NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A NOISE-MASKING PHYSICAL LAYER SECURITY METHOD FOR MULTIPLE-INPUT, MULTIPLE-OUTPUT DIGITAL COMMUNICATION SYSTEMS

by

Robert C. Sellin

March 2018

Thesis Advisor:	Frank Kragh
Second Reader:	Ric Romero

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2018	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE
A NOISE-MASKING PHYSICAL LAYER SECURITY METHOD FOR MULTIPLE-INPUT, MULTIPLE-OUTPUT DIGITAL COMMUNICATION SYSTEMS

5. FUNDING NUMBERS

6. AUTHOR(S) Robert C. Sellin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

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

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

In this thesis, we develop a method of using a noise-masking system to increase the security in a multiple-input, multiple-output communication system by using known channel-state information to calculate a specific masking signal for each block of a space-time block-coded signal. This masking signal is invisible to the intended receiver since it is designed to cancel out within the equalization process. Using mathematical analysis and numerical simulation of the communication system, we find that it is possible to design an effective security system by employing this method. Finally, we extend this insight to a communication system involving wavelet packet modulation and find that this masking method can be adjusted to this more complicated system.

14. SUBJECT TERMS
noise masking, wavelet packet modulation, WPM, multiple-input multiple-output, MIMO, Alamouti space-time block code, STBC, channel state information, CSI

15. NUMBER OF PAGES 63

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.

A NOISE-MASKING PHYSICAL LAYER SECURITY METHOD FOR MULTIPLE-INPUT, MULTIPLE-OUTPUT DIGITAL COMMUNICATION SYSTEMS

Robert C. Sellin
Lieutenant Commander, United States Navy
B.S., University of Kentucky, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2018

Approved by: Frank Kragh
Thesis Advisor

Ric Romero
Second Reader

R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this thesis, we develop a method of using a noise-masking system to increase the security in a multiple-input, multiple-output communication system by using known channel-state information to calculate a specific masking signal for each block of a space-time block-coded signal. This masking signal is invisible to the intended receiver since it is designed to cancel out within the equalization process. Using mathematical analysis and numerical simulation of the communication system, we find that it is possible to design an effective security system by employing this method. Finally, we extend this insight to a communication system involving wavelet packet modulation and find that this masking method can be adjusted to this more complicated system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. OBJECTIVE 1
- B. MOTIVATION 1
- C. THESIS CHAPTER BREAKDOWN 2

II. BACKGROUND 3
- A. WIRELESS CHANNEL 3
  - 1. Channel Simulation 3
  - 2. Channel Estimation 4
- B. NOISE MASKING 4
- C. MULTIPLE-INPUT, MULTIPLE-OUTPUT (MIMO) 7
  - 1. Time Diversity 7
  - 2. Spatial Diversity 7
  - 3. Alamouti Space-Time Block Coding 7
- D. WAVELET PACKET MODULATION 9
  - 1. Fourier Transform (FT) 10
  - 2. Discrete Fourier Transform (DFT) 10
  - 3. Discrete Wavelet Transform (DWT) 10
  - 4. Application 11

III. METHOD 13
- A. TERMINOLOGY 13
  - 1. Masking Vector 13
  - 2. Channel State Vector 13
  - 3. Intended Receiver 14
  - 4. Eavesdropper 14
- B. CALCULATION 16
  - 1. Mask Effect 16
  - 2. Signal Power and Mask Power 19
  - 3. Additional Constraints 19
  - 4. Mask Vector Calculation 20

IV. RESULTS 23
- A. SIMULATION 23
  - 1. Signal Generation 24
  - 2. Channel 24
  - 3. Alamouti Coding 24

4. Mask Addition 25
5. Receiver 25
6. Equalization 26
7. Decision 26
8. Demodulation 27
9. Error Analysis 27
10. Results 27
B. SUMMARY 30

V. APPLICATION TO WPM 31
A. WPM AND STBC ORDER 31
B. EQUALIZATION 32
C. MASK CALCULATION 33
D. RESULTS 35

VI. CONCLUSIONS AND RECOMMENDATIONS 37
A. OBJECTIVES 37
B. CHALLENGES AND FURTHER RESEARCH OPPORTUNITIES 38
1. Channel-State Information (CSI) Methods 38
2. Optimization of Mask Calculator 38
3. Build SDR and Simulate 38
4. Alternate Channel Performance 39

SUPPLEMENTAL 41
A. MATLAB SCRIPTS 41
B. MATLAB FUNCTIONS 41
C. SUPPORTING DOCUMENTATION 42

LIST OF REFERENCES 43

INITIAL DISTRIBUTION LIST 45

LIST OF FIGURES

Figure 1. Noise Masking System for a Line of Sight Communication Link. Source: [3]....6

Figure 2. Secrecy Performance of OPALS. Source: [3]....6

Figure 3. Alamouti-Encoded Scheme Showing Mask Addition....23

Figure 4. Simulated BER Performance for QPSK Modulated 2x2 Alamouti STBC....28

Figure 5. BER at Eavesdropper, Masked Signal....29

Figure 6. Flow Chart for WPM Mask Addition....32

Figure 7. Simulated BER Performance 2x2 Alamouti STBC Using Additive vice MRC Equalization....35

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Encoding Scheme Assignment. Adapted from [2] and [12]. 8

Table 2. Variables Used for Channel Estimation and Equalization. Adapted from [2] and [12]. 8

Table 3. Encoding Scheme Assignment. Adapted from [2] and [12]. 16

Table 4. Variables Used for Channel Estimation and Equalization. Adapted from [2] and [12]. 16

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

2x2	two-transmitter, two-receiver
AM	amplitude modulation
AWGN	additive white Gaussian noise
BER	bit error rate
CSI	channel state information
DFT	discrete Fourier transform
DWT	discrete wavelet transform
FM	frequency modulation
FT	Fourier transform
IDFT	inverse discrete Fourier transform
IDWT	inverse discrete wavelet transform
MIMO	multiple-input, multiple-output
MISO	multiple-input, single-output
ML	maximum likelihood
MRC	maximum-ratio combining
MSR	mask-to-signal ratio
OFDM	orthogonal frequency-division multiplexing
SDR	software-defined radio
SNR	signal-to-noise ratio
STBC	space-time block coding
QAM	quadrature amplitude modulation
QPSK	quadrature phase-shift keying
SMR	signal-power-to-mask-power ratio
WPM	wavelet packet modulation

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work is dedicated to my mother, Elizabeth Sellin, for making education number one; to Mr. Maras at Morton Middle School for convincing me math was cool; and to my partner, proofreader, and sanity-checker, Christina Larson.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE

Military wireless communication systems require continuous improvement and application of increasingly secure and covert methods to stay ahead of today's sophisticated threats. As our reliance on wireless communication grows, this need becomes even more vital. While wireless communication systems offer the enemy the ability to intercept communication signals without making physical contact or even revealing their existence, these systems also offer a variety of avenues for security. In any wireless communication system, two major fundamental challenges are added to that of a wired system: fading and interference [1]. In this thesis, we attempt to take advantage of a known set of channel states to increase the security of multiple-input, multiple-output (MIMO) wireless communication by understanding the communication link between multiple antennas, then using that information to devise an additive masking signal that will intentionally degrade the message quality to any receiver other than the intended receiver. The final objective is to apply this masking scheme to a previously developed communication system utilizing wavelet packet modulation (WPM).

B. MOTIVATION

In this work, we explore an alternative or additional layer of security beyond encryption. In [2], Cribbs designed and tested a functional software defined radio system for a MIMO channel utilizing WPM. In [3], Tollefson, Jordan, and Gaeddert described a method for using a masking signal to drastically increase the security of a line-of-sight communication system. We apply the ideas in [3] to the complex communication system designed in [2] using analytic decomposition of the channel and signal and computer simulation to provide bit error rate statistics. Our application also extends to non-line-of-sight communications. In possible military applications, this method could transfer some responsibility for communication security to physical security as the signal would only able to be correctly deciphered within a small physical radius of the intended receiver. The use

of WPM may also allow for increased covertness and subcarriers with a variety of simultaneous data rates.

C. THESIS CHAPTER BREAKDOWN

In this thesis, the background, modeling, simulation, and application of the masking method to a WPM system are discussed. The background discussed in Chapter II presents the underlying theory and motivation for the work including the concepts of the wireless channel, noise masking as a method of covert communication, and MIMO. The method described in Chapter III includes a conceptual and detailed description of the mathematical implementation of the masking method. In Chapter IV, simulation setup and results are presented. These results are the extended to apply to a WPM system in Chapter V, where the intricacies and theoretical challenges of applying the masking technique to a WPM system as well as simulation results are detailed. Finally, we present conclusions and recommendations in Chapter VI, including an overall summary of results and highlighting opportunities for future research into the topic.

II. BACKGROUND

A. WIRELESS CHANNEL

Among the greatest obstacles to the development and advancement of wireless communications is understanding the wireless channel. Durgin begins his book stating, "There are few things in nature more unwieldy than the power-limited, space-varying, time-varying, frequency-varying wireless channel" [4]. This complication is due to the interaction of the propagating waves with the diverse and changing environment between transmitters and receivers [4]. While a signal in a wired system is subject to relatively small and predictable degradation to the signal as it travels from transmitter to receiver, the airborne wireless electromagnetic signal is not confined to a conductive medium and, therefore, degrades as it expands through time and space [5]. This fading is compounded by physical obstacles between transmitter and receiver. Interference is the additional degradation of the signal due to other signals existing in the same frequency band at the same time in the same space [1]. The fading phenomena are captured quantitatively in wireless communications by the channel state h. Mathematically, h is a complex value which, when multiplied by the complex envelope of the transmitted signal in the absence of noise, produces the complex envelope signal received by the receiver. Very early in the development of wireless technology, engineers realized that calculating channel conditions based on a known set of environmental parameters was quantitatively possible for only very geometrically simple channels.

