSP) in first radial	1
	range[m], Number SSP in depth	0.0, 501
`pebath.inp`	Number of bathymetry points	1
	range[km] and depth[m]	0.0, 1000
`pebotprop.inp`	Number of range points	1
	range[km], sound speed[m/s], gradient[1/s], density [g/cm^3], compression attenuation[dB/m/kHz], shear speed[m/s], shear attenuation[dB/m/kHz]	0.0, 1700.0, 0.0, 1.8, 0.25 0.0, 0.0

Table 4.2. MMPE Model Parameters - Shallow

Input File	**Parameter**	**Values**
`pefiles.inp`	nzout, depmin[m], depmax[m]	500, 0, 200
	nrout, rngmin[km], rngmax[km]	500, 0, 3.0
	nz, dr[km], depcalc[m], c0[m/s]	0, 0.0, 0.0, 1500.0
`pesrc.inp`	Source depth[m]	60
	Array length[m]	0.0
	D/E angle [deg]	0.0
	Center frequency [Hz]	2500
	Frequency bandwidth [Hz]	2048
	Number of frequencies	4096
`pessp.inp`	Water volume attenuation	1
	Number of SSP in first radial	1
	range[m], Number SSP in depth	0.0, 9
`pebath.inp`	Number of bathymetry points	1
	range[km] and depth[m]	0.0, 100.0
`pebotprop.inp`	Number of range points	1
	range[km], sound speed[m/s], gradient[1/s], density [g/cm^3], compression attenuation[dB/m/kHz], shear speed[m/s], shear attenuation[dB/m/kHz]	0.0, 1700.0, 0.0, 1.8, 0.25 0.0, 0.0

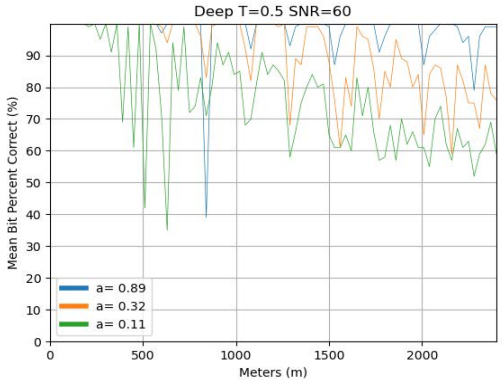
Table 4.3. Experiment Parameters

Parameter	**Values**
Model	Deep, Shallow
Symbol Period (T)	0.5s, 0.25s, 0.10s
Auxiliary Signal Gain (α)	0.11, 0.32, 0.89
SNR	40dB, 60dB
Range	200m, 500, 1000m, 1500m, 2000m

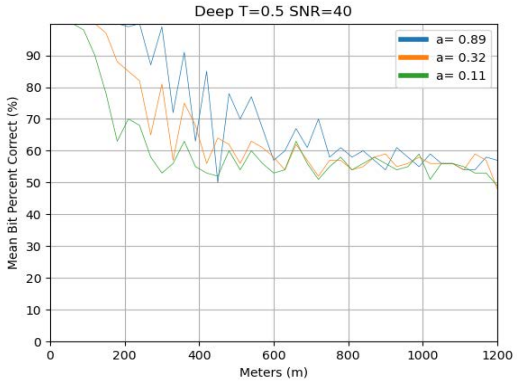
Model sub-parameters are presented in Table 4.1 and Table 4.2. The first set of parameters is deemed the "deep" model. This collection of parameters is consistent with what one would expect were they to sample an environment far from the shoreline, in"deep water" where the effects of land mass or the ocean floor is minimized and or negligible. This environment

and resultant sound speed profile is wholly distinct from a“shallow”environment which is shown in the next figure to capture the effects of far shallower water depths with a sea floor that comes into play with respect to the sound speed profile and acoustic reflections or refractions. When conducting operations one would generally expect to operate in these two broad environments, which is why we evaluate our results in both environments going forward.

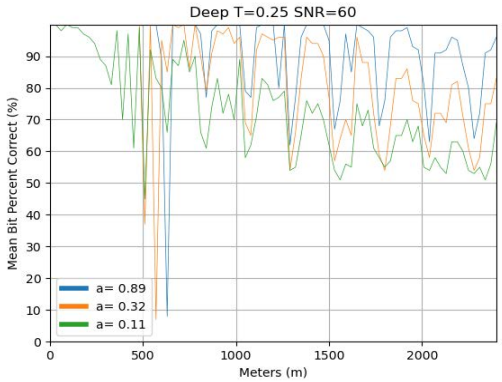
Deep Model - Simulation Results



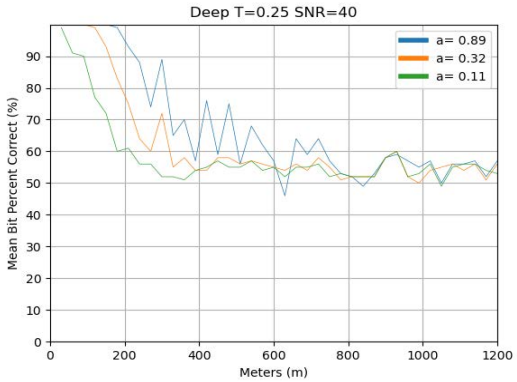
(a) Deep, T = 0.5s, SNR = 60dB



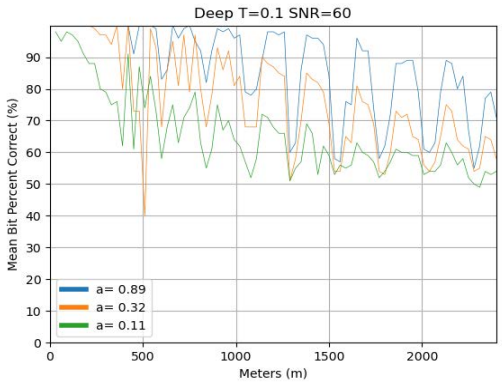
(b) Deep, T = 0.5s, SNR = 40dB



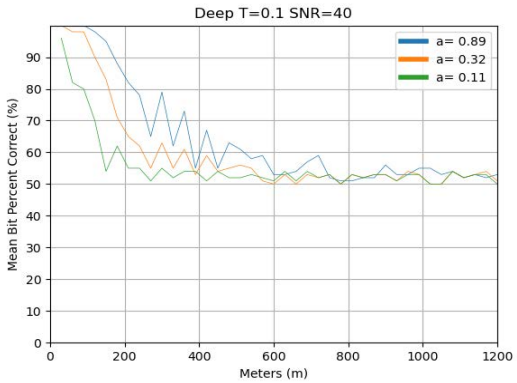
(c) Deep, T = 0.25s, SNR = 60dB



(d) Deep, T = 0.25s, SNR = 40dB



(e) Deep, T = 0.10s, SNR = 60dB



(f) Deep, T = 0.10s, SNR = 40dB

Figure 4.1. Deep Model - Ideal Values by Period, α, Range, SNR

Results are consistent with the fluctation of values. Beginning with symbol period T, The smaller value of period T, results in decreased performance. The trade-off of increasing symbol speed is outweighed by the abilility for our current implementation to send a signal through a challenging underwater environment. Regardless, there is a performance cost when extracting the final transmitted signal that will be seen when implementing higher symbol embedding rates. To rephrase, lower T values (0.10 is lower than 0.5) means that you are embedding more symbols into the same time length of message. Because you are embedding 10 symbols vice 2 (0.10 T vs. 0.5 T) the extraction method has a more difficult time correctly resolving the symbols after transmission and attenuation. α values are also as we expect, α corresponds to the amplitude of the"message"symbols we embed relative to the cover audio. The lower the amplitude, the worse the performance. As range increases, peformance decreases, this is due to attenuation through the underwater medium. As discussed in previous Chapters, the underwater environment has a more pronounced effect than air at relatively lower distances. SNR values are chosen to show performance in a noisy environment (40dB) and in a better, more ideal environment (60dB) with regards to interfering noise in the environment. The 40dB's (noisy) performance has significant adverse effects on performance.

We are using a notional cutoff rate of 95% symbol recovery rate. As we discuss later in this Section, 95% is approximately the cutoff for Solomon-Reed forward error correction to be applied at a practical time cost. We discuss in more depth the details for each set of results in the corresponding Sections below.

Figure 4.1 (a) is deep model. Its period is T = 0.5s, which is the slowest permutation of this experiment. This period represents how fast symbols are embedded and extracted into our cover signal via Passerieux's method. As discussed above, slower symbol embedding, results in less embedded message symbols over a given section of cover audio. This results in the transfer of less, useful data. The performance cost of increased symbol rates results in degradation of extraction quality and fewer symbols being correctly recovered during extraction. For the purposes of this experiment, the slower period allows for better results when compared to graphs with otherwise identical parameters. Figure 4.1 (c) and Figure 4.1 (e) are both deep channels and SNR = 60dB but with periods of 0.25s and 0.10s, respectively. The three plots within Figure 4.1 (a) represent differing α values which correspond to the amplitude of the hidden message symbol relative to the cover. The greater

the α value, the greater the likelihood that the hidden symbol will be detected and extracted correctly. Higher α values correspond to a stronger hidden symbol, therefore it follows that the plots within a graph with higher α vales would have a higher percentages of symbol recovery. It stands to reason that an experienced sonar operator would have a higher chance of detecting a modified signal as α increases, future work would need to test acceptable rates of α. Distance is the greatest indicator of negative performance. The greater the distance between source and destination the worse the symbol recovery performance. This negative effect due to distance is expected as signal attenuation continues to occur the farther a signal travels. High α values are able to mostly overcome attenuation and maintain high symbol resolution at this combination of distance, period and SNR for the deep channel MMPE model. This results in the transmitted signal carrying a higher embedded data amplitude, possibly resulting in a higher probability of detection.

