Spring 5-25-2019

Physical Layer Security for Mimo Wireless Systems

Joseph R. Childress

PHYSICAL LAYER SECURITY

FOR MIMO WIRELESS

SYSTEMS

by

Joseph Raymond Childress, B.S.

A Thesis Presented in Partial Fulfillment
of the Requirements of the Degree
Master of Science

COLLEGE OF ENGINEERING AND SCIENCE
LOUISIANA TECH UNIVERSITY

May 2019

LOUISIANA TECH UNIVERSITY
GRADUATE SCHOOL

March 28, 2019
Date of thesis defense

We hereby recommend that the thesis prepared by

Joseph Raymond Childress, B.S.

entitled **PHYSICAL LAYER SECURITY FOR MIMO WIRELESS SYSTEMS**

be accepted in partial fulfillment of the requirements for the degree of

Master of Science in Engineering, Electrical Engineering Concentration

Dr. Chester Wilson, Supervisor of Thesis Research

Dr. Chester Wilson,
Head of Electrical Engineering

Members of the Thesis Committee:
Dr. Chester Wilson
Dr. Jinyuan Chen
Dr. Mickey Cox

Approved:

Hisham Hegab
Dean of Engineering & Science

Approved:

Ramu Ramachandran
Dean of the Graduate School

GS Form 13
(01/19)

ABSTRACT

A steadily growing portion of modern communication systems in use today is based on wireless technologies that make use of smaller and more portable electronic devices. As a result, the need to provide a light-weight security strategy for these systems is becoming a more important problem. This thesis focuses on two techniques that belong to an active research area known as Physical Layer Security (PLS). While the underlying techniques of PLS have been known for some time, the potential secrecy benefits of them need further investigation. These potential benefits have generated a rising interest with the development of Multiple Input Multiple Output (MIMO) multi-antenna systems. The first PLS technique considered in this thesis is that of beamforming which is made possible using MIMO. Here a sender can focus the information signal in the direction of the intended receiver while reducing the quality of the signal observed by a potential eavesdropper. In addition to beamforming, the technique of artificial noise (AN) is also investigated. AN requires the sender to generate a random noise signal in addition to the information signal to further degrade an eavesdropper's ability to detect and decode the information signal being

directed to the intended receiver. MATLAB simulations based on these PLS techniques are performed and the results presented.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Thesis. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Thesis. Further, any portions of the Thesis used in books, papers, and other works must be appropriately referenced to this Thesis.

Finally, the author of this Thesis reserves the right to publish freely, in the literature, at any time, any or all portions of this Thesis.

Author _____

Date _____

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BF	Beamforming
BSC	Binary Symmetric Channel
CSI	Channel State Information
CSIT	Channel State Information at the Transmitter
CVX	Convex Optimization
DMC	Discrete Memoryless Channel
IoT	Internet of Things
IP	Internet Protocol
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
MRC	Maximal Ratio Combining
OSI	Open Systems Interconnect
PHY	Physical
PLS	Physical Layer Security
QPSK	Quadrature Phase Shift Keying
RX	Receive

SDR	Software-Defined Radio
SIMO	Single Input Multiple Output
SISO	Single Input Single Output
SNR	Signal to Noise Ratio
SVD	Singular Value Decomposition
TCP/IP	Transmission Control Protocol / Internet Protocol
TX	Transmit
ZF	Zero-Forcing

ACKNOWLEDGEMENTS

First, I would like to express my appreciation to my advisor, Dr. Chester Wilson for his patience, guidance and support during my thesis work. I would also like to thank Dr. Jinyuan Chen for introducing me to the field of Physical Layer Security which became the focus of my graduate research culminating in the preparation of this thesis. In addition, I also wish to express my gratitude to Dr. Mickey Cox for his guidance and mentorship throughout my years of university study.

I also wish to express my deepest gratitude to my family for their endless love, support and understanding without which I would not have been able complete this thesis.