1. Channel Simulation

Since quantitatively predicting wireless channel conditions is not practical, statistical methods for modeling behavior were developed. In 1944, Rice introduced the concept of utilizing random propagation models in the calculation of wireless channels [6]. The Ricean channel was predictive under certain conditions, particularly amplitude-modulated (AM) and some frequency-modulated (FM) radio transmissions, as it incorporated both line-of-sight transmission and multipath transmission or scatter [4]. The omnidirectional Rayleigh fading channel is a method of statistical estimation based on

the assumption that the multiple paths that the signal takes lead to (on average) an equal amount of energy encountering the receiver from all directions [1]. In this thesis, we implement the common example of the Rayleigh channel model for all simulations and hope that future work will show satisfactory performance for other common channel conditions

2. Channel Estimation

Channel estimation is the process by which the channel state is calculated. This estimate is then used to calculate the sent signal from the received signal [1]. Though channel estimation is important in most communication systems, it is absolutely vital to implementation of this masking method because those estimates are used directly in the calculation of the mask. We implement training symbols at prescribed intervals to accomplish this task. When the receiver is expecting to receive a training symbol whose value is known to both sender and receiver, it is able to calculate the channel condition by examining the difference in the known sent symbol and the actual received result [1]. As with most communication systems, these training symbols allow the receiver to estimate the channel states for equalization of the received signals. In this method, these channel states are also used by the transmitter to calculate the masking component, as discussed in Chapter III.

B. NOISE MASKING

Every wireless communication system relies on the concept of signal-to-noise ratio (SNR). In order for a message to be received clearly, the signal-power-to-noise-power ratio at the receiver must be greater than or equal to some prescribed minimum value that corresponds to minimum acceptable performance; therefore, one way to degrade an eavesdropper's ability to effectively receive communication is to add noise to the environment. Unfortunately, adding noise to the environment tends to degrade the ability of all receivers, both intended and otherwise. When multiple antennas are involved, this is no longer true because more than one signal is in the environment at the same time, allowing us to design additive noise signals that cancel out at the intended receiver. Signals with common frequency, propagation direction, and polarization will interfere with each

other additively, resulting in perceived gain where maxima coincide and perceived fade where they oppose [1]. When done intentionally by multiple transmit antennas, this is known as beamforming. Beamforming is a method of leveraging this characteristic by controlling the phase shifts of each specifically spaced transmit antenna to direct signal energy to a desired location. Noise masking is related to beamforming, but the goal is to spread the masking signal over a wide range of possible receiver locations except in the direction of the intended receiver [7]. In [7], Goel and Negi show that secrecy capacity defined in [8] can be significantly improved using noise masking techniques. In [3] the authors show a comparison of the effectiveness and power economy of different masking signals. These sources lay the groundwork for many of our masking calculations. The conceptual system used in [3] is shown in Figure 1. Their goal, like ours, was to eliminate the ability of an eavesdropper to receive a decodable signal in the side lobes by using a tailored masking signal. The important aspect is the red colored masking signal radiant intensity as compared to the blue colored communication signal radiant intensity. The masking signal overwhelms the communication signal in the side lobes but does not affect the signal in the intended direction of communication. In non-line-of-sight communications, this concept becomes more complex since the channel is time-varying, space-varying, and stochastic. This makes the mask calculation a complicated task that must be done in real time with frequent recalculations.

The research in [3] proved that as the mask-to-signal ratio (MSR) was increased, the communication system could effectively eliminate signal reception in the side lobes as seen in Figure 2. In this thesis, we attempt to accomplish a similar outcome in the more complex multipath wireless environment.

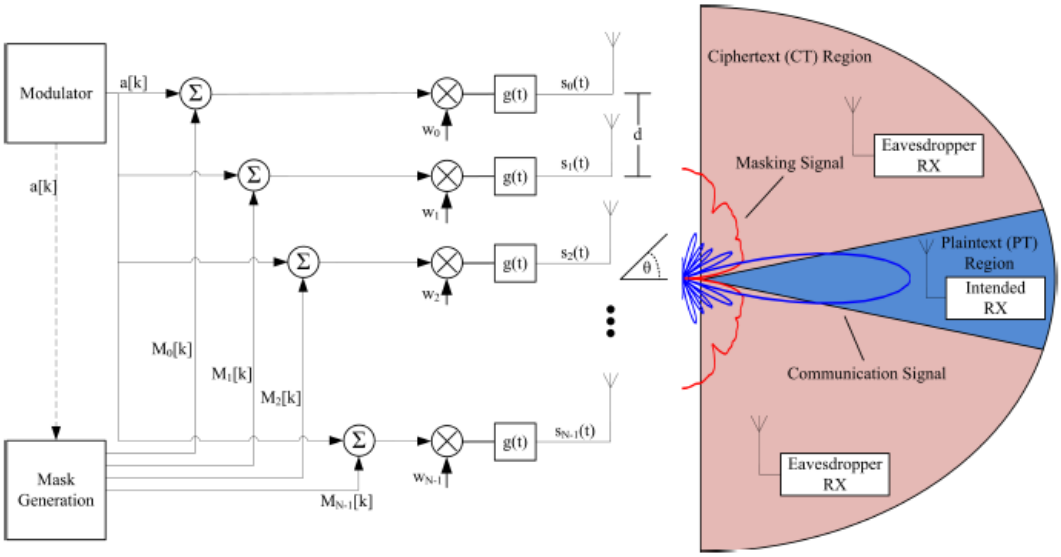

Figure 1. Noise Masking System for a Line of Sight Communication Link.
Source: [3].

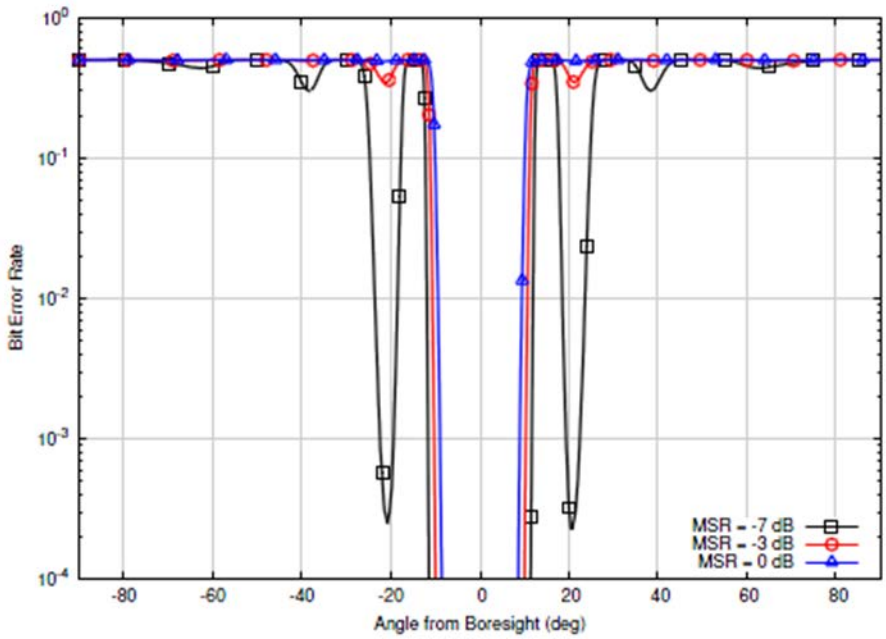

Figure 2. Secrecy Performance of OPALS.
Source: [3].

C. MULTIPLE-INPUT, MULTIPLE-OUTPUT (MIMO)

In the wireless channel as described previously, each of the many paths a signal may take between transmitter and receiver yield both positive and negative interference, resulting in times and frequencies with widely varying quality of transmission. Wireless channel states tend to be complex, short-lived, and very difficult to predict. Diversity techniques attempt to overcome the losses in transmission ability due to deep fades by finding independent signal paths for communications [9].

1. Time Diversity

The simplest way to find these independent paths is to simply repeat the message in a known pattern. This is precisely how we overcome poor reception on a radio channel or phone line: we have the speaker repeat the message and use the two transmissions of the same message to fill in the missed sections of each individual transmission. This is an example of time diversity. In this example the amount of data sent per repetition is called a block. Time diversity is simple in that it requires no additional complexity in either the transmitter or receiver but has the drawback of lowering transmission rate.

2. Spatial Diversity

Instead of repeating the message from one antenna, an alternate diversity measure is to send the message or receive the message with multiple antennas. Spatial diversity, or antenna diversity, is the technique to achieve a gain in signal-to-noise ratio (SNR) accomplished by implementing multiple antennas at the transmitter and/or the receiver as compared to the same system with one transmit and one receive antenna by utilizing independent paths for propagation [9]. The drawback to spatial diversity is the interference that multiple copies of the same message have on each other at the receiver. This effect is mitigated with coding techniques that allow receivers to discriminate between the channels.

3. Alamouti Space-Time Block Coding

Alamouti space-time block coding (STBC), or Alamouti code, combines the spatial and time-diversity techniques previously described. Alamouti code describes a widely used space-time code first described in 1998 in [10] that utilizes two transmit antennas to

transmit two data stream samples in each of two time slots. In the first time slot, antennas one and two transmit the first and second sample (s_0 and s_1), respectively. In the next time slot, antennas one and two transmit the negative complex conjugate of the second sample and the complex conjugate of the first message section ($-s_1^*$ and s_0^*), respectively. The * superscript denotes the complex conjugate. This coding is often represented in matrix form, with the columns representing time slots and the rows representing the transmit antennas [11]; i.e.,

$$\mathbf{G} = \begin{bmatrix} s_0 & -s_1^* \\ s_1 & s_0^* \end{bmatrix}. \tag{1}$$

This is more explicitly delineated in Table 1, where the time slots and antennas are identified. In each time slot, each receive antenna receives a symbol from each transmit antenna over a channel with channel condition as defined in Table 2. In later chapters, this is referred to as the unmasked case.