Figure 4.1 (b) is deep model. Its period is T = 0.5s, which is the slowest permutation of this experiment. As opposed to Figure 4.1 (a), Figure 4.1 (b), uses a SNR of 40dB which is much lower than the 60dB SNR we use elsewhere in the experiment. In the experiment 40Hz represents a realistic,"noisy", underwater, acoustic environment. We show the performance disparity between a more ideal environment (60dB) and a less ideal environment (40dB) where there is a lot of noise interfering with our ability to detect and process our acoustic signal. This additional noise is due to a number of possible sources such as ships in close proximity, oil or mine operations, a large collection of biological organisms or some combination of all. The added noise in the environment makes it difficult to interpret our transmitted acoustic signal. As a result the signal is received with a lower degree of fidelity which in turn negatively affects our ability to extract the transmitted message. It is difficult to extract a symbol based on mathematical transformations when the input signal, the received cover message, has been corrupted by attenuation and noise. The lower SNR, 40dB, represents a scenario where the noise present in the environment has a significant impact and our received signal has been negatively impacted accordingly. When comparing the performance of Figure 4.1 (a) with Figure 4.1 (b) you can see that there are similar trends based on distance and alpha values, indeed these trends hold throughout the experiment. The lowered SNR value however causes distance to quickly and severely impact the successful transmission rate until its steady state of 50%. A steady state of 50% represents a truely random chance of deciphering if the bit is a 0 or 1 in our binary

phase shift key Passerieux transformation algorithm. As discussed earlier the α plots are consistent in what we expect however they converge at a distance of approximately 750m. The change in SNR for these sets of simulations shows that attenuation has a catastrpohic effect on symbol recovery and greatly reduces the range as compared to Figure 4.1 (a). This observation, however is made irrespective of the ability to bridge the gap using different form factors. For example, a possible solution would be to place a series of communicating nodes that would communicate in hops.

Figure 4.1 (c) is similar to Figure 4.1 (a) however its period is 0.25s as opposed to Figure 4.1 (a) whose period is 0.5s. The overall performance is worse than Figure 4.1 (a) but it follows similar trends. The performance is expected and demonstrably worse than Figure 4.1 (a) because the change in period value represents faster embedding and extraction. Faster, more frequent embedding and extraction leaves less margin for attenuation error. More information in the same window reduces performance across a lossy environment such as ours. The reduction in performance is enough to significantly affect our plots, which generally, follow the trends in Figure 4.1 (a). Notably, the α = 0.89 high value plot is siginificantly degraded. In Figure 4.1 (a) the high α value plot is minimally affected by distance for our model, but at lower α values it is not able to overcome the attenuation. Performance for all three α plots does not converge for our distance window but performance for α = 0.89 and 0.32 is much lower.

Figure 4.1 (d) is very similar to Figure 4.1 (b). Like Figure 4.1 (c), Figure 4.1 (d) has a period of 0.25s and an overall lower performance. The lowered performance results in the three plots reaching their poor symbol recovery steady state at 400m and 800m for α = 0.32 and 0.89, respectively. The α = 0.89 plot appears to enter its ~50% steady state at approximately the same time as the α = 0.89 plot in Figure 4.1 (b) but this is possibly due to external factors of the simulation itself as the general symbol recovery rate for Figure 4.1 (d) is lower than Figure 4.1 (b).

Figure 4.1 (e) is similar to Figure 4.1 (a) and Figure 4.1 (c), it differs in its period value which is 0.10 seconds. Figure 4.1 (e) trends similarly to Figure 4.1 (a) and Figure 4.1 (c) but once again, its symbol recovery performance is a step below Figure 4.1 (c) which itself is a step below Figure 4.1 (a). Figure 4.1 (e) is the first of the SNR 60dB deep channel experiments that appears to reach a steady state of 50%. The α = 0.11 plot appears to hit

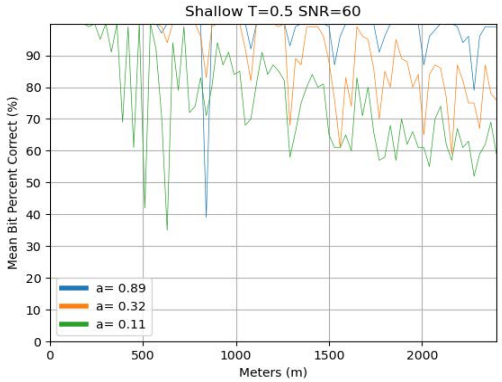
that low 50% benchmark at the edge of our distance window of 2000m. Plot α = 0.89 consistently peaks below a 95% recovery rate after 1000m.

Figure 4.1 (f), like Figure 4.1 (e) is similar to its SNR 40dB predecessors. Figure 4.1 (f) has a period of T = 0.10s and worse overall performance than Figure 4.1 (d) or Figure 4.1 (b). Its steady state happens even sooner than Figure 4.1 (d) but again, it stops at approximately 50%.

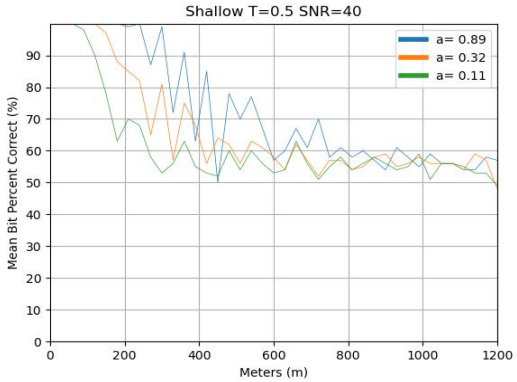
For the deep channel simulation, 60dB SNR is generally a strong enough parameter to keep the symbol recovery rate from reaching a steady state of 50% at up to 2000m. However, symbol recovery rates varied with distance wildly depending on the α value. The 40dB SNR graphs are much worse. The maximum distance at which high recovery rates are achieved is 200m. As shown later in the thesis, rates below 95% prove to be catastrophic for transmitting packets with reliability. Figure 4.1 (a) where α = 0.89, is able to intermittently sustain high recovery rates across the total 2000m window. The same plot is less consistent but is still able to continuously peak in Figure 4.1 (c). The α = 0.89 plot is high in Figure 4.1 (e) out to 1000m before intermittently peaking out to 1500m. The α = 0.32 plot is strong out to 1000m and finally consistently fell below ~95% around the 1500m mark. Figure 4.1 (a) is higher and more consistent than Figure 4.1 (c). Figure 4.1 (e) is the most affected for this α = 0.32 value, experiencing valleys at the 500m mark and dropping below 95% at 800m.

If possible, emphasis should be placed on improving SNR via increasing the power of the transmitted signal or by reducing environment noise so as to increase symbol resolution effective distance. Greater α values, steganographic symbol noise amplitudes, are the next most important factor for symbol recovery distance in deep channels, in some cases improving performance by over 1000m. Lower periods also help symbol recovery rates marginally, which can actually be quite significant in cases where the degradation of the performance curve is gentle. In SNR = 60dB cases, the attentuation is gradual enough that period rates are the difference in 500m to 1000m of consistent transmission performance, but in the SNR = 40dB simulation, the attenuation is so strong that the affect of period, while noticeable, only added 100m of addtional distance, if at all.

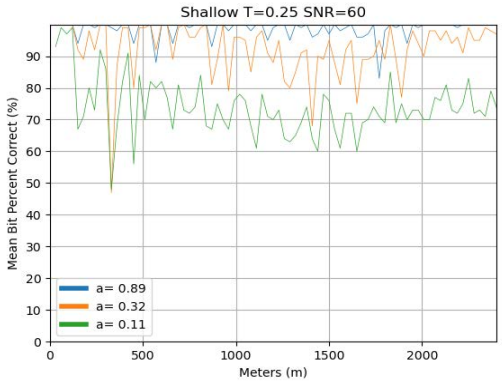
Shallow Model - Simulation Results



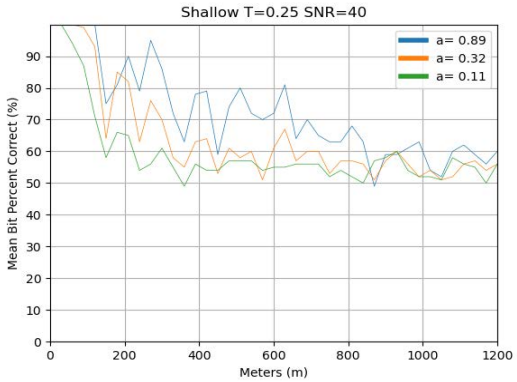
(a) Shallow, T = 0.5s, SNR = 60dB



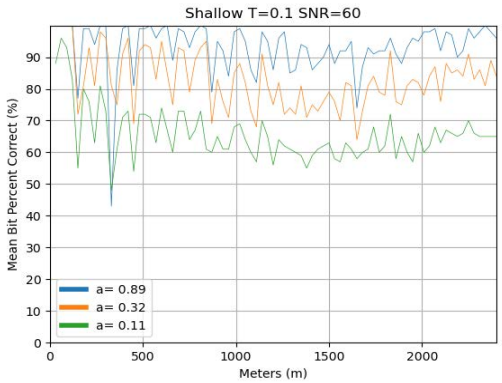
(b) Shallow, T = 0.5s, SNR = 40dB



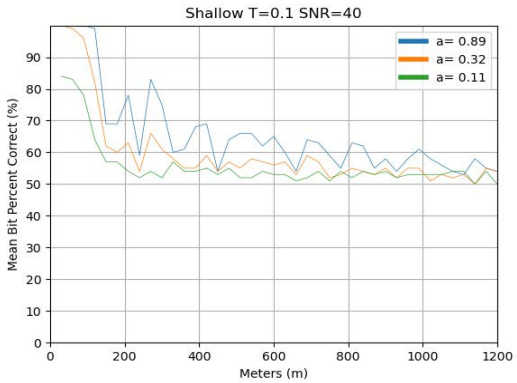
(c) Shallow, T = 0.25s, SNR = 60dB



(d) Shallow, T = 0.25s, SNR = 40dB



(e) Shallow, T = 0.10s, SNR = 60dB



(f) Shallow, T = 0.10s, SNR = 40dB

Figure 4.2. Shallow Model - Ideal Values by Period, α, Range, SNR

The above shallow model graphs are arranged in a manner similar to the deep model channel graphs. Figure 4.2 (a) is shallow model. The period is 0.5 seconds which is the smallest of the period values used. Figure 4.2 (a) generally performs better than the other period values as shown in Figure 4.2 (c) and Figure 4.2 (e). Figure 4.2 (a) has a SNR of 60dB as opposed to Figure 4.2 (b), Figure 4.2 (d), and Figure 4.2 (f), which have a SNR of 40dB. Figure 4.2 (b) has identical parameters to Figure 4.2 (a) other than the SNR. Figure 4.2 (b) has a SNR of 40dB. The overall performance of Figure 4.2 (a) compared to Figure 4.2 (b) is much better, with only one of the α values reaching a low steady state around 55% accurate symbol recovery. Within Figure 4.2 (a), the three plots corresponded to three α values. These are the same values in the above deep model graphs. The α value = 0.11 plot performs much lower than 0.89 or 0.32. All three α values have valleys that dip below the 95% threshold but the α = 0.89 plot maintains somewhat consistent performance above that with the 0.32 plot falling below reliability past approximately 1300 meters. This trend between α values is consistent across all graphs including the deep model simulation.