CHAPTER 1

INTRODUCTION

1.1 Physical Layer Security Explained

The need to deliver secure communications utilizing wireless systems is an increasingly complex challenge given both the broadcast nature of the wireless medium and the rapid advancements in technology available to potential eavesdroppers as shown in **Figure 1-1:** Typical Eavesdropper Scenario. To meet this challenge, system designers have traditionally leveraged cryptography implemented at the upper layers of the protocol stack. The computational resource-intensive nature of cryptography-based security however does not scale well when employed in devices which are continuously growing smaller in size and have reduced power constraints. Lighter weight security implementations will be needed for this new generation of smaller devices, especially as the proliferation of Internet of Things devices continues at an ever-increasing rate.

Physical Layer Security is an increasingly important research area in wireless communications. PLS is a collection of different security techniques that seek to exploit the random nature of wireless channels to either obscure the information being exchanged over the channel and/or provide a mechanism to generate private keys that can then be used to facilitate encrypted communications. This thesis focuses on the potential benefits of two areas of active PLS research, which are beamforming and artificial noise.

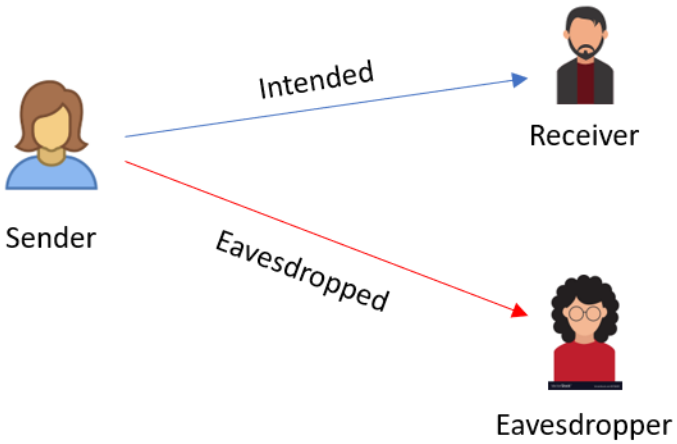

Figure 1-1: Typical Eavesdropper Scenario.

The concept of providing a level of secrecy to wireless communications is based on a field of study known as information theory, which was first introduced in a paper published by Claude Shannon in 1949 [1]. Among the ground-breaking ideas presented in this paper was the notion of perfect secrecy using a secret key-based cypher system shown in **Figure 1-2**.

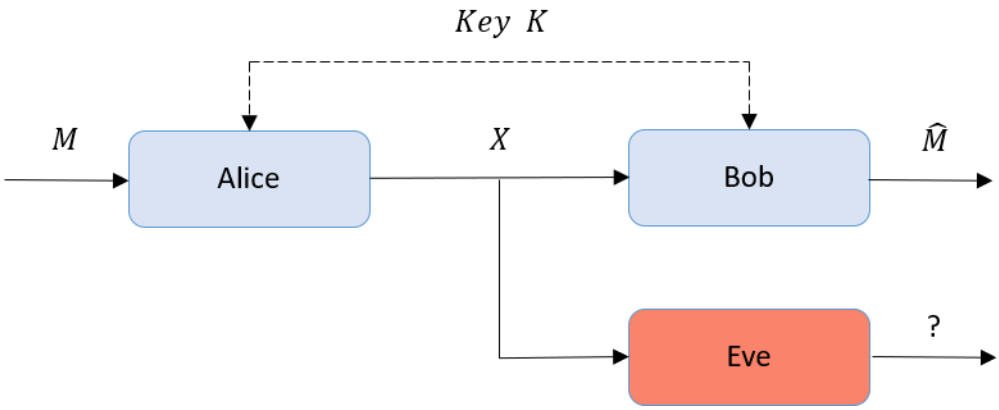

Figure 1-2: Shannon's Cipher System Model.

In Shannon's Cipher Model, the sender Alice encrypts a message M using a secret key K which is known to Bob but not the eavesdropper Eve. Since this model is

pessimistic, meaning it assumes the system contains no noise, both Bob and Eve receive the same cryptogram X. Bob can use the secret key K to decrypt the cryptogram to obtain $\widehat{M}$, which is a matching estimation of the original message M. Eve, on the other hand, is left to only guess the components of the original message since she has no knowledge of K.

Information theory provides a means to determine the capacity limits of communication systems. If a system can be designed such that the communication capacity between a sender and an intended receiver is measurably greater than that between the sender and a potential eavesdropper, the difference between their channel capacities will yield a measurable secrecy capacity where the eavesdropper is only able to detect and decode a portion of the overall original information signal. It is this concept that forms the basis of PLS.