Table 1. Encoding Scheme Assignment.
Adapted from [2] and [12].

Output Data Stream Time Sample	TX Antenna 0 Data Stream	TX Antenna 1 Data Stream
N	s_N	s_{N+1}
$N+1$	$-s_{N+1}^*$	s_N^*

Table 2. Variables Used for Channel Estimation and Equalization.
Adapted from [2] and [12].

Channel Variables	RX Antenna 0	RX Antenna 1
TX Antenna 0	h_0	h_2
TX Antenna 1	h_1	h_3

Sample Number	RX Antenna 0	RX Antenna 1
N	r_0	r_2
$N+1$	r_1	r_3

The four transmissions are then received by the two receive antennas after passing through Rayleigh fading channels. In the noiseless case, the set of received signals is

$$\begin{aligned} r_0 &= h_0 s_N + h_1 s_{N+1} \\ r_1 &= -h_0 s_{N+1}^* + h_1 s_N^* \\ r_2 &= h_2 s_N + h_3 s_{N+1} \\ r_3 &= -h_2 s_{N+1}^* + h_3 s_N^* . \end{aligned} \tag{2}$$

Note that the channel estimate values are assumed constant throughout the transmission of both samples. Given known training symbols, the receiver calculates the channel states and then deduces the sent symbols by comparing the decision metrics

$$x_N = \frac{h_0^* r_0 + h_1 r_1^*}{|h_0|^2 + |h_1|^2} = \frac{h_2^* r_2 + h_3 r_3^*}{|h_2|^2 + |h_3|^2} \tag{3}$$

and

$$x_{N+1} = \frac{h_1^* r_0 - h_0 r_1^*}{|h_0|^2 + |h_1|^2} = \frac{h_3^* r_2 - h_2 r_3^*}{|h_2|^2 + |h_3|^2} \tag{4}$$

to the known set of possible vectors.

Throughout this thesis, the receiver's specific method of calculating and combining these decision metrics is vital to constructing a masking vector that meets the objectives.

D. WAVELET PACKET MODULATION

Wavelet packet modulation (WPM), introduced in [13], is similar to the much more common orthogonal frequency-division multiplexing (OFDM) in that it is also a multiple subcarrier modulation scheme which utilizes a transform and inverse transform pair to mathematically convert a system involving frequency-selective fading to one involving flat fading [12]. Much like OFDM utilizes the inverse discrete Fourier transform (IDFT) and discrete Fourier transform (DFT) pair, WPM utilizes the inverse discrete wavelet transform (IDWT) at the transmitter and the discrete wavelet transform (DWT) at the receiver [13]. We build our description of the WPM by first briefly describing, the Fourier Transform (FT), DFT, and finally DWT.

1. Fourier Transform (FT)

The well-known FT is used in a wide variety of mathematics and engineering areas of study and is heavily used by communication engineers. Among many other uses, the FT can be utilized to extract frequency information from a sinusoidal signal. The FT requires infinite time, so it is not ideal for use with non-stationary signals.

2. Discrete Fourier Transform (DFT)

The DFT improves on the FT for communication uses by segmenting a time-varying signal and performing the transform on each segment, then sampling in both time and frequency. For a discrete time sequence $x[n]$ where $0 \le n \le N-1$, the DFT of $x[n]$ is

$$X[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[nT]\, e^{-j2\pi nk/N},\ 0 \le k \le N-1 \tag{5}$$

where k is the frequency-domain index, T is the time between samples, and N is the total number of samples [1]. The quantity NT, referred to as the window, represents the time-domain portion of the signal which is considered. As the window is made larger, more time information is involved. This leads to a refinement of frequency resolution which is k/NT in Hz, and the DFT approaches the FT. As the window gets smaller, the opposite effect occurs: the DFT involves less time information, and frequency resolution is lowered. This is a physical manifestation of the well-known Heisenberg uncertainty principle originally applied to calculation of momentum and position of moving particles. [14].

3. Discrete Wavelet Transform (DWT)

The DWT was developed in an effort to mitigate the uncertainty weaknesses in the DFT [14]. Where the DFT achieves constant resolution at all times and frequencies by specifying a window, the DWT divides the time-frequency spectrum differently, such that higher frequency portions of the signal are calculated at better time resolution and poorer frequency resolution, while the lower frequency portions of the signal are calculated with poorer time resolution and better frequency resolution [14].

The process involves multiple steps of filtering and downsampling, where downsampling describes the process of eliminating some percentage of the samples. For example, downsampling by two means removing every other sample in the set. We now describe an example used in [14] where we are applying the DWT to a signal containing 512 discrete samples and frequencies ranging between zero and 1000 Hz. The first step is filtering the signal through both a low pass filter that results in an output frequency range of zero to 500 Hz and a high pass filter that results in an output frequency range of 500 to 1000 Hz. Looking only at the result of the filters, the output is now oversampled per the Nyquist limit since the bandwidth is reduced by half and can, therefore, be downsampled by two without losing any additional information with respect to the ability to reconstruct the discrete time signal. By downsampling this output by two we have completed the first step of the DWT. Overall we have reduced the time resolution by half by removing half of the samples but doubled the frequency resolution since each of the high and low frequency portions of the signal covers half of the previous amount of the frequency spectrum. The transform is completed by iterative application of this method to break the signal into subcarriers. In Chapter IV, we mathematically implement this form of modulation and devise a means of applying the masking method developed in Chapter III.

4. Application

WPM has been shown to outperform other modulation methods in specific severe interference environments, such as in the presence of a narrow band jammer in concert with an impulsive time-domain interferer in [13], and has been shown effective in wireless fading environments in [15]. The significant difference that allows these gains in BER and bandwidth efficiency is that OFDM subcarriers are all of equal bandwidth (and, therefore, equal data rate), whereas WPM subcarriers do not have this limitation, allowing for increased flexibility in signal construction [12], [16].

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHOD

This scheme involves developing a masking signal to be applied to a two-transmitter, two-receiver (2x2) multiple-input, multiple-output (MIMO) Alamouti space-time block code (STBC) signal such that the masking signal does not affect communication with an intended receiver but degrades an eavesdropper's ability to decipher the signal. To accomplish this, we design a masking signal that adds zero to the decision metrics at the intended receiver and a nonzero additive value to the decision metrics at an eavesdropper's receiver.

A. TERMINOLOGY

1. Masking Vector

The masking signal consists of four complex-valued quantities which are added to the four transmissions of the Alamouti STBC. These values need to be recalculated rapidly enough to remain consistent with channel state. These quantities are denoted M_0, M_1, M_2, and M_3 and are collectively referred to as $\mathbf{M}$, the masking vector. The masking vector elements M_0 and M_1 are added to s_0 and s_1, respectively, and transmitted during time slot one; M_2 and M_3 are added to the negative complex conjugate of s_1 and the complex conjugate of s_0, respectively, and transmitted during the second time slot. This masking vector is calculated to pair with a corresponding set of channel states that identify the intended receiver.

2. Channel State Vector

The set of four channel states that describe the channel between each transmit and receive antenna at a certain time is referred to as $\mathbf{H}$. As discussed in Chapter II, these channel states are modeled as complex-valued Gaussian random variables. By modeling the channel in this way, we assume that the coherence bandwidth of the channel is larger than the bandwidth of the transmitted signal, with the result that the entire frequency range of the signal experiences identical fading [9]. This type of fading is referred to as flat

fading. The channel-state vector is the fingerprint of the communication channel, affected by fading, scattering, reflection, physical objects, interference, humidity, and many other factors. Our method uses this fingerprint to tailor an additive masking signal that makes the signal decipherable only at the intended receiver. Due to the rapidly changing nature of these factors, the channel states are a rapidly changing function of time and position.

For the purposes of this thesis, the channel-state information (CSI) must be measured by the receiver and communicated back to the transmitter. This is an important additional task that our masking method requires of the receiver. To accomplish this, the transmitter sends known training symbols with all components of the masking vector set to zero at a known interval. The receiver can then calculate the channel states and communicate them back to the transmitter. From this point forward it is assumed that the transmitter has perfect knowledge of channel states.

3. Intended Receiver

The intended receiver refers to a receive antenna pair at the location and time that produces the channel state $\mathbf{H}$ which the transmitter uses to derive the masking signal $\mathbf{M}$. This receiver uses the training symbols to calculate the channel- state vector that describes the channel from transmitter to receiver. This scheme uses this information as a seed to an algorithm that calculates an additive mask to allow minimum bit error ratio (BER) at a receiver with this channel-state vector and much larger BER at a receiver with a different $\mathbf{H}$. To do this we take advantage of the decision metric calculations employed by the receive antennas.

4. Eavesdropper

An eavesdropper is any receiver whose position results in a channel state $\mathbf{H}$ significantly different from that of the intended receiver. This can vary widely based on real world conditions, but to get a realistic estimate we use calculations based on [9]. Coherence time and Doppler spread are the time and frequency domain descriptions of the effects of small scale fading [9]. Doppler spread describes the range of frequencies within which the broadening effect of the Doppler effect is significantly greater than zero [9]. Coherence time is the time-domain view of Doppler broadening, and it represents the

amount of time that the channel impulse response is essentially non-changing [9]. The two values are inversely proportional to one another. Though these can be estimated in many ways based on the range of values considered to be significantly greater than zero, those studying modern digital communications tend to use an estimate for coherence time that is descriptive but not overly restrictive [9]. This conservative estimate of coherence time is

$$T_C = \sqrt{\frac{9}{16\pi f_m^2}}, \tag{6}$$

where f_m is the maximum Doppler shift, calculated as the ratio of receiver velocity-to-signal wavelength, $f_m = v/\lambda$ [9]. This quantity can now be used to calculate the spatial sampling interval Δx, the amount of distance covered by the receiver after which the channel-state information has changed significantly

$$\Delta x = \frac{vT_C}{2}, \tag{7}$$

where Δx is the sample spacing interval and v is the target velocity [9]. We can manipulate these equations by substituting (6) into (7) and incorporating the relationship between the center signal frequency and signal wavelength λ to calculate the effective receive radius by eliminating velocity, yielding

$$\Delta x = \lambda\sqrt{\frac{9}{64\pi}}. \tag{8}$$

This estimate gives us an idea of the physical area around the intended receiver where the masking components add to zero, or the distance between intended receiver and eavesdropper that makes their channels essentially uncorrelated. If our transmission frequency is 900 MHz, this indicates an effective receive radius of approximately 6 cm. For all but the lowest carrier frequencies, the plaintext region is very small, meaning a greater level of security for our method.