Figure 4.2 (b) is once again a shallow model graph, however the only parameter difference between it and Figure 4.2 (a) is the SNR of 40dB. The reduced signal strength is represented by a noisier environment and reduced SNR, results in lower performance and a much steeper decline in said performance as distance is increased between the transmitting and receiving sources. The α = 0.32 and 0.11 plots reach a low steady state around 500 meters, much sooner than Figure 4.2 (a). α = 0.89 reaches a low steady state at approximately 700 meters. This a very significant decrease in performance; however, the greater concern is that the rapid decline in performance results in accurate symbol resolution only out to 100 to 300 meters, which can be unuseable in certain applications. Beyond the effect on performance as determined by distance, the relationship between the other parameters is consistent with what is seen in prior graphs and the deep model.

Figure 4.2 (c) differs from Figure 4.2 (a) by using a period of T = 0.25s. The first half of the graph, 0 - 1000 meters is what we expect, lower performance. The second half however is not what we expect. The performance seems to increase rather than continue a downward trend. Shallow bodies of water tend to be more prone to interference due to the presence of human and aquatic interference. The ocean floor also comes into play at shallow depths and cause unknown effects in the propagation of sound. It is likely that there is some unknown presence in the model that causes superior performance for these parameters at that depth

and distance. Rather this is likely somewhat of a unique occurence combined with natural performance fluctation. A repeat of the overall experiment using a completely different model or even a real world test would likely show continued downward performance as distance increases.

Figure 4.2 (d) uses a period of T = 0.25s, like Figure 4.2 (c). 4.2 (d) uses a SNR of 40dB like Figure 4.2 (b) and Figure 4.2 (f). Results are as expected and consistent with other graphs, including those in the deep model simulation. The α = 0.32 and 0.11 plots achieve a low steady state around 350 meters, with the 0.89 value reaching steady state around 900 meters. The steady state of the α = 0.89 plot is achieved at a greater distance than the α = 0.89 plot of graph (b) and thus better, but this can be explained due to variance, we do not believe that the performance for period T = 0.25 seconds performs better than Figure 4.2 (b). All three α values dip below 95% performance before 100 meters which is a very, very short distance for some underwater applications.

Figure 4.2 (e), is similar to Figure 4.2 (c), but with a lower overall performance. Of note, The α = 0.89 plot generally hovers around 90% symbol resolution after 1000 meters. That symbol resolution is not practical for applying protocols that guarantee transmission. All three plots appear to trend upwards around 2000 meters. This again is unusual and not to be expected in all environments over additional distances.

Figure 4.2 (f) has markedly lower performance than other similar graphs, but it is possible that the exact distances would have variance. The high plot α = 0.89 averages 60% or below around 400m, well before the comparable Figure 4.2 (d). The low α value, α = 0.11 never achieves a symbol resolution above 95%. Again, those two deviances could be due to variance, but a decline in performance is expected with these parameters (SNR = 40dB, period T = 0.10s) when compared to the other graphs.

The shallow model results differ slightly than those in the deep model simulation. The shallow simulations that use a SNR of 60dB generally perform better than the deep model. Additionally, results appear more stable over longer distances. The deep model shows a clear negative relationship with performance and distance, where as the shallow model is much more gradual and even appears to perform better near the end, likely due to variance. The SNR = 40dB graphs are very similar to the deep channel experiments. It appears that the distortion and attenuation present in a 40dB environment outpaces any significant

differences between the deep and shallow models.

Ideal Frame Size

The below graphs show the goodput vs. bit error performance of multiple frame sizes between 5B and 255B. Results are taken for both deep and shallow channel models. Each graph represents a different combination of SNR and α for a given channel model at period T = 0.5s.

Larger frame sizes perform better when calculating goodput vs. bit error. Based on the performance we see here we choose a frame size of 256B + 8B header for a total of 264Bto use in our follow on calculations presented in Section 4.1 Ideal Parity Symbol Value and Section 4.1 Goodput vs. Distance.

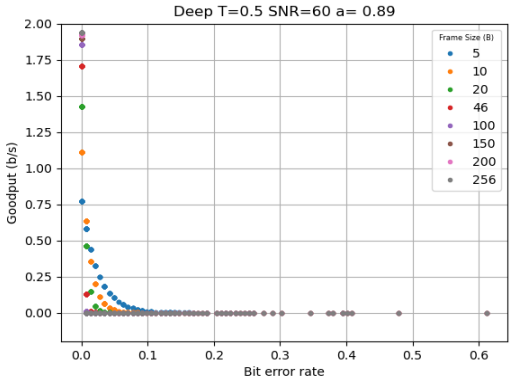
Figure 4.3 (a), Figure 4.3 (c), and Figure 4.3 (e) are very similar and are presented as one in this discussion. These graphs all use a SNR of 60dB which is much higher than the 40dB values we use for the other graphs. As discussed previously, high symbol recovery rates (95%+) are required for practical forward error correction. A symbol recovery of 95% is achievable at relatively low distances when comparing 40dB SNR to 60dB SNR. The bit error along the x-axis refers to the simulation results section. At this stage, the goodput is largely the calculation of the frame size and the header. Therefore it follows that lower frame sizes have more stable goodput performance. That is, at high bit error rates, a frame failure is less likey to happen in smaller frame sizes. To over simplify: A frame of 5, has 5 chances to fail because a frame requires every packet to be sent correctly in a row in this simple example. A 256 size frame has 256 chances to fail. Therefore, once again, lower frame sizes peform better than higher frame sizes at higher bit error rates. Conversely, large frame sizes have a higher maximum goodput because the percentage of overhead packets being sent is lower than in low frame sizes. In a 5 packet frame, there is still an 8B header, therefore 5/13 or 38% of the data is useful data. In a 256 packet frame with an 8B header, 256/264 97% of the data is useful. These tradeoffs are shown nicely in Figure 4.3 and Figure 4.4. Frame sizes 5, 10 and 20 show low but non-zero performance at or above ~5% bit error. The 46 frame shows low performance slightly above 1% bit error. At the maximum goodput side, the top of the y-axis, frames 100 - 256 are largely grouped together around 1.9 b/s. Our scheme is maximized at 2.0 b/s for BPSK. Attenuation is a significant factor in our environment and accepting some bit error will provide signifcant gains in

effective distance. Distance is the greatest indicator of higher bit error and consequently, lower bitrate. The larger frame sizes are very steep and an all-or-nothing goodput is not very practical in a scheme such as ours that requires bit error rates below 3% to be useful. The smaller frame sizes are much more effective at higher bit error rates but we find the tradeoff in performance to be too low. At best, the goodputs of the small frame sizes are less than half or less than a third of the maximum goodput, 2.0 b/s. Additionally the goodput we see at higher bit error rates is sub .5 b/s and .25 b/s. These goodput rates when looked at on their own are very poor for practical communcation purposes which is why we do not value them as much when weighing our ideal frame size.

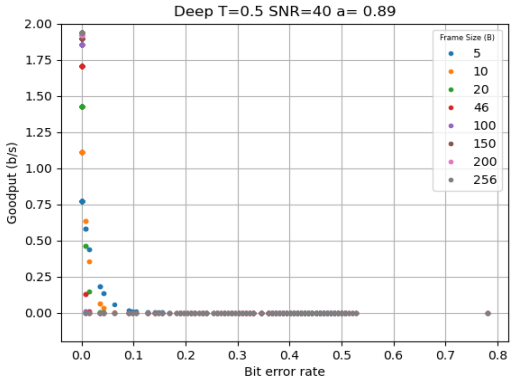
For the SNR = 40dB graphs, Figure 4.3 (b), Figure 4.3 (d) and Figure 4.3 (e). The general trends hold true. Frame sizes 5, 10 and 20 have some level of performance with some bit error albiet at low goodput. Frame sizes 100 through 256 are clumped with very similar goodput near the theoretical maximum. Frame size = 46 continues to be a tradeoff with reduced, but still relatively high goodput and some performance at low bit error levels. This value marks the turning point but is still not high enough considering the constant drop in goodput at the high end of the goodput spectrum. The dropoff in goodput performance is much less gradual for the shallow channel simulation Figure 4.4. This is due to the previous graphs showing a sharp decline in symbol resolution with increasing distance as compared to the deep model Figure 4.3. There are fewer points that are below a certain bit error and thus have catastrophically low goodputs. The fewer points results in these graphs being far more sporadic in their plots.

The big takeaways from Figure 4.4 shallow model, largely follow the deep model discussion of ideal frame size. The performance measured in goodput at an SNR of 60dB and 40dB, sharply declines as a result of bit error, which is in itself a result of range-based attenuation. There is a a relatively gradual or uniform increase in attenuation and bit error with increasing distance. This increased bit error however, results in exponentional decrease in performance due to the requirement to transmit an entire frame of packets (between 13 B and 264 B) in all-or-nothing manner. The result is then that bit errors can cause the goodput to be reduced to almost zero between ~0 and 0.1% bit errors. A rather rapid decline.