Many recent developed wireless communication standards have incorporated MIMO technology. Using MIMO, system designers not only have found a means to engineer platforms that can provide system users with improved signal performance, but an even more interesting possibility of enhancing overall secrecy by exploiting the random nature of multi-channel MIMO systems.

In this thesis two different PLS techniques, namely beamforming and artificial noise generation, are investigated through a series of MATLAB simulations to better understand the potential secrecy benefits provided through the application of these techniques. The technique of beamforming can be broken down into two categories. The first is transmit beamforming, which involves the use of phase shifts of the transmitted signals across multiple antennas to focus the transmitted signals toward an intended

receiver while reducing the signal level transmitted in other directions. The second, called receive beamforming, makes use of spatial diversity to process the various received signals from multiple receive antennas resulting in an increased SNR at the receiver. The potential transmitter power reduction benefits from RX beamforming through Maximal Ratio Combining is also considered. Artificial noise generation is also analyzed to investigate its impact on secrecy between a transmitter and an intended receiver by generating additional artificial noise that is directed in directions other that of the intended receiver.

CHAPTER 2

BACKGROUND

2.1 Information-Theoretic Secrecy

2.1.1 Fundamentals of Information Security

In this section, the relevant background information within the topics of the information theory and MIMO communications are presented. These two topics are building blocks for PLS and the related PLS techniques investigated in this thesis.

The principles behind a receiver detecting a signal and successfully decoding it are rooted in information theory. Many of the principles in information theory involve random variables and their various outcome probabilities. Like a coin flip with its two possible outcomes being heads or tails, digital communication systems involve determining whether a 0 or a 1 was sent across a channel. A traditional model used to depict the probabilities of the outcomes associated with a communication system is that of the Binary Symmetric Channel shown in **Figure 2-1** [2].

The outcome of the BSC is a random variable with two possible outcomes, 0 or 1. This model simplifies the depiction of information being passed through a channel with potential for errors. The probability of making an incorrect estimation of the original value is represented by F. The error probability F is related to effects the actual physical communication channel has on the signals being passed through it.

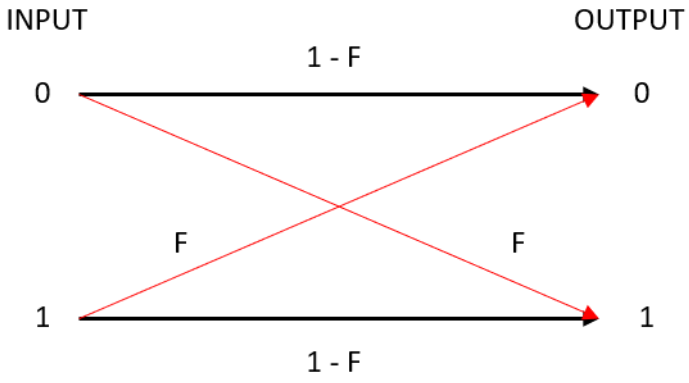

Figure 2-1: Binary Symmetric Channel Model.

2.1.2 Error Correction Coding

Since it is impractical to remove all source of errors from a communication system, system designers must implement solutions to compensate for them. A common technique known as error correction coding implements a coding scheme that can reduce the number of potential errors by adding in a level of redundancy into the encoded information or codeword [3]. A model for an error correction coding system is presented in **Figure 2-2**.

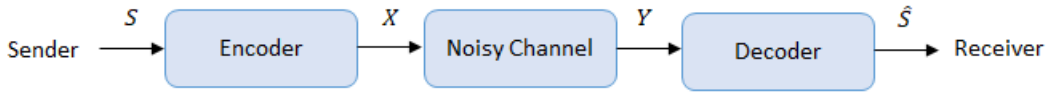

Figure 2-2: Error Correction Coding System Diagram.