B. CALCULATION

1. Mask Effect

We start by investigating the effect of adding a generalized unitless complex-valued masking vector $\mathbf{M}$ to unitless Alamouti-coded symbols and evaluating its effect on the receiver's decision metrics. We then use this known effect to calculate a *specific* $\mathbf{M}$ such that it cancels at the receiver. In order to perform this calculation, it is essential to assume the transmitter has perfect knowledge of the channel state as discussed previously.

Adding a component of the additive masking vector $\mathbf{M} = [M_0 \quad M_1 \quad M_2 \quad M_3]$ to each individual coded transmission in (1) yields

$$\mathbf{G} = \begin{bmatrix} s_0 + M_0 & -s_1^* + M_2 \\ s_1 + M_1 & s_0^* + M_3 \end{bmatrix}. \tag{9}$$

Following the assignment pattern from Chapter II, we assign the encoding scheme and channel variables in Tables 3 and 4.

Table 3. Encoding Scheme Assignment.
Adapted from [2] and [12].

Output Data Stream Time Sample	TX Antenna 0 Data Stream	TX Antenna 1 Data Stream
N	$s_N + M_0$	$s_{N+1} + M_1$
$N+1$	$-s_{N+1}^* + M_2$	$s_N^* + M_3$

Table 4. Variables Used for Channel Estimation and Equalization.
Adapted from [2] and [12].

Channel Variables	RX Antenna 0	RX Antenna 1
TX Antenna 0	h_0	h_2
TX Antenna 1	h_1	h_3

Sample Number	RX Antenna 0	RX Antenna 1
N	r_0	r_2
$N+1$	r_1	r_3

The four transmissions are then received by the two receive antennas after passing through a faded channel. In a noiseless environment, the set of received transmissions is

$$\begin{aligned} r_0 &= h_0(s_N + M_0) + h_1(s_{N+1} + M_1) \\ r_1 &= h_0(-s_{N+1}^* + M_2) + h_1(s_N^* + M_3) \\ r_2 &= h_2(s_N + M_0) + h_3(s_{N+1} + M_1) \\ r_3 &= h_2(-s_{N+1}^* + M_2) + h_3(s_N^* + M_3). \end{aligned} \tag{10}$$

Note that the channel estimate values are assumed constant throughout the transmission of both samples. Now at receive antenna 0 we can conclude

$$h_0^* r_0 + h_1 r_1^* = s_N \left(|h_0|^2 + |h_1|^2 \right) + |h_0|^2 M_0 + h_0^* h_1 \left(M_1 + M_2^* \right) + |h_1|^2 M_3^*. \tag{11}$$

Solving for the transmitted symbol yields

$$s_N = \frac{h_0^* r_0 + h_1 r_1^*}{|h_0|^2 + |h_1|^2} - \frac{|h_0|^2 M_0 + h_0^* h_1 \left(M_1 + M_2^* \right) + |h_1|^2 M_3^*}{|h_0|^2 + |h_1|^2}. \tag{12}$$

Similarly, at receive antenna 1

$$h_2^* r_2 + h_3 r_3^* = s_N \left(|h_2|^2 + |h_3|^2 \right) + |h_2|^2 M_0 + h_2^* h_3 \left(M_1 + M_2^* \right) + |h_3|^2 M_3^* \tag{13}$$

and

$$s_N = \frac{h_2^* r_2 + h_3 r_3^*}{|h_2|^2 + |h_3|^2} - \frac{|h_2|^2 M_0 + h_2^* h_3 \left(M_1 + M_2^* \right) + |h_3|^2 M_3^*}{|h_2|^2 + |h_3|^2}. \tag{14}$$

By implementing these calculations, each receive antenna can calculate the sent symbol as in the multiple-input, single-output (MISO) case. Per [11] and [17], the maximum-ratio combining (MRC) decision statistic is calculated by finding the weights to apply to the terms from each antenna in order to maximize SNR:

$$\begin{aligned} x_N = {} & \frac{h_0^* r_0 + h_1 r_1^* + h_2^* r_2 + h_3 r_3^*}{|h_0|^2 + |h_1|^2 + |h_2|^2 + |h_3|^2} - \\ & \frac{\left(|h_0|^2 + |h_2|^2 \right) M_0 + \left(h_0^* h_1 + h_2^* h_3 \right) \left(M_1 + M_2^* \right) + \left(|h_1|^2 + |h_3|^2 \right) M_3^*}{|h_0|^2 + |h_1|^2 + |h_2|^2 + |h_3|^2}. \end{aligned} \tag{15}$$

The specific method of equalization and decoding utilized by the receiver is essential to the correct calculation of the mask elements. This constitutes necessary a priori agreement or a dedicated hardware constraint in the design phase. For the purposes of this chapter, we implement MRC due to its common usage and its maximization of SNR. This masked decision metric differs from the unmasked decision metric discussed in Chapter II only in the addition of the second term containing members of the masking vector. This term represents the effect of the masking vector $\mathbf{M}$ on the receiver's calculation of the decision metric for x_N. Note that if no masking vector were applied or if each component of the masking vector were set to zero, the results would be the same as in [2] and [12], allowing the decision statistic to be calculated directly.

In our case, a receiver armed with the received signal and the calculated channel states can calculate the decision statistic x_N with high accuracy only if all terms including a member of the $\mathbf{M}$ vector add to zero or are insignificant compared to the first term; i.e.,

$$\left(|h_0|^2 + |h_2|^2\right) M_0 + \left(h_0^* h_1 + h_2^* h_3\right)\left(M_1 + M_2^*\right) + \left(|h_1|^2 + |h_3|^2\right) M_3^* = 0. \tag{16}$$

This is the first equation required to determine the components of the masking vector. With this condition met (that is, at the intended receiver), the MRC decision variable is exactly as it is in the unmasked case, and successful resolution is available. This is the desired effect at the intended receiver. At an eavesdropper, the channel conditions are uncorrelated with the channel conditions at the intended receiver within the limitations of the faded channel; therefore, the term added to the decision metric does not equal zero and negatively affects the accuracy of the adversary decision statistic, increasing BER. This is the desired effect of the masking vector. Similar manipulation to solve for x_{N+1} gives

$$h_1^* r_0 - h_0 r_1^* = s_{N+1}\left(|h_0|^2 + |h_1|^2\right) + h_0 h_1^* M_0 + |h_1|^2 M_1 - |h_0|^2 M_2^* - h_0 h_1^* M_3^* \tag{17}$$

and

$$h_3^* r_2 - h_2 r_3^* = s_{N+1}\left(|h_2|^2 + |h_3|^2\right) + h_2 h_3^* M_0 + |h_3|^2 M_1 - |h_2|^2 M_2^* - h_2 h_3^* M_3^*. \tag{18}$$

Now the x_{N+1} decision statistic is

$$x_{N+1} = \frac{h_1^* r_0 - h_0 r_1^* + h_3^* r_2 - h_2 r_3^*}{|h_0|^2 + |h_1|^2 + |h_2|^2 + |h_3|^2} - \frac{\left(h_0 h_1^* + h_2 h_3^*\right) M_0 + \left(|h_1|^2 + |h_3|^2\right) M_1 - \left(|h_0|^2 + |h_2|^2\right) M_2^* - \left(h_0 h_1^* + h_2 h_3^*\right) M_3^*}{|h_0|^2 + |h_1|^2 + |h_2|^2 + |h_3|^2}. \tag{19}$$

This is resolvable without mask impact by the receiver when

$$\left(h_0 h_1^* + h_2 h_3^*\right) M_0 + \left(|h_1|^2 + |h_3|^2\right) M_1 - \left(|h_0|^2 + |h_2|^2\right) M_2^* - \left(h_0 h_1^* + h_2 h_3^*\right) M_3^* = 0. \tag{20}$$

A masking vector which meets the requirements of (16) and (20), therefore, is undetectable to the intended receiver but degrades the eavesdropper's fidelity.

2. Signal Power and Mask Power

In the calculation of both the signal power and the mask power, we use the one-Ohm normalization convention, which results in normalized power in units of volts^2. Specifically, the average normalized mask power from the combination of the two transmit antennas is

$$P = \frac{1}{2} A^2 \sum_{i=0}^{3} |M_i|^2 \tag{21}$$

where A is an amplitude in volts. For this thesis, we refer to the unitless sum of the magnitude of the masking vector components $\sum_{i=0}^{3} |M_i|^2$ as mask power. Similarly, we refer to the unitless sum of the magnitudes of the signal components $\sum_{i=0}^{3} |s_i|^2$ as signal power.

3. Additional Constraints

First, we must consider how to bound the mask power. Setting all mask components to zero meets the criteria of (16) and (20) but fails to degrade the eavesdropper's ability to intercept the message. If mask power is permitted to be arbitrarily large, we are not creating a realistic model. To ensure that total masking power is limited we require

$$\sum_{i=0}^{3} \left| M_i \right|^2 = 1. \tag{22}$$

As stated in the previous section, we refer to this quantity as the power of the mask using the one-Ohm normalization convention. In the simulations presented in Chapter IV, we alter (22) to control the signal-to-mask ratio (SMR) by changing the right-hand side to the appropriate constant. This affects the mask value but only affects the mask calculation process trivially.