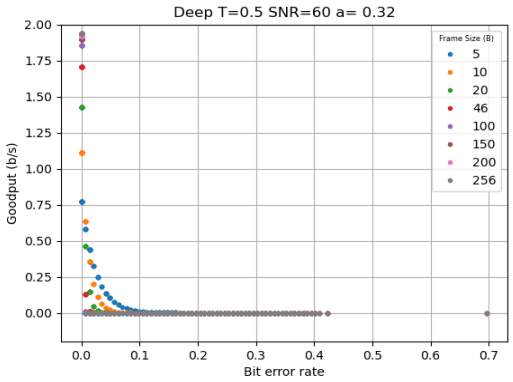
Deep Model Period T = 0.50 sec



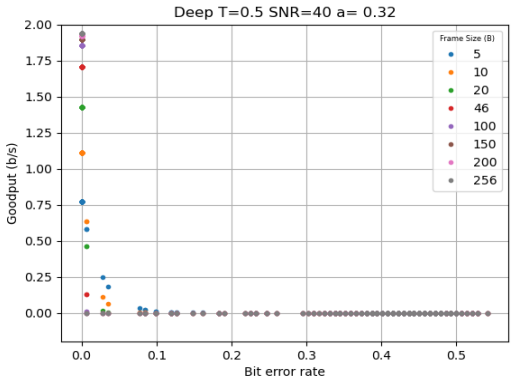
(a) $\alpha = 0.89$, SNR = 60dB



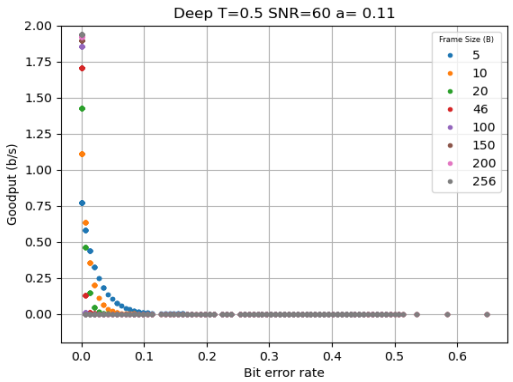
(b) $\alpha = 0.89$, SNR = 40dB



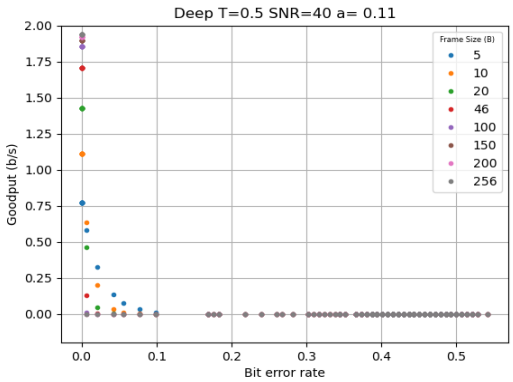
(c) $\alpha = 0.32$, SNR = 60dB



(d) $\alpha = 0.32$, SNR = 40dB



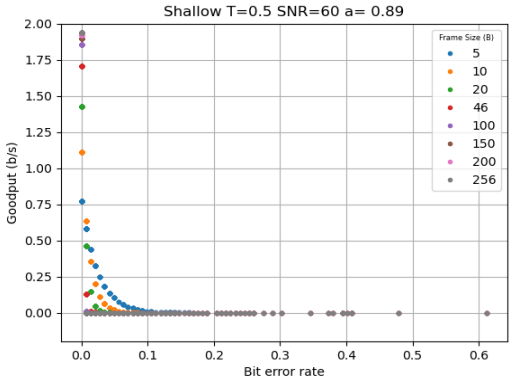
(e) $\alpha = 0.11$, SNR = 60dB



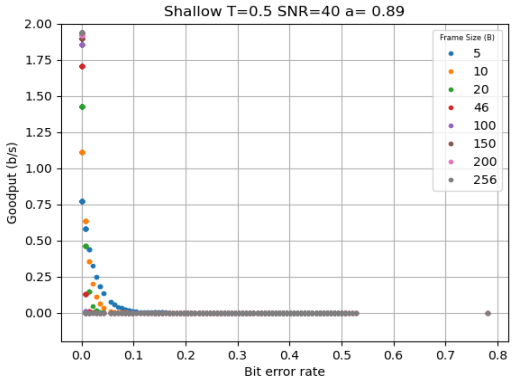
(f) $\alpha = 0.11$, SNR = 40dB

Figure 4.3. Deep Model Goodput vs. Bit Error - Frame Sizes

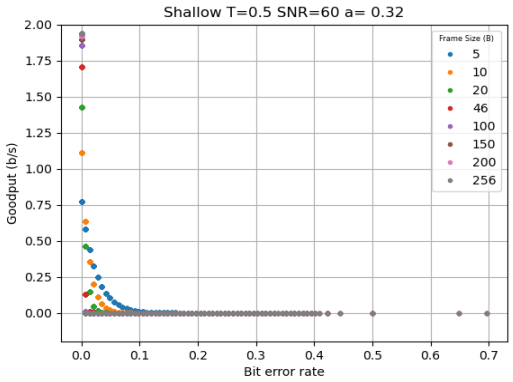
Shallow Model Period T = 0.50 sec



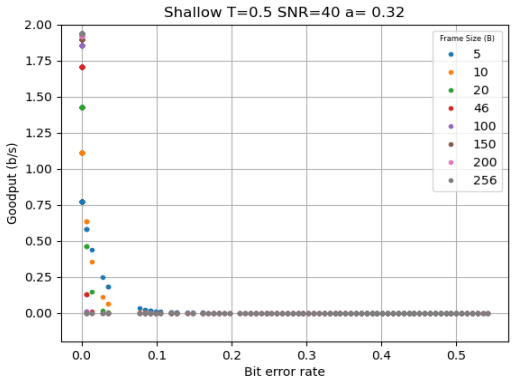
(a) $\alpha = 0.89$, SNR = 60dB



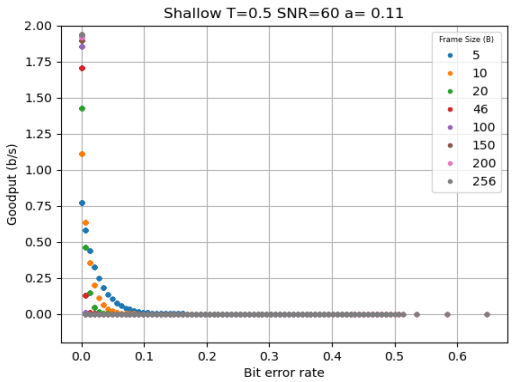
(b) $\alpha = 0.89$, SNR = 40dB



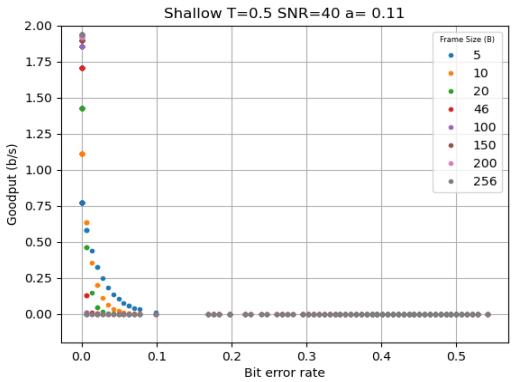
(c) $\alpha = 0.32$, SNR = 60dB



(d) $\alpha = 0.32$, SNR = 40dB



(e) $\alpha = 0.11$, SNR = 60dB



(f) $\alpha = 0.11$, SNR = 40dB

Figure 4.4. Shallow Model Goodput vs. Bit Error - Frame Sizes

Ideal Parity Symbol Value

The below graphs, Figure 4.5, and Figure 4.6, show the goodput vs. bit error performance for multiple Reed-Solomon parity symbol values: 2 to 170 symbols. Results are taken for both deep and shallow channel models. Each graph represents a different combination of SNR and α for a given channel model at period T = 0.5s.

Larger parity symbol values result in more, high goodput values. This is to be expected as the additional parity symbols allow for greater corrections to take place. More corrections result in greater success and throughput at lower bit error values. The more corrections, the more attenuation that can be overcome. On the other end of the spectrum, lower parity symbol values result in higher goodput. Each parity symbol takes the place of useful data. When you transmit more parity symbols, you transmit less useful data in a given period, decreasing the goodput. By transmitting less parity symbols you are able to transmit more data during a given transmission or time frame, resulting in higher goodput.

For our given frame size, 256B frame + 8B header, 170 symbols is the maximum amount of parity symbols that can be included. The maximum is only able to correct bit errors out to approximately ~96%. The lower parity symbol values do not achieve marked improvement over one another. Their goodput is very similar and their bit error correction is also extremely low. When choosing an“optimal”value, three breakpoints stand out - maximum, minimum, and 64 parity symbols out of 264 frame and header. Selecting the maximum value allows for the greatest degree of correction, bit error values, and transmit distance due to distance being perhaps the greatest source of attenuation and bit error in an underwater acoustic environment. Next, the minimum parity symbol value, while offering the least flexibility in bit error, offers the highest goodput and is ideal for those whose environments preclude considerations outside of speed. The final breakpoint and the value we choose is 64 parity symbols out of a 264 symbol frame. 64 offers the highest speed while still allowing for some bit error fluctations. This helps to insulate against occurrences where bit error dips above 1%.

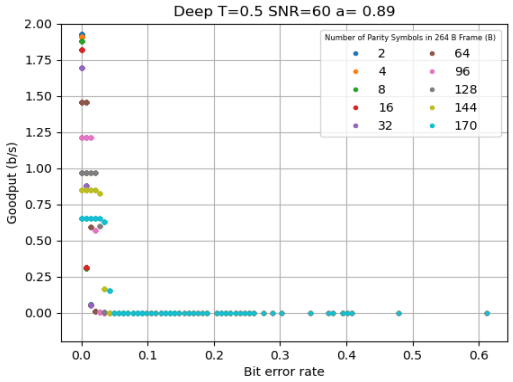
Analysis is performed to look at the effect of smaller parity symbol values on distance. On average, distance is reduced by ~30% when comparing 64 parity symbols to 2 parity symbols. Distance is highly valued in the application of masked underwater acoustic communications.