Additionally, following [3], we introduce an arbitrary but convenient constraint on the sum of the masking vector components

$$\sum_{i=0}^{3} M_i = 0. \tag{23}$$

4. Mask Vector Calculation

Now that we know that effect of the mask on the receiver, we must use the channel-state vector $\mathbf{H}$ that represents the channel from transmitter to intended receiver to find acceptable values for $\mathbf{M}$. Acceptable values include those sets of complex mask numbers that result in zero alteration of the decision statistics for either the odd- or even-indexed symbols, sum to zero, and have unity power. To calculate $\mathbf{M}$, we must solve three complex linear equations, (16), (20), and (23), with four complex-valued unknowns and one nonlinear constraint (22). Treating the real and imaginary part of each variable and equation separately, we are left with seven equations and eight unknowns. To approach this problem, we temporarily neglect the nonlinear constraint and focus on the three linear constraints. This set of three equations and four complex-valued unknowns is an underdetermined system and, therefore, has many possible solutions.

First, we bound the system by adding an additional linear constraint. This linear constraint must be independent of the other three linear constraints and must add to a nonzero constant, e.g.,

$$\frac{1}{4}M_0 + \frac{1}{4}M_1 + \frac{1}{4}M_2 - \frac{1}{4}M_3 = 1. \tag{24}$$

When we include (24) with (16), (20), and (23), we have four complex linear equations with four complex-valued unknowns. This system has a distinct solution which can be found quickly. We call this solution $\mathbf{B}$. We now take advantage of the fact that the constant (right-hand side) term of each of the linear equations which are essential to the calculation is zero. Any valid solution to these three can be scaled by any constant, and the result is another solution to the three essential equations. Note that a scaled $\mathbf{B}$ no longer solves the full system of equations, specifically it does not solve (24). This is not problematic since (24) was arbitrarily but conveniently chosen.

Now we must find the constant by which to scale $\mathbf{B}$ to meet our power constraint. We calculate the average power of $\mathbf{B}$, then apply the scale that forces it to unity, which yields

$$\mathbf{M} = \frac{\mathbf{B}}{|\mathbf{B}|}. \tag{25}$$

The resulting vector $\mathbf{M}$ is a solution to (16), (20), (22), and (23) and therefore represents a masking agent which meets the requirements of not affecting communication to the intended receiver and significantly degrading effectiveness of an eavesdropper.

With $\mathbf{M}$ calculated, the transmitter appends the mask components to each coded symbol prior to transmission as described in Table 3. When received by the intended receiver, all terms containing a member of $\mathbf{M}$ add to zero in the decision statistic, and the message is received. An eavesdropper calculates each decision statistic with a nonzero additive complex-valued term which degrades their eavesdropping ability.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS

A. SIMULATION

Simulation was conducted using MATLAB software. Though some Alamouti simulation code is available, all tend to simplify channel calculations by using a mathematical manipulation to apply the coding scheme to the channel vice the data symbols. The additive nature of our masking scheme precluded this manipulation, so we produced encoding software. After coding the basic two-transmitter, two-receiver (2x2) scheme but before adding mask, we verified that our software produced equivalent results for both simulation [17] and theory [10], [18]. The basic layout of the simulation is shown in Figure 3.

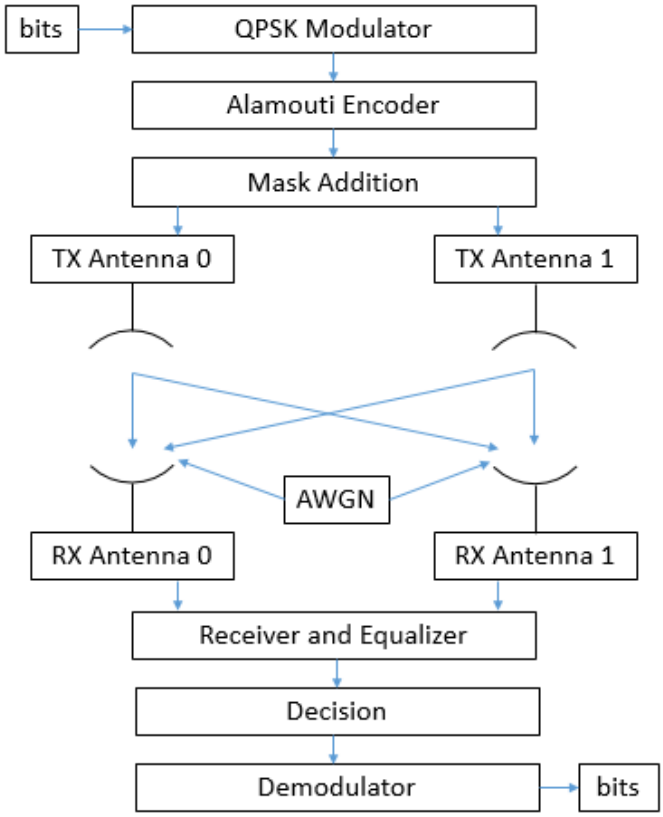

Figure 3. Alamouti-Encoded Scheme Showing Mask Addition

1. Signal Generation

To simulate a random bit stream, we utilized the *randi* function. We then modulated that bit stream into gray coded quadrature phase-shift keying (QPSK) symbols by first grouping the bits into sets of two, then encoding that pair as the magnitudes of the real and imaginary portions of the symbol. We now have one symbol for every two bits. At this point we normalize the symbols to have unit energy by multiplying each by $1/\sqrt{2}$. This allows simpler implementation of a range of energy-per-bit-to-noise-power-spectral-density ratio (E_b/N_0) values.

2. Channel

In the case of a 2x2 MIMO system, the channel-state vector $\mathbf{H}$ consists of four complex values per block of the Alamouti coded signal. For the purpose of simulation, each member of the state vector $\mathbf{H}$ is modeled as a circularly symmetric complex Gaussian random variable based on the Rayleigh channel model. This assumption is valid when there are a large number of statistically independent paths due to scattering and reflection [1]. These statistically independent paths combine to create each of the channel-state values, so by the central limit theorem, it is reasonable to use independent and identically distributed zero-mean Gaussian random variables for both the real and complex portions of the variable [1]. In MATLAB this is implemented by using the *randn* function to create both the real and imaginary parts of each member of $\mathbf{H}$. These values are also normalized to unit energy since the channel states are used to model fading, not gross attenuation due to distance.

3. Alamouti Coding

In order to fit the Alamouti coding scheme, the QPSK symbols are separated into blocks of two symbols. In MATLAB, this is done using the *reshape* function to convert the one by n row vector into a two by $n/2$ matrix. Now each column is a set of two consecutive symbols. Each column must be replicated in order to create the second copy for the time diversity aspect of the STBC. This was accomplished using the *kron* function.

Each even column must have its two members switch positions, the complex conjugate is calculated, and the resulting first column multiplied by -1. For example,

$$\begin{bmatrix} s_0 & s_1 & s_2 & s_3 \ldots \end{bmatrix} \rightarrow \begin{bmatrix} s_0 & -s_1^* & s_2 & -s_3^* \ldots \\ s_1 & s_0^* & s_3 & s_2^* \ldots \end{bmatrix}. \tag{26}$$

4. Mask Addition

The mask is calculated as described in Chapter III. In order to add correctly to the matrix of coded symbols, the mask vector is reshaped into a two-row matrix, and each block of four state parameters is replicated. The vector addition yields the masked signal at the transmitter, i.e.,

$$\begin{bmatrix} s_0 + M_0 & -s_1^* + M_2 & s_2 + M_4 & -s_3^* + M_6 & \ldots \\ s_1 + M_1 & s_0^* + M_3 & s_3 + M_5 & s_2^* + M_7 & \ldots \end{bmatrix}. \tag{27}$$

5. Receiver

These coded, masked symbols now travel via their respective channels to the two receive antennas. Mathematically, this involves multiplying each transmission by its respective channel-state value and adding white Gaussian noise (AWGN). The state vectors are created as explained previously, and the AWGN is modeled as a circularly symmetric complex Gaussian random variable with zero mean. The noise variance is easily calculated for a range of E_b / N_0 because the energy per bit is normalized. For example, during the first time slot, antenna 0 receives

$$\hat{r}_0 = \left(s_0 + M_0\right) h_0 + \left(s_1 + M_1\right) h_1 + n_0 , \tag{28}$$

where n_0 represents the complex component of the noise vector associated with receive antenna 0 and time slot 0. In order to execute this over a large matrix, the state vector is reshaped into a two-row matrix then array multiplied by the masked symbols matrix. The columns of this resulting matrix are summed and noise is added.

6. Equalization

The receiver now has a row vector of received data with two entries per data symbol. These are mathematically manipulated to produce the MRC decision statistic as described in Chapter II. In MATLAB, this requires multiple reshaping and replicating operations on the channel-state matrix. First, we must recognize that even and odd indexed symbols are calculated with different equations. Note that MATLAB array indexing begins with one, so even-subscripted members of a row vector occupy odd-valued columns. To solve for odd-indexed decision metrics, the channel-state matrix is treated as a row vector, and the complex conjugate of each odd-indexed term is taken. Then we take the complex conjugate of each even-indexed component of the received matrix **r**. Finally, these are combined by array multiplication, reshaping, and summing columns to yield $x_0 = h_0^* r_0 + h_1 r_1^* + h_2^* r_2 + h_3 r_3^*$ for the first two symbols. Even-indexed decision metrics are found similarly, except the complex conjugate is taken on the even-indexed terms of the received vector and the odd-indexed terms of the channel-state vector. Additionally, the odd-indexed terms of the channel-state vector must be multiplied by negative one per the Alamouti code to yield $x_1 = h_1^* r_0 - h_0 r_1^* + h_3^* r_2 - h_2 r_3^*$.

7. Decision

For true MRC per [10] and [11], these decision statistics are normalized by dividing them by the sum of the square of the absolute values of the channel states, but for QPSK maximum-likelihood (ML) decision making this is unnecessary since the normalization affects only the magnitude. The decision is made based only on the phase; therefore, the ML decider only has to test the phase of the decision metric against a range of known possible symbols and select the symbol closest in phase. Simply, since the encoded symbols have phases of $\pi/4$,$3\pi/4$,$5\pi/4$, and $7\pi/4$, the detector only needs to find the quadrant of the phase of each decision metric and assign it to the symbol associated with that quadrant of the complex plane. MATLAB allows this easily using the *discretize* function on the angle of the decision metrics.

8. Demodulation

Once the received symbols have been decided, each symbol must be broken into its two-bit content. This is done immediately following the *discretize* function, as we assign a two-bit output corresponding to each symbol decision.

9. Error Analysis

We now must find erroneously passed information by comparing the sent bit stream to the received bit stream. The errors are counted by summing the absolute values of the difference of the two vectors, and the BER is calculated by dividing that sum by the number of bits transmitted.

10. Results

To simulate BER performance, we implemented a sample size of 10^7 bits and a signal-power-to-mask-power ratio (SMR) of 0-dB for each of the three scenarios, where SMR is defined as

$$SMR = \frac{E\left\{\left|\mathbf{s}\right|^2\right\}}{\left|\mathbf{M}\right|^2}, \tag{29}$$

where $E\{\ \}$ is the expectation. The mask power is not an expectation because (22) forces the mask power to a chosen constant. For consistency in units, we again use the one-Ohm normalized power convention for both the signal power and the mask power.

The results of the three simulations displayed in Figure 4 demonstrate the effectiveness of the mask to degrade the signal at an eavesdropper while not affecting the signal at the intended receiver. First, the blue line represents an unmasked case which acts as the baseline for unmasked signals and also represents the real situation when training symbols are passed. These results are consistent with the theoretical BER in [18] and simulation results in [10] and [17]. This result is valid for any receiver (intended or eavesdropper) because no mask is applied. The second case is the signal with mask applied and sent to the intended receiver. The result verifies that the mask does not cause a detectable change at the intended receiver. Finally, the third case is the BER of the masked

signal at an eavesdropper. This eavesdropper was simulated by resetting the $\mathbf{H}$ to an independent circularly symmetric complex random value after each calculation of $\mathbf{M}$.

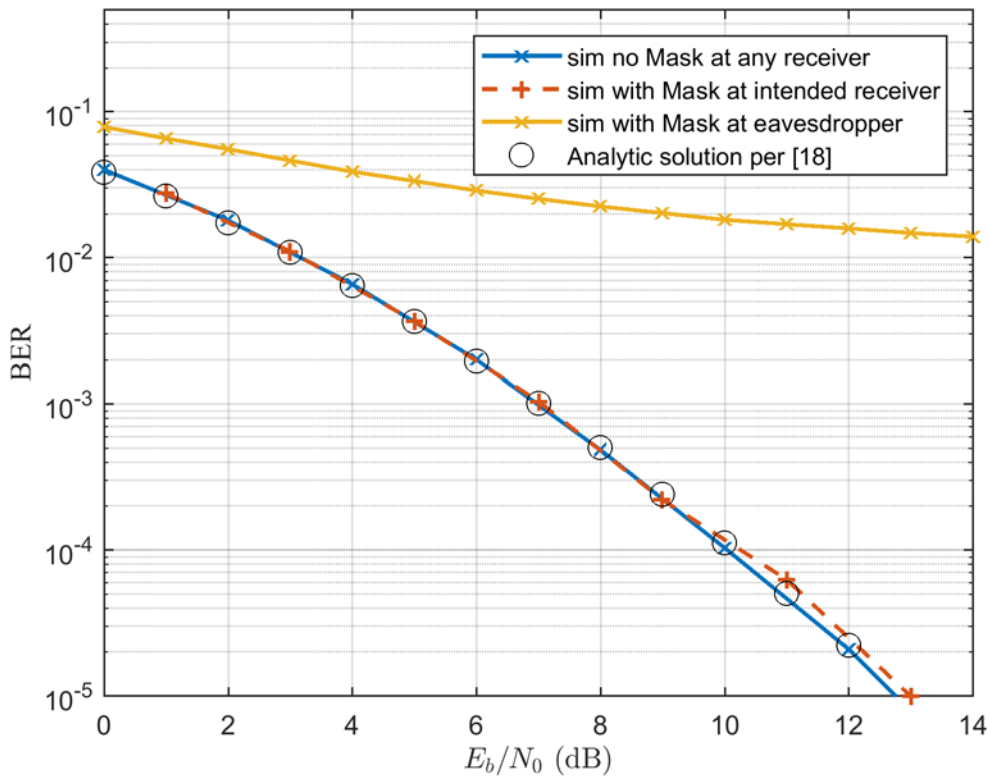

Figure 4. Simulated BER Performance for QPSK Modulated 2x2 Alamouti STBC

In Figure 5, we examine the BER results at an eavesdropper over a range of signal-to-mask ratios for five values of SNR. In order to independently examine the effect of changing the signal-power-to-mask-power ratio without affecting E_b/N_0, we altered the mask calculation algorithm to force the power of the mask to certain values, then applied these masks to a range of E_b/N_0. With a small signal-to-mask ratio, the noise dominates as the error source and results are consistent with the masked case in Figure 4. As the mask power is raised while signal power is held constant, its effect becomes significant as the error source. This shows that for any E_b/N_0, as the

signal-power-to-mask-power ratio decreases, the BER at the eavesdropper increases. It also shows that for a larger E_b/N_0, the effect of the mask is even more pronounced. The total effect is that enhanced security can be accomplished either by decreasing E_b/N_0 or by increasing the mask power. In a radio designed with adjustable mask power, raising mask power effectively moves left along the horizontal axis, raising BER and, therefore, increasing security.

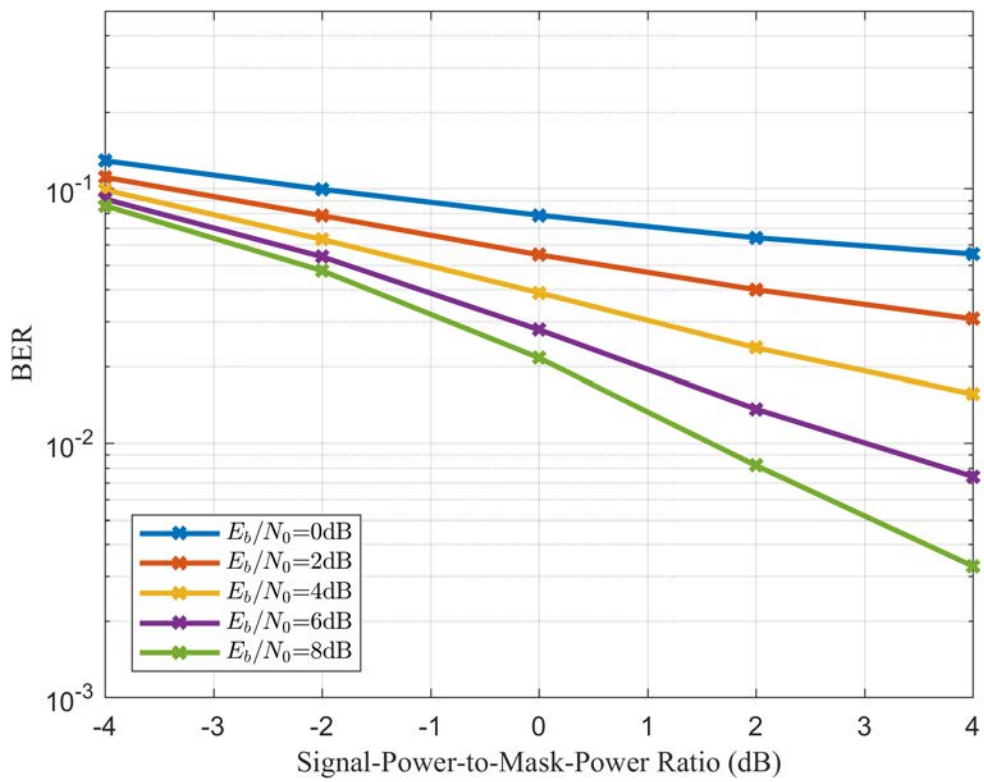

Figure 5. BER at Eavesdropper, Masked Signal

B. SUMMARY

In order to simulate the effect of our masking method, we designed MATLAB software to analyze each step of the communication process from message bit stream at the sender to message bit stream at the receiver. After verifying this process to be consistent with published theoretical and experimental results, we designed and implemented software to use known CSI to calculate a mask vector added to the Alamouti-coded symbols before entering the channel such that its effect added to zero at the intended receiver but distorted reception for an eavesdropper. These simulations revealed that this process did in fact degrade reception at an eavesdropper as shown in Figure 4, and the amount of degradation was dependent on the ratio of transmitted power between the signal and mask. This lends itself to the possibility of building a radio with the ability to vary or eliminate this mask effect depending on power constraints and threat environment.

V. APPLICATION TO WPM

In this chapter, we investigate the challenges and opportunities encountered in attempting to apply the noise masking method of Chapter III to a wavelet packet modulated (WPM) Alamouti space-time block-coded (STBC) signal. First, we determine the simplest order in which to apply the WPM and STBC. To do so, we rely on the framework for application of a general STBC signal to a WPM scheme as laid out in Appendix C of [12] and theoretical background from [19], then incorporate our masking scheme and, finally, add receive antenna diversity.