Starting with the deep channel experiment, once again our graphs are split into two categories: SNR = 60dB and 40dB. Each SNR category has three graphs which represent α values of 0.89, 0.32, and 0.11. For the SNR = 60dB figures, Figure 4.5 (a), Figure 4.5 (c), and Figure 4.5 (e), we see a tight grouping of 2 through 16 parity symbols, losing very little of their maximum goodput. The maximum goodput associated with 32 parity symbols is below the maximum goodput of 2 parity symbols through 16 parity symbols, but the 32 parity symbol maximum goodput is still relatively high. The first four plots, associated with 2 through 16 parity symbols, have a very steep dropoff. In all three graphs, only 16 has a data point beyond nearly zero bit error and that data point is still only slightly above 0.25 b/s goodput. The maximum goodput associated with 32 parity symbols is better than the previous maximums associated with 2 through 16 parity symbols. The maximum goodput of 32 parity symbols is approximately 1.7 b/s, the next data point is approximately 0.8 b/s. The plots of 2 parity symbols through 32 parity symbols, reach a steady state of nearly zero goodput past 0.02 bit error. Starting with 64 parity symbols we see correction rates and thus maximum goodput beyond ~0 bit error. Plots associated with 64 - 170 parity symbols have increasingly steady maximum goodput out to ~0.01 through ~0.04 bit error, respectively. Each of the larger parity symbol values also has significant decreasing levels of goodput as the parity symbols used for correction use the available frame space for transmitting data. The maximum goodput of 170 parity symbols hovers below 0.7 b/s goodput, well below the values for 2 through 64 parity symbols.

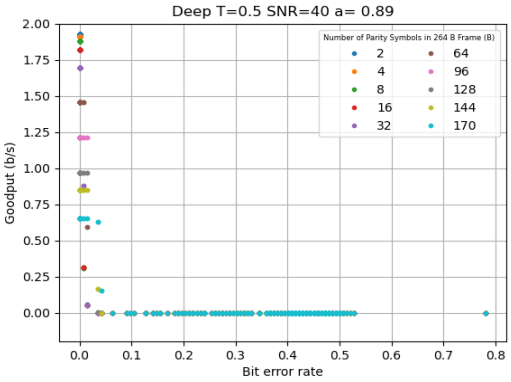
The SNR = 40dB graphs Figure 4.5 (b), Figure 4.5 (d), and Figure 4.5 (e) follow very closely with what we saw from the SNR = 60dB graphs in the preceding paragraph. There are two differences. The first is that the degree of performance is lesser from the 40dB graphs. Where the SNR = 60dB parity bits were able to correct out to ~0.04, these SNR = 40dB graphs cluster around 0.01 for the 96 through 170 parity values. There are additional points out to ~0.03 and ~0.04 but there is a large gap reflecting the lack of low bit error points in general from the 40dB experiment. The 40dB SNR rate represents an environment with a lot of noise and as a result, there are fewer high quality points and they are relatively sporadic compared to what we see from 60dB. The second deviation, is that the high bit error, low goodput points we do see are significantly below the 60dB graphs. The 40dB graphs consistently see bit error data points that are much higher on the x-axis. For practical purposes, this is a moot point as the goodput for all these points is close to zero which is

completely unusable for our applications. This is consistent and expected from what we saw from the series of graphs presented so far. We choose 64 parity symbols as the value for follow on sections.

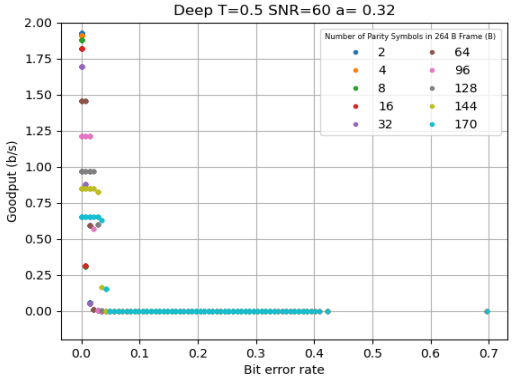
Deep Model Period T = 0.50 sec



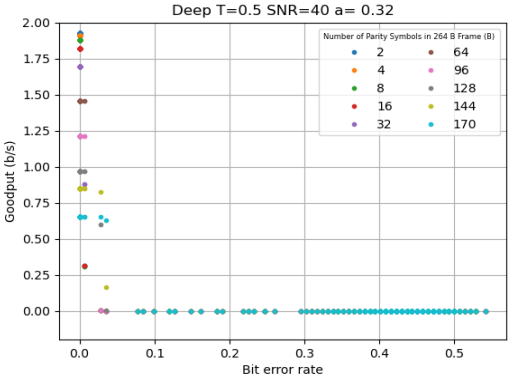
(a) $\alpha = 0.89$, SNR = 60dB



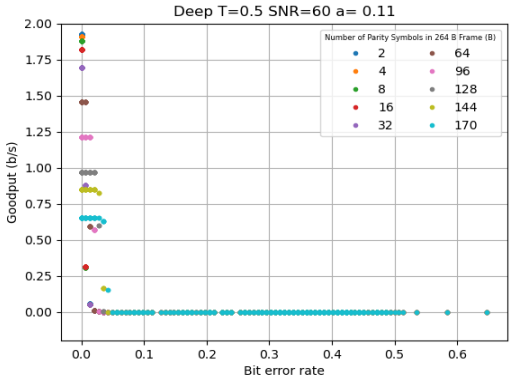
(b) $\alpha = 0.89$, SNR = 40dB



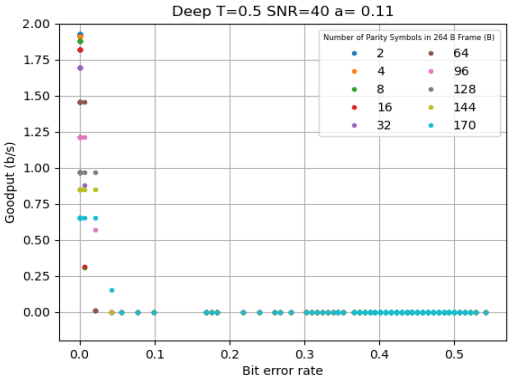
(c) $\alpha = 0.32$, SNR = 60dB



(d) $\alpha = 0.32$, SNR = 40dB



(e) $\alpha = 0.11$, SNR = 60dB

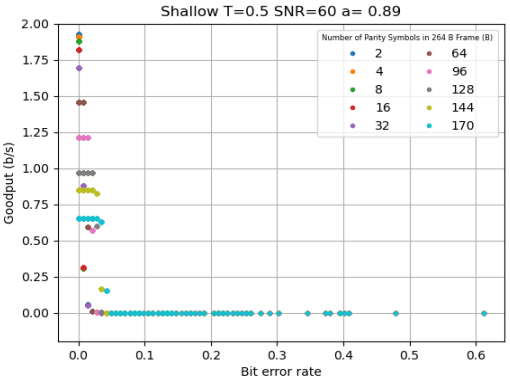


(f) $\alpha = 0.11$, SNR = 40dB

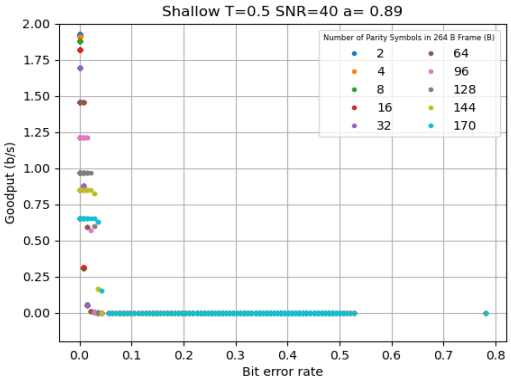
Figure 4.5. Deep Model Goodput vs. Bit Error - Parity Symbol Value

The Figure 4.5 deep model and Figure 4.6 shallow model results are nearly identical. The 60dB SNR in particular differs only in a point or two on each graph (Figure 4.6). The similarity in the graphs of Figure 4.6 is likely due to the strong SNR and again, the catastrophic effect of the environment. These two factors push our results towards a more pass/fail, binary representation. For sufficiently low bit error rates, less than approximately 0.04, the correction of Reed-Solomon allows for near maximum performance. For higher bit error rates, approximately 0.04 and above, goodput will sharply decline to nearly zero. As a result, the deep and shallow model results for this portion of the experiment are more binary in their results. The SNR = 40dB graphs Figure 4.6 (b), Figure 4.6 (d), and Figure 4.6 (f) differ from their deep model counterparts Figure 4.5 (b), Figure 4.5 (d), and Figure 4.5 (f) more so than the 60dB SNR graphs Figure 4.6 (a), Figure 4.6 (c), and Figure 4.6 (e). The 40dB plots are largely the same as the 60dB plots but the higher parity bit values are able to maintain a high goodput over a larger range of bit errors. The fact that the SNR=40dB shallow model plots have more non-zero goodput data points compared to the deep model 40dB plots indicates that the deep model does not have as many data points available in that bit error band as the shallow model. The deep model is more gradual, it linearly increases through the bit error data set and again, would have graphed in a sharply declining fashion. If we were to extrapolate the graphs data points we would expect the frame transmission would show up as full goodput out to 0.04 bit error rate, then nearly 0 goodput for bit error rates greater than 0.04. The shallow model is more chaotic and has more peaks at greater distances and is able to capture those additional bit error ranges.