A. WPM AND STBC ORDER

First, we investigate possible orders of operation for the proposed radio. Results from [2] and [12] suggest that the WPM should follow the STBC. Per [13] and [19], the complex envelope of a WPM signal yields

$$s_{WPM}(t) = A\sum_{i=1}^{J}\sqrt{2^{l_i}}\sum_{m=-\infty}^{\infty}\alpha_m^i p_{n_i}\left(\frac{2^{l_i}t}{T}-m\right), \tag{30}$$

where $n_i \in \mathbb{Z}_+$, $-l_i \in \mathbb{Z}_+$, $\mathbb{Z}_+$ is the set of non-negative integers, $p_{n_i}()$ are orthogonal pulses that each define one of J subchannels, and α_m^i are the transmitted channel symbols. Applying Alamouti STBC to this type of signal is troublesome because the first summation over the J subcarriers acts to spread scaled versions of the encoded pulses over both time and frequency; however, on a per subchannel basis, we let $J=1$ because J represents the number of subchannels. This eliminates the first summation and results in $n_J = n_1$ and $l_J = l_1$. The first member of each of the sets n_i and l_i is zero; therefore, $n_J = n_1 = 0$ and $l_J = l_1 = 0$, which yields

$$s_1(t) = A\sum_{m=-\infty}^{\infty}\alpha_m p_0\left(\frac{t}{T}-m\right), \tag{31}$$

which is recognizable as the complex envelope of a quadrature amplitude modulation (QAM) encoded pulse train. In Chapter III, we showed that the masking scheme is effective

on a per subchannel basis. For these reasons, we prove the viability of the masking scheme in a radio in which the transmitter applies WPM to the signal following STBC encoding and before the transmit antennas, as shown in Figure 6. This order is also followed in [2] and [12].

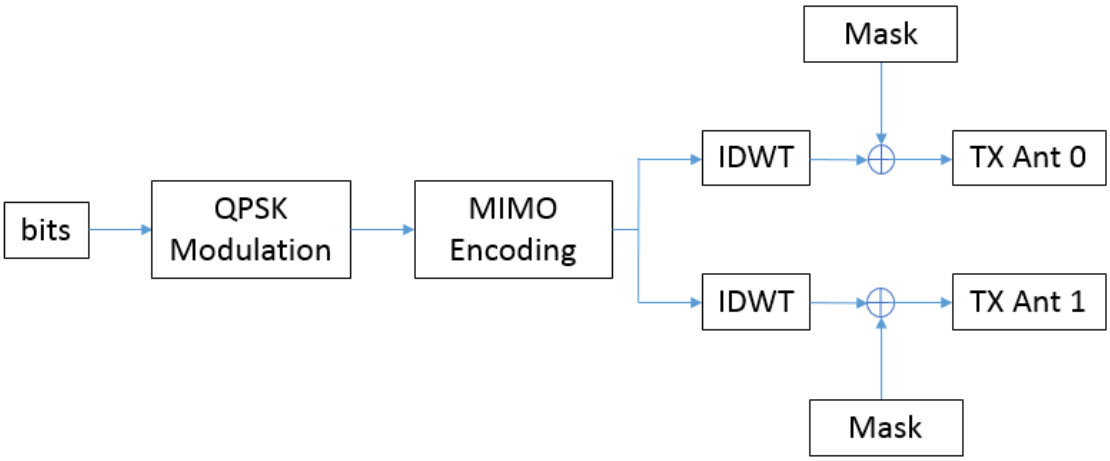

Figure 6. Flow Chart for WPM Mask Addition

B. EQUALIZATION

As in Chapter III, the key to devising a masking method that cancels at the intended receiver is taking advantage of knowledge of the method of equalization at the receiver. Previously, we devised a masking signal calculation based on the assumption of the use of maximum-ratio combining (MRC) at the receive end. This is not the case in both [2] and [12]; therefore, the masking signal designed previously does not work for the Cribbs SDR. As discussed in Chapter II, each receive antenna has the ability to calculate a decision metric for each symbol on its own. By employing two receive antennas, the system has two values for the decision metric for each symbol. In Chapter III, we discussed the MRC method to maximize the likelihood of correct symbol selection. This is not the only method available for equalization. Though MRC gives the best results, it requires a relatively complex calculation. Cribbs chose instead to calculate the decision metrics as the sum of

the decision metrics from the two receive antennas for each symbol. This significantly changes the mask equalization and the required mask calculation.

C. MASK CALCULATION

The equalization method for the WPM system proposed in [2] works by calculating the decision metric for each symbol independently in each receive antenna as if each were part of a multiple-input, single-output (MISO) system. These complex results are then averaged to yield the decision statistic; therefore, we must alter the calculations from Chapter III.

In an identical fashion to Chapter III, the set of four transmissions received by the two receive antennas after passing through noiseless fading channels is

$$\begin{aligned} r_0 &= h_0(s_N + M_0) + h_1(s_{N+1} + M_1) \\ r_1 &= h_0(-s_{N+1}^* + M_2) + h_1(s_N^* + M_3) \\ r_2 &= h_2(s_N + M_0) + h_3(s_{N+1} + M_1) \\ r_3 &= h_2(-s_{N+1}^* + M_2) + h_3(s_N^* + M_3). \end{aligned} \tag{32}$$

At receive antenna 0

$$s_N = \frac{h_0^* r_0 + h_1 r_1^*}{|h_0|^2 + |h_1|^2} - \frac{|h_0|^2 M_0 + h_0^* h_1 \left(M_1 + M_2^*\right) + |h_1|^2 M_3^*}{|h_0|^2 + |h_1|^2}, \tag{33}$$

and at receive antenna 1

$$s_N = \frac{h_2^* r_2 + h_3 r_3^*}{|h_2|^2 + |h_3|^2} - \frac{|h_2|^2 M_0 + h_2^* h_3 \left(M_1 + M_2^*\right) + |h_3|^2 M_3^*}{|h_2|^2 + |h_3|^2}. \tag{34}$$

Due to the weighted averaging method employed, the new decision statistic yields

$$x_N = \left(\frac{1}{2}\right)\begin{pmatrix} \dfrac{h_0^* r_0 + h_1 r_1^*}{|h_0|^2 + |h_1|^2} + \dfrac{h_2^* r_2 + h_3 r_3^*}{|h_2|^2 + |h_3|^2} - \\ \dfrac{|h_0|^2 M_0 + h_0^* h_1 \left(M_1 + M_2^*\right) + |h_1|^2 M_3^*}{|h_0|^2 + |h_1|^2} - \\ \dfrac{|h_2|^2 M_0 + h_2^* h_3 \left(M_1 + M_2^*\right) + |h_3|^2 M_3^*}{|h_2|^2 + |h_3|^2} \end{pmatrix}. \tag{35}$$

At the intended receiver, we desire that the final two terms add to zero; i.e.,

$$\frac{|h_0|^2 M_0 + h_0^* h_1 \left(M_1 + M_2^*\right) + |h_1|^2 M_3^*}{|h_0|^2 + |h_1|^2} + \frac{|h_2|^2 M_0 + h_2^* h_3 \left(M_1 + M_2^*\right) + |h_3|^2 M_3^*}{|h_2|^2 + |h_3|^2} = 0. \tag{36}$$

Similar manipulation to solve for x_{N+1} yields

$$x_{N+1} = \left(\frac{1}{2}\right)\begin{pmatrix} \dfrac{h_1^* r_0 - h_0 r_1^*}{|h_0|^2 + |h_1|^2} + \dfrac{h_3^* r_2 - h_2 r_3^*}{|h_2|^2 + |h_3|^2} - \\ \dfrac{h_0 h_1^* M_0 + |h_1|^2 M_1 - |h_0|^2 M_2^* - h_0^* h_1 M_3^*}{|h_0|^2 + |h_1|^2} - \\ \dfrac{h_2 h_3^* M_0 + |h_3|^2 M_1 - |h_2|^2 M_2^* - h_2 h_3^* M_3^*}{|h_2|^2 + |h_3|^2} \end{pmatrix}. \tag{37}$$

This is resolvable by the receiver when the final two terms add to zero; i.e.,

$$\frac{h_0 h_1^* M_0 + |h_1|^2 M_1 - |h_0|^2 M_2^* - h_0^* h_1 M_3^*}{|h_0|^2 + |h_1|^2} + \frac{h_2 h_3^* M_0 + |h_3|^2 M_1 - |h_2|^2 M_2^* - h_2 h_3^* M_3^*}{|h_2|^2 + |h_3|^2} = 0. \tag{38}$$

In order to update the mask calculator to accommodate this change, (36) and (38) replace (16) and (20). Additionally, the equalizing software must be updated to implement this scheme.

D. RESULTS

In order to test this new setup, the software used in Chapter III was used in its original form with the exception of the mask calculator and the equalizer. These were edited to reflect the calculations shown in Section C. Simulation results for this method were nearly identical to the previous method with the exception of larger BER for all cases due to non-ideal equalization as shown in Figure 7. This system requires at least a 2.0-dB increase in E_b/N_0 to achieve results similar to the MRC case described in Chapters III and IV. Note that these results represent BER for one subchannel of the WPM transmission. The mask still successfully and significantly degraded eavesdropper performance while not affecting BER at the intended receiver.