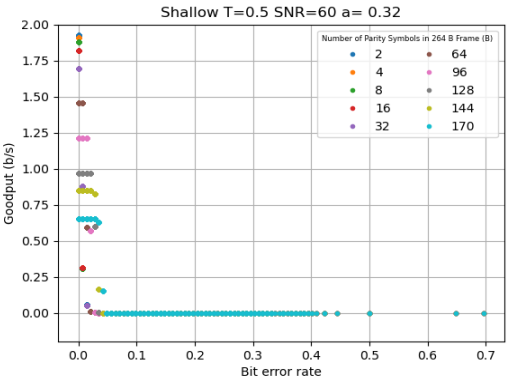
Shallow Model Period T = 0.50 sec



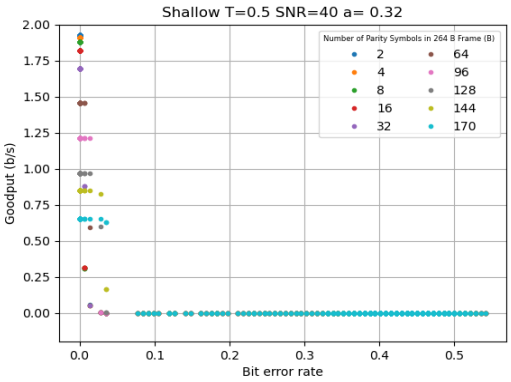
(a) $\alpha = 0.89$, SNR = 60dB



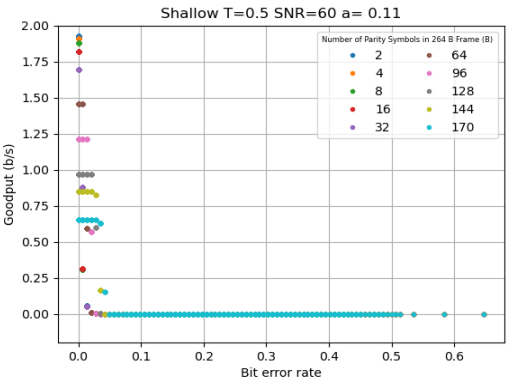
(b) $\alpha = 0.89$, SNR = 40dB



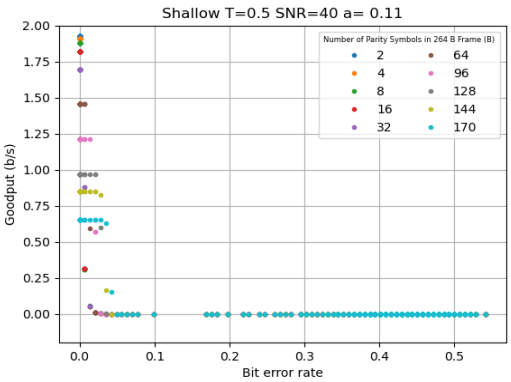
(c) $\alpha = 0.32$, SNR = 60dB



(d) $\alpha = 0.32$, SNR = 40dB



(e) $\alpha = 0.11$, SNR = 60dB



(f) $\alpha = 0.11$, SNR = 40dB

Figure 4.6. Shallow Model Goodput vs. Bit Error - Parity Symbol Value

Goodput vs. Distance

The culmination of our analysis is a plot of goodput vs. distance with multiple curves representing the theoretical maximums of different commonly used MAC schemes at our chosen SNRs of 60dB and 40dB.

When calculating the Reed-Solomon symbol error rates and binomial total transmission success rates we use a frame size and number of parity symbols that we heuristically choose from the previous two plots. Frame = 264B and parity symbol value = 64B.

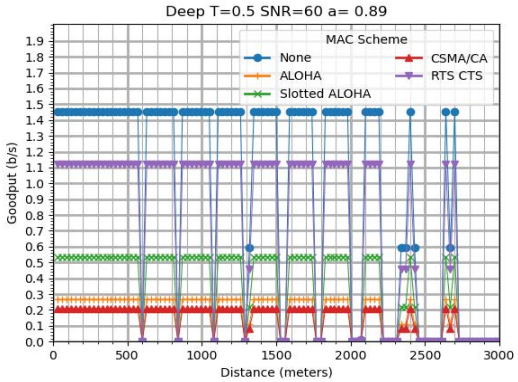
Distance is the biggest factor affecting bit error rate at our SNR. As such, Figure 4.7 and Figure 4.8 show an expected relationship between increasing distance and decreasing performance. Goodput appears to be a polarizing performance metric. Goodput will nearly instantaneously decrease from its full value to nearly zero once bit error rate crosses below a threshold. When bit error is below a certain threshold, of around ~3%, Reed-Solomon correction is able to stabilize our implementation's goodput to its near maximum. For greater bit error rates, the failure caused by the need to transmit an entire frame plummets the goodput. For a frame size of 264, we are counting on a process repeating 264 times and not expecting a single error. This is why, the goodput is so sensitive to our bit error. Frame size could be reduced in order to stabilize the graceful reduction in goodput however the tradeoff in goodput as shown in Figure 4.3 and Figure 4.4 is not valuable to the overall performance from a speed and distance perspective. Decreased frame sizes result in lower goodput as shown in Figure 4.3 and Figure 4.4.

The below graphs represent combinations of SNR and α for a given channel model.

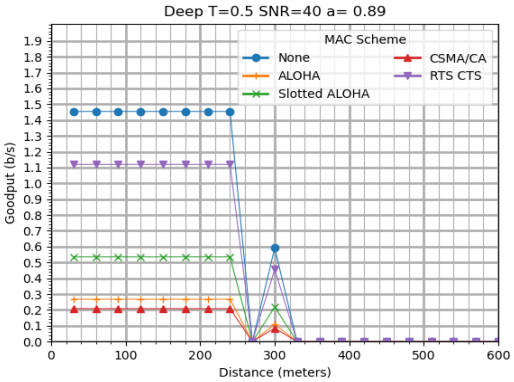
The following section refers to Figure 4.7 Deep Model. Figure 4.7 (a), as expected, is the best performing combination of parameters. It has high goodput out to 2000 meters, spiking past 2500 meters. At approximately 1 nautical mile, the performance of Figure 4.7 (a) is feasible for some underwater operations. Figure 4.7 (c) has high goodput out to almost 1500 meters which is still a good distance. Figure 4.7 (e) suffers the most at only going out to 500 meters which is still useful in some military operations during limited tasks. Likewise, replicating our forward error correction requirements and results as shown in Figure 4.7 (b) is not useful in a wide range of operations due to its maximum, simulated distance of 300 meters. The forward error correction requirements of Figure 4.7 (d) and Figure 4.7 (f) cause the effective goodputs to hover around 100 meters and are essentially unusable for the many

operations. All of these distances relative to each other are expected based on what we have seen from the α values and SNR. The individual plots for all of the graphs in Figure 4.7 represent the expected theoretical maximum for common MAC schemes – RTS/CTS. Slotted ALOHA, ALOHA, CSMA/CA. All of the schemes impose a cost, therefore not applying a MAC (none) is predictably, the highest goodput rate. RTS/CTS is by far the MAC with the highest goodput, 1.1 b/s, and though it is 77% of the rate, it is still only half of the 2.0 b/s rate we originally started with before applying forward error correction. A goodput of 1 b/s is a very low transmission speed however it is still useable and considering that we applied real world forward error correction and MAC it is encouraging that we are still able to achieve such a rate. Again, this is a very low rate but not an automatic disqualifier for acoustic environments. Slotted Aloha is approximately half of RTS/CTS at slightly above 0.5 b/s. This rate is likely impractical but for reliable communications with multiple users, it is again encouraging as a last resort. ALOHA and CSMA/CS are another step below Slotted ALOHA and should be considered unusable, even including the mitigating factors of protocol and environment.

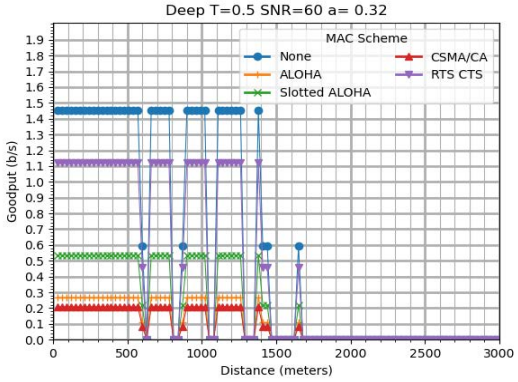
Deep Model Period T = 0.50 sec



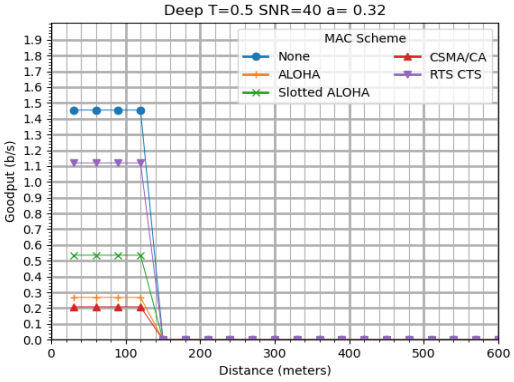
(a) $\alpha = 0.89$, SNR = 60dB



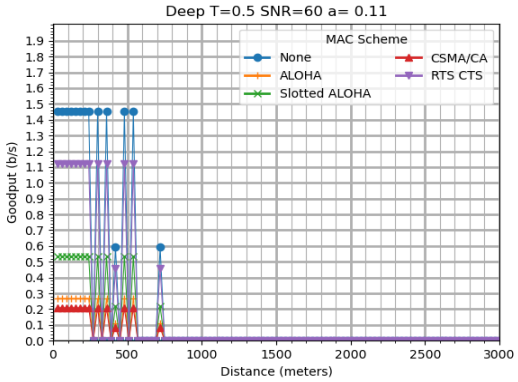
(b) $\alpha = 0.89$, SNR = 40dB



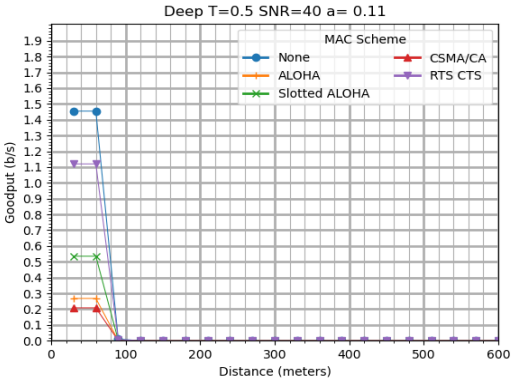
(c) $\alpha = 0.32$, SNR = 60dB



(d) $\alpha = 0.32$, SNR = 40dB



(e) $\alpha = 0.11$, SNR = 60dB

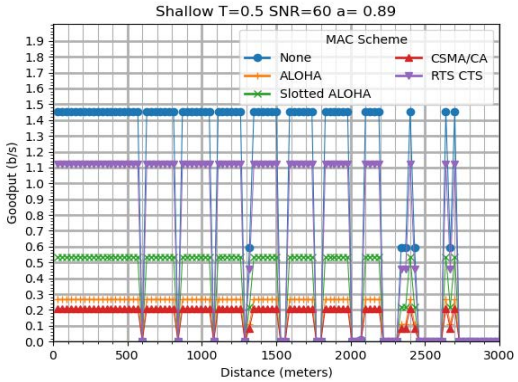


(f) $\alpha = 0.11$, SNR = 40dB

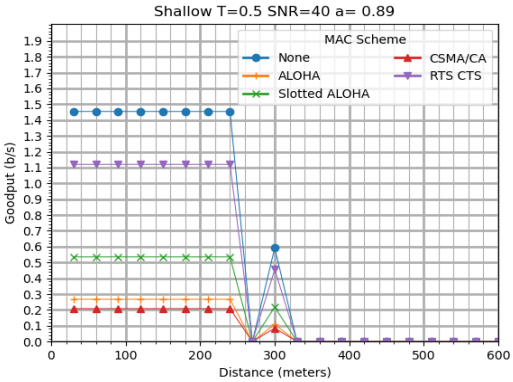
Figure 4.7. Deep Model Goodput vs. Distance - MAC

The shallow model graphs, Figure 4.8, are identical to the deep model graphs, Figure 4.7. This similarity is not expected, however this is due to the smoothing that occurs as a result of Solomon-Reed forward error correction and once again, the destructive nature of the underwater acoustic environment on goodput. As seen repeatedly throughout the experiment, a low bit error rate is required for a successful goodput. This goodput then, is near all-or-nothing with little variation. The differences in the model add more points with varying levels of bit error which do not show up or rather, are flattened to a near-zero goodput. Additional future research could use a different simulation altogether or sea trials to gain additional performance data but there appears to be a clear and effective, positive impact of Reed-Solomon forward error correction to stabilize goodput based on bit error within a 3% bit error rate performance envelope out to a given distance. The distance is determined by such parameters as SNR as well as the α encoding used in our implementation of Passerieux's method.