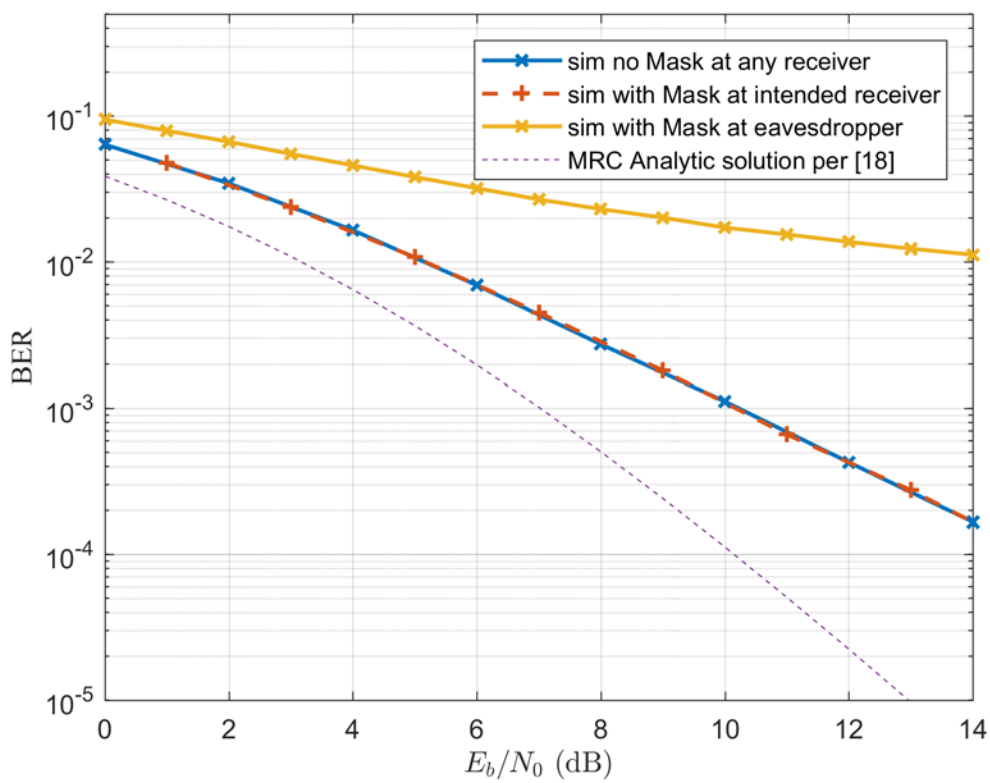

Figure 7. Simulated BER Performance 2x2 Alamouti STBC Using Additive vice MRC Equalization

Based on these results, this method can be applied to a communication system that employs WPM by applying it on a per-subchannel basis following MIMO encoding provided that the method of equalization is known and accounted for in the mask calculation.

VI. CONCLUSIONS AND RECOMMENDATIONS

Through an analytical approach and computer simulations, we have shown in this research that with known channel-state information a masking signal can be calculated that physically and severely limits the area in which a multiple-input, multiple-output (MIMO) encoded, wavelet packet modulated (WPM) signal can be deciphered, thereby foiling would-be eavesdroppers.

A. OBJECTIVES

The first objective of this research was to analytically break down the Alamouti space-time block code method and investigate the effect of a complex-valued additive noise signal on a receiver's decision statistics. In this pursuit we realized that this was possible and that it depended heavily on the equalization method employed. By first breaking down the maximal ratio combining method, we analytically solved for a masking vector that resulted in zero effect at the receiver with the known channel-state information and a nonzero effect elsewhere. We then designed software to perform this calculation with additional constraints in order to efficiently add an effective masking vector to the transmitted signal. Results displayed in Figures 4 and 5 in Chapter IV show that this method is effective, and the first objective was met.

The second objective was to determine if this method could be manipulated to be effective in a specific, more complex communication system proposed by [12] and implemented in software defined radio by [2]. We analytically showed in Chapter V that the masking method could be effective on a wavelet packet modulated version of the system used in Chapter III but only when applied to each individual subchannel. A second issue was that this system used a different method of equalization, requiring significant changes to the calculation of the masking vector. These calculations and subsequent results are shown in Chapter V.

B. CHALLENGES AND FURTHER RESEARCH OPPORTUNITIES

Though the objectives were met, significant challenges revealed many areas available for additional research.

1. Channel-State Information (CSI) Methods

Though training symbols are a well understood and popular method of determination of channel states, the lower throughput that results from this method has led to significant research into channel reciprocity [20], [21]. These methods involve the transmitter calculating the channel states via feedback and passing the estimates to the receiver, mitigating the throughput lost to training symbols [22]. These methods rely on the electromagnetic principle that waves traveling over the same channel in either direction encounter the same set of obstacles causing interference and, therefore, can be used for estimation [21]. These methods could be applied to further improve the throughput of the method described in this thesis by removing the need for the receiver to communicate the channel states back to the transmitter.

2. Optimization of Mask Calculator

Our method of calculating the mask from the channel state is effective but has room for optimization. Specifically, the final equation created to bound the linear solution before scaling can be manipulated significantly as long as it meets the requirements of independence and resulting in a nonzero sum. Deeper analysis to determine which components of this equation yield more effective mask vectors is yet to be determined.

3. Build SDR and Simulate.

A final logical step in further research is to recreate Cribbs' software-defined radio (SDR) utilizing gnu radio and implement a system to sense channel conditions, calculate mask vectors, and prove the utility of the system, utilizing guidance in [2] and [23]. It may also be possible to devise a system that could work with an automatic gain control algorithm in the receiver. This system would allow deeper research into optimization of mask power, as this is a limiting factor on final system performance. Additionally, maximal-ratio combining can be implemented to enhance receiver performance.

4. Alternate Channel Performance

Further research into a masking agent's performance in a Ricean or unfaded channel will give increased insight into the flexibility of this method. Differing channel estimation methods will involve different channel-state parameters and significantly different calculations.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL

Included in this section is a list of all supplemental files that are available upon request. To obtain a copy of these files, contact the Dudley Knox Library located on the campus of the Naval Postgraduate School in Monterey, California. In all of the following, MRC refers to those scripts and functions required for maximal ratio combining analysis as described in Chapters III and IV. WPM refers to those scripts and functions required for wavelet packet modulation subchannel analysis, as described in Chapter V. Files without MRC or WPM in their file names are compatible with both types of simulations.

A. MATLAB SCRIPTS

- MRC_System.m
- WPM_System.m
- SMR_vs_BER.m
- Theory_MIMO_BER.m

B. MATLAB FUNCTIONS

- Analytic_SER.m
- Data_Symbols.m
- Decider.m
- Encoder.m
- MRC_Equalizer.m
- MRC_Mask_Calculator.m
- WPM_Equalizer.m
- WPM_Mask_Calculator.m

C. SUPPORTING DOCUMENTATION

- Readme.txt
- Gnu Radio Quick Start.pdf

LIST OF REFERENCES

[1] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge University Press, 2005.

[2] M. R. Cribbs, "Multiple-input multiple-output wavelet packet modulation based software-defined radio transceiver design," M.S. thesis, Dept. of Elect. and Comput. Eng., NPS, Monterey, CA, USA, 2015.

[3] E. Tollefson, B. R. Jordan Jr., and J. D. Gaeddert, "Out-phased array linearized signaling (OPALS): A practical approach to layer encryption," *IEEE Military Commun. Conf.*, Tampa, FL, 2015, pp. 294–299.

[4] G. Durgin, *Space-Time Wireless Channels*. Upper Saddle River, NJ, USA: Pearson Education, Inc., 2003.

[5] F. Ulaby and U. Ravaioli, *Fundamentals of Applied Electromagnetics*. Upper Saddle River, NJ, USA: Pearson Education, Inc., 2010.

[6] S. Rice, "Mathematical analysis of random noise," *AT&T Tech J*, vol. 23, pp. 282–332, July 1944.

[7] S. Goel, R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[8] C. E. Shannon, "Communication theory of secrecy systems," *AT&T Tech J*, vol. 28, no. 4, 656–715, 1949.

[9] T. S. Rappaport, *Wireless Communications*. Upper Saddle River, NJ, USA: Prentice Hall, Inc., 1996.

[10] S. M. Alamouti. "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[11] T. T. Ha, *Theory and Design of Digital Communication Systems*. New York, NY, USA: Cambridge University Press, 2011.

[12] B. Comar and S. Frazier. "Decoding and equalization for a joint Alamouti-MIMO and wavelet packet modulation system" [unpublished]. 2014.

[13] A. R. Lindsey. "Wavelet packet modulation for orthogonally multiplexed communication," *IEEE Trans. Signal Process*, vol. 45, no. 5, pp. 1336–1339, May 1997.

[14] The Wavelet Tutorial. (2017, Dec. 11). [Online]. Available: http://cseweb.ucsd.edu/~baden/Doc/wavelets/polikar_wavelets.pdf

[15] E. Okamoto, I. Yasunori, and I. Tetsushi. “Application of wavelet packet modulation to mobile communication,” *IEICE T Fund. Electr.*, vol. 87.10, 2004.

[16] A. Jamin and P. MA. Jamin and P. Mähönen. “Wavelet Packet Modulation for Wireless Communications,” *Wirel Commun Mob Com*., vol. 5, no. 2, March 2005.

[17] Alamouti STBC with 2 receive antenna. (2017, Nov. 27). [Online]. Available: http://www.dsplog.com/2009/03/15/alamouti-stbc-2-receive-antenna

[18] H. Shin and J. H. Lee. “Exact Symbol Error Probability of Orthogonal Space-Time Block Codes,” *Proc. IEEE GLOBECOM*, vol. 2, pp. 1197–1201, Nov. 2002.

[19] F. Kragh, “Wavelet packet modulation tutorial” [unpublished]. Feb. 2014.

[20] F. Kaltenberger, H. Jiang, M. Guillaud, R. Knopp, “Relative channel reciprocity calibration in MIMO/TDD systems,” *Future Network and MobileSummit Conf. Proc*., pp. 1–10, 2010.

[21] M. Guillaud, D. T. M. Slock, R. Knopp, “A practical method for wireless channel reciprocity exploitation through relative calibration,” *Proc. Int. Symp. Signal Process. Its Appl.*, 2005, pp. 403–406.

[22] A. Das and B. D. Rao. “SNR and noise variance estimation for MIMO systems,” *IEEE Trans. Signal Process.*, vol. 60, no. 8, pp. 3929–941, Aug. 2012.

[23] R. Sellin. “Gnu Radio quick start” [unpublished]. 2017.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California