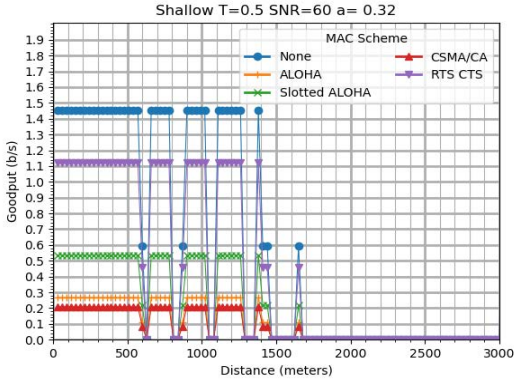
Shallow Model Period T = 0.50 sec



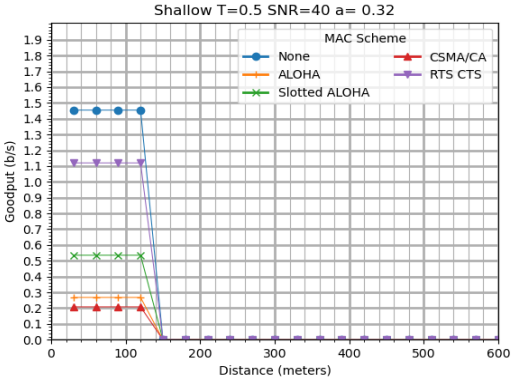
(a) α = 0.89, SNR = 60dB



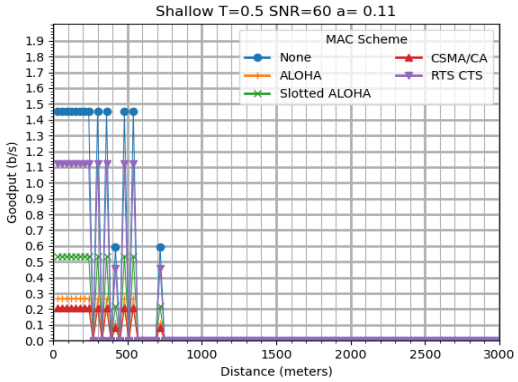
(b) α = 0.89, SNR = 40dB



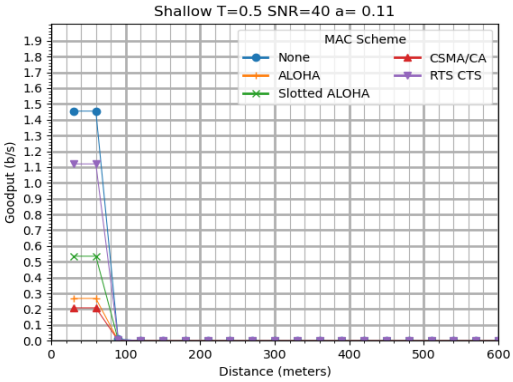
(c) α = 0.32, SNR = 60dB



(d) α = 0.32, SNR = 40dB



(e) α = 0.11, SNR = 60dB



(f) α = 0.11, SNR = 40dB

Figure 4.8. Shallow Model Goodput vs. Distance - MAC

The multiple MAC values are a theoretical throughput maximum based on channel utilization and the specific environment we choose to model with the Monterey-Miami Parabolic Equation at an SNR of 60dB or 40dB. The further reduction in throughput and goodput ranges from significant to severe. RTS/CTS, while still significant, shows a qualitative feasiblity using our current model. Slotted ALOHA also has a severe impact on performance, however depending upon the application it appears to remian within the realm of possible. CSMA/CA and standard ALOHA severely degrade the channel to essentially unuseable levels for general purposes. One expects to pay a relative price when operating MAC schemes, however the objective results for two of the lower schemes appear to be too much, while the better performing schemes are promising.

4.2 MAC utilization

In Figure 4.7 and Figure 4.8 we show the transformation of the goodput if a MAC scheme were to be added. The following represents an upper-bound on the performance. Real world implementations will be slower than those presented here.

In Chapter 3 we show the formula for computing maximum theoretical channel utilization.

ALOHA's utilization is given by the equation [14]:

$$S = Ge^{-2G}S_{max} = 0.184 \tag{4.1}$$

Equation 3.3

Slotted ALOHA achieves an ideal efficiency of 0.368 at a load of 1, given by the equation [14]:

$$S = Ge^{-G}S_{max} = 0.368 \tag{4.2}$$

Equation 3.4

We use the non-persistent form of CSMA/CA to calculate CSMA's efficiency. The equation used is [14], [23]:

$$S = \frac{gTe^{-agT}}{gT(1+2a)+e^{-agt}}S_{max} = 0.143 \tag{4.3}$$

Equation 3.5

RTS/CTS is determined by the following equations [21]:

$$TMT_{APP} = \frac{\beta}{\alpha + \beta} \times TMT_{802.11} \tag{4.4}$$

[21]

We assume no fragmentation. TMT refers to the maximum throughput, TMT_{APP} is the TMT of the application layer, α is the total overhead above MAC layer, β is the application datagram size and $TMT_{802.11}$ is the TMT of 802.11 MAC layer.

$$TMT_{802.11} = \frac{MSDUsize}{DelayperMSDU} \tag{4.5}$$

MSDU is the MAC Service Data Unit.

$$DelayperMSDU = (TDIFS + TSIFS + TBO + TRTS + TCTS + TACK + TDATA) \tag{4.6}$$

SIFS is the time for which the receiver will wait before sending the CTS and acknowledgement package to the sender and the time the sender waits after receiving a CTS and before sending data to the receiver. TBO is the back off time. TRTS is time to send RTS. TCTS is time to send CTS. TACK is time to acknowledge.

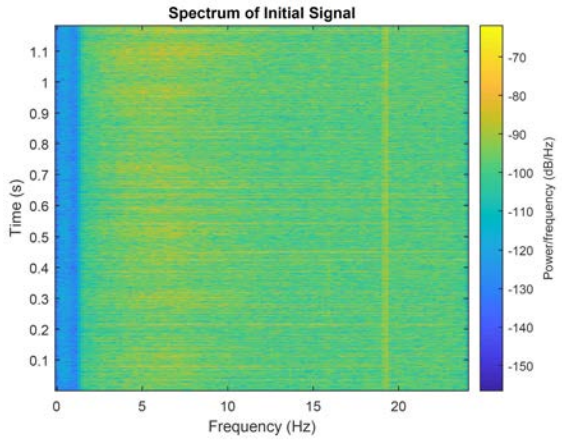
S_{max} = 77% [16].

4.3 CDMA

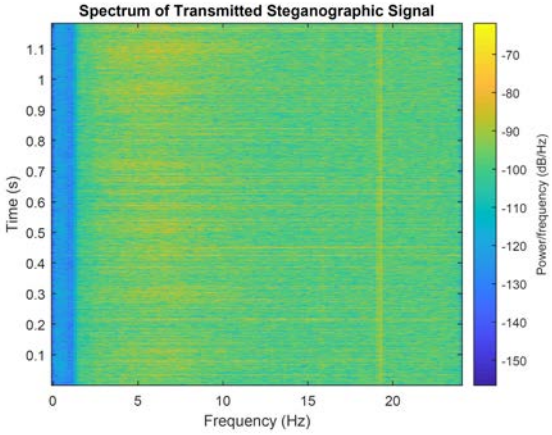
4.3.1 Spectrogram and Constellation

The spectrogram in Figure 4.9 reveals the obvious distortion caused by the introduction of the Walsh code. The Walsh code is simplified to the most basic orthogonal code“10101010”and still the distortion is apparent. The Walsh code is added to the message before it is embedded within the cover audio. Adding the code post embedding would undoubtedly cause further distortion and was not attempted as it would defeat the purpose of covert communication.

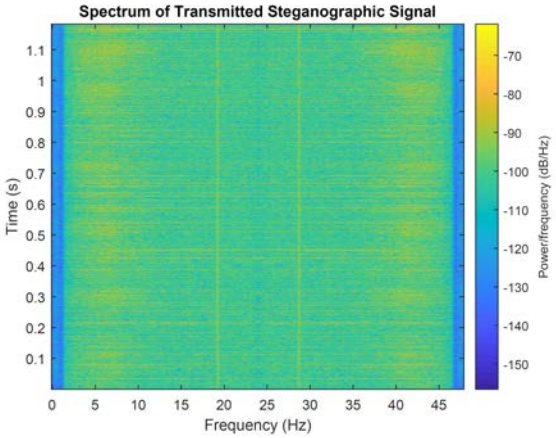
Figure 4.9 (a) is our initial cover signal, the whale sound as viewed in the spectrum. Figure 4.9 (b) is that same cover signal following the passerieux process of embedding it with bits from our steganographic code. Figure 4.9 (a) and Figure 4.9 (b) are identical to the human eye and the human ear, as one would expect of a successful hidden message. Figure 4.9 (c) however, is the addition of a Walsh style orthogonal code. The implementation of CDMA would expect to multiplex multiple sources via an orthogonal code then embed them. Figure 4.9 (c) is different than Figure 4.9 (a) or Figure 4.9 (b). Additionally it shows a heavy polar bias, likely due to the introduction of "1s" and "0s" in orthogonal codes. This clear, man made distortion is obvious at a cursory glance let alone to a trained acoustic analyst that a military operation would be attempting to deceive and defeat. CDMA implementations do not seem possible when used with this implementation of Passerieux's steganographic method.



(a) Spectrum of Cover Audio



(b) Spectrum with Embedded Bits



(c) Spectrum with Walsh Orthogonal Code

Figure 4.9. Spectrogram Distortion

4.4 Summary

Chapter 4 consists of three general parts. At the beginning of Section 4.1, we show the results of our model and establish the parameters by which we conduct analysis. Overall the shallow model performs slightly better than the deep model but they are very similar. The two largest effects on performance are SNR and α values. The 60dB SNR parameter consistently and significantly outperforms the 40dB value. Larger α values also consistently and significantly outperform smaller values. Performance is based on symbol resolution which translates directly to effective distance. Later in Section 4.1, we show a performance envelope for goodput vs. distance or bit error. We calculate our goodput based on heuristic

methods for applying Reed-Solomon forward error correction, frame and header values as well as for different variables in our model and in Passerieux's method. We use a 264B frame size to maximize the goodput and to mitigate the effect that a fixed header size of 8B would impose on goodput. We choose 64 parity symbols as that value maximizes goodput while offering some forward error correction resiliency due to the added parity symbols. We see consistent throughput out to ~2000m, ~1300m, and ~500m using 60dB SNR and α values of 0.89, 0.32, and 0.11, respectively. We see consistent throughput out to ~240m, ~120m, and ~60m using 40dB SNR and α values of 0.89, 0.32, and 0.11, respectively. During Section 4.1 we apply MAC schemes to show an expected ceiling for the goodput one can expect when operating in our environment. We see ~1.4 b/s for unaltered goodput, ~1.1 b/s for RTS/CTS, ~0.5 b/s for Slotted ALOHA, ~0.28 b/s for ALOHA, and ~0.2 b/s for CSMA. Finally, in Section 4.3 this experiment seeks to apply CDMA and found it unsuitable for Passerieux covert communications. The distortion caused by applying an orthogonal code is too apparent for use in a stealthy scenario. In Chapter 5, we summarize the research that took place and outline future research avenues.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Conclusions and Future Work

Underwater acoustic communications operate in a very challenging environment. This experiment and analysis operates using a model and not the real world where there will undoubtedly be additional challenges and introduced chaos.

5.1 Conclusions

We are able to show a performance envelope for expected goodput using a multitude of factors and model variables. At an SNR of 60dB and 40dB using the Monterey-Miami Parabolic Equation, consistent transmission and recovery is observed in both deep and shallow model experiments out to 2000 meters with spikes at out to 2500 meters. Reed-Solomon forward error correction is effective. The cost is reducing the goodput to ~72% of the total goodput 1.44 b/s. After forward error correction we see an unaltered goodput of 1.44 b/s. We then model best case scenario speed costs when implementing some common MAC schemes. The best case goodputs we see after applying forward error correction and MAC schemes to Passerieux's implementation of acoustic communication are ~1.1 b/s for RTS/CTS, ~0.5 b/s for Slotted ALOHA, ~0.28 b/s for ALOHA, and ~0.2 b/s for CSMA. Data rates continue to be objectively slow but are promising considering military applications operate with vastly stripped down data requirements when compared to civilian applications. CDMA as a means to increase overall data transmitted does not appear to be a viable method using this implementation of Passerieux. Covert communications using Passerieux's method in a local operation appears viable as of this analysis. Additional work must be done to continue to take advantage of the parameters and insights that were achieved in this experiment.

5.2 Future Work

5.2.1 Protocol Development

The analysis conducted here will be valuable in crafting a protocol to take advantage of data field sizes and header sizes in order to achieve an intended goodput. Further, the same

information can help to set expectations and tailor outcomes based on the distance and operating environment when constructing the protocol. Lower layer protocols leave room for improvement in the space. Protocols that are effective over the air would need to be improved, altered or disregarded in masked underwater acoustic communications as applied to Passerieux's method.

5.2.2 Sea Trials

Additional at-sea trials is the next logical step to confirm discrepancies between our presented theoretical analysis and the real world. Testing would also be valuable in constructing performance profiles for specfic geographic areas and conditions.

5.2.3 Additional SNR Selections

A simulation or real world experiment utilizing greater SNR would be a good next step. Specifically we recommend SNR of 150dB to 180dB. SNR of 150dB to 180dB represent realistic ranges for whales. This is another possible organic ocean cover sound and would likely result in greater transmission ranges as the increased source levels would reach a receiving node at an acceptable dB level after distance-based attenuation. Care should be taken to account for the increased likelihood of cover detection and possible counter-detection by an adversary sonar operator due to the increased source noise level.

5.2.4 Cover Sound Selection

In Section 2.2.3 SNR Selection, we discuss our chosen SNRs of 60dB and 40dB. One can observe natural whale sounds as high as 230dB [13]. As discussed in Chapter 2, this sound level is not practical in covert communications as it is likely to attract more attention despite being a naturally occurring sound. There could be some niche scenarios or operations where an extremely large dB could be easily explained.

Finally, this analysis does not address power directly, however the discrepancies between the results of SNR values provides an opportunity for future applications to manage SNR by increasing or decreasing power as desired and required by a chosen performance envelope in a real world at-sea context.

List of References

[1] M. Shinego, G. Edelson, F. Menas, M. Richman, R. Nation, and E. Will, "Underwater acoustic data communications for autonomous platform command, control and communications," BAE Systems, Nashua, NH, Tech. Rep. N00014-99-1-0208, feb 2001.

[2] J. M. Passerieux, "Stealth underwater acoustic communications based upon steganography techniques," in *2nd International Conference and Exhibition on Underwater Acoustics*, 2014.

[3] R. Ferrao, "Underwarer masked carrier acoustic communication: Modeling and alaysis," M.S. thesis, Naval Postgraduate School, Computer Science Department, Monterey, California, 2018.

[4] S. Reed, "Polynomial codes over certain finite fields," pp. 300–304, 1960. Available: https://faculty.math.illinois.edu/~duursma/CT/RS-1960.pdf

[5] H. Dol, B. Quesson, and F. Benders, "Covert underwater communication with marine mammal sounds," *Undersea Defence Technology-UDT Europe 2008, 10-12 June 2008, Glasgow, UK*, 2008.

[6] University of Rhode Island and Inner Space Center, "What are common underwater sounds," 2020. Available: https://dosits.org/science/sounds-in-the-sea/what-are-common-underwater-sounds/

[7] P. Zakarauskas, "Ambient noise in shallow water: A survey of the unclassified literature," 1986. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a167696.pdf

[8] E. Harland, S. Jones, and T. Clarke, "Sea 6 technical report: Underwater ambient noise," 2005. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/197303/SEA6_Noise_QinetiQ.pdf

[9] M. Amorim, R. Vasconcelos, M. Bolgan, S. Pedroso, and P. Fonseca, "Acoustic communication in marine shallow waters: Testing the acoustic adaptive hypothesis in sand gobies," 2018. Available: https://jeb.biologists.org/content/221/22/jeb183681

[10] S. Liu, G. Qiao, and A. Ismail, "Covert underwater acoustic communication using dolphin sounds," *The Journal of the Acoustical Society of America*, vol. 133, no. 4, pp. EL300–EL306, 2013.

[11] J. M. Passerieux, “Method and system for acoustic communication,” France Patent 2017/0 149 522 A1, May 25, 2017.

[12] S. Verlag, “Binomial distribution,” New York, NY, pp. 44–45, 2008. Available: https://doi.org/10.1007/978-0-387-32833-1_34

[13] O. Alliance, “Powerful sound sources in the ocean: Sperm whales and military sonars,” 2021. Available: https://whale.org/powerful-sound-sources-ocean-sperm-whales-military-sonars/

[14] Cheung, “Summary: Analysis of the carrier sense multiple access (csma) scheme,” 2019. Available: www.mathcs.emory.edu/~cheung/Courses/558/Syllabus/00/CSMA/summary.html

[15] A. Chan, P. I. R. Madyastha, and D. Karger, “Local decoding of walsh codes to reduce cdma despreading computation,” 2005. Available: https://www.wirelessinnovation.org/assets/Proceedings/2005/2005-sdr05-2-1-01-chan.pdf

[16] A. Sweedy, A. Semeia, S. Y. Sayed, and A. H. Konber, “The effect of frame length-fragmentation and rts-cts mechanism on ieee 802.11 mac performance,” March 2015.

[17] K. Smith. Monterey-Miami Parabolic Equation. [Online]. Available: https://oalib-acoustics.org/PE/MMPE/mmpeintro.html

[18] B. Petrioli and S. Petroccia, “Multiplexing data and control channels in random access underwater networks,” 2009. Available: https://ece.northeastern.edu/fac-ece/basagni/papers/BasagniPPS09.pdf?fbclid=IwAR2Fugi2Ly7ll216FKH7IekKLFxKHhfSPf4hQKHfe7Stwq4ITS0PgDSbNJA

[19] P. Basagni and S. Petroccia, “Optimized packet size selection in underwater wireless sensor network communications,” pp. 321–337, 2012. Available: https://ece.northeastern.edu/fac-ece/basagni/papers/BasagniPPS12.pdf?fbclid=IwAR0zXg2l-kz-VpKTlURWE3NmQsgtQHnQg5rvc_baWLHRrNcSEfcYOk-OSgI

[20] Sonar and Mudholkar, “Analytical study of reed-solomon error probability,” pp. 297–304, 2016. Available: https://www.ripublication.com/ijes16/ijesv8n2_15.pdf?fbclid=IwAR0qLN0euh9Ce2KvwRs7QBMJBpjnB8cnLgc28q2G3dvZdTGB4Gg_v-t3t2sf

[21] Jangeun Jun, P. Peddabachagari, and M. Sichitiu, “Theoretical maximum throughput of ieee 802.11 and its applications,” in *Second IEEE International Symposium on Network Computing and Applications, 2003. NCA 2003*, April 2003, pp. 249–256.

[22] NOAA, “Cetacean sounds,” 2014. Available: https://swfsc.noaa.gov/textblock.aspx?Division=PRD&ParentMenuId=148&id=5776

[23] Icai, “Throughput analysis,” 2019. Available: http://bbcr.uwaterloo.ca/~lcai/ece418/5-2.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California