The sender provides the original source information bits to the encoder that in turn maps the source information to a codeword that adds several redundant bits to the source bits. After the data is then passed through the noisy channel, the potential for error is presented. However, due to the redundant bits added by the encoder before transmission, the decoder removes the bits added for redundancy and the original source

information bits are recovered by the receiver. The presence of the redundant bits allows the decoder to overcome potential information bit errors. A common approach for error correction coding is to surround a single information bit with redundant identical bits, i.e. a single 0 source information bit may be encoded as 000 to increase the probability of a correct estimation of the original source bit 0 by the decoder. The spectral efficiency of the coding scheme is represented by the coding rate R which is defined as

$$R = \frac{K}{N} \qquad \textbf{Eq. 2-1}$$

where K represents the amount of source bits within the code compared to the total length of the code in bits represented by N.

2.1.3 Wyner's Wiretap Channel

In 1975, Wyner introduced a concept that is at the foundation of PLS called the wiretap channel model [4]. In this model, the wiretapper (referred to as the eavesdropper) attempts to intercept the information being passed between legitimate users by "tapping" the main channel between the users by means of a "wiretap" channel. During periods when the intended receiver's channel is "more reliable" than that of the eavesdropper, there is a measurable amount of information that can be securely shared between the sender and the intended receiver. Under this model, secrecy is solely provided by the exploitation of the random properties of the eavesdropper's wiretap channel. In [4], Wyner presented two cases of the wiretap channel, namely the special case and the general case.

Under the special case shown in **Figure 2-3**, the sender and the intended receiver communicates over a noiseless channel. The eavesdropper also receives the same communication through a memoryless BSC. The encoder is fed blocks of K bits from the

source represented as $S^K = (S_1,\cdots,S_K)$ which encodes S^K into a binary N vector $X^N = (X_1,\cdots,X_N)$ with length N. Wyner's wiretap channel considers error probability, transmission rate, and equivocation rate as important parameters.

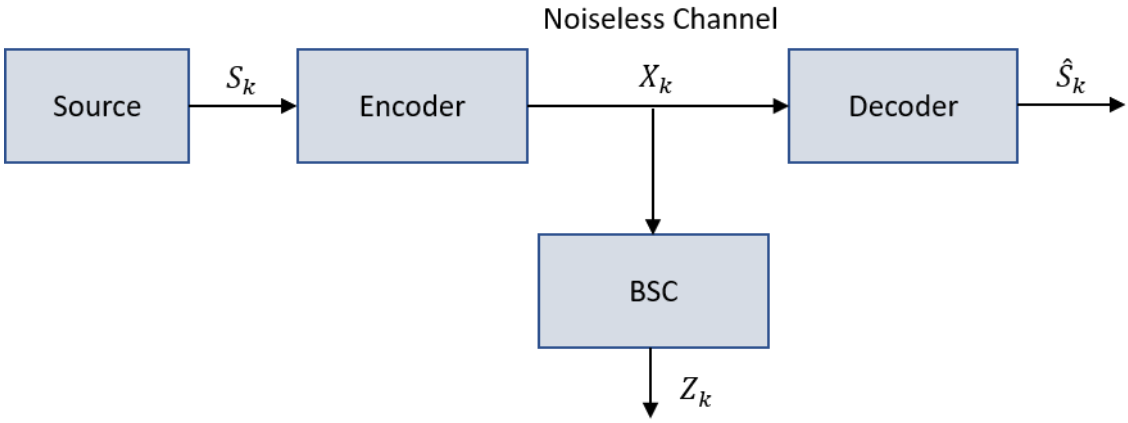

Figure 2-3: Wyner Wiretap Channel (special case) [4].

The error probability is

$$P_e = \frac{1}{K}\sum_{K=1}^{K} P_r\{S_K \neq \hat{S}_K\}. \qquad \textbf{Eq. 2-2}$$

The encoded sequence X^N is seen by the eavesdropper through the BSC (i.e. the wiretap channel). The bit flip probability is $p_0(0 < p_0 \leq \frac{1}{2})$. The output sequence through the wiretap channel

$$Z^N = (Z_1,\cdots,Z_N). \qquad \textbf{Eq. 2-3}$$

The channel's transmission rate is

$$R = \frac{K}{N} \qquad \textbf{Eq. 2-4}$$

measured in source bits per transmitted symbol. The equivocation rate which represents the degree of confusion on the part of the eavesdropper is defined as

$$\Delta = \frac{1}{K} H(S^K | Z^N). \quad \textbf{Eq. 2-5}$$

The objective is for the channel to provide a low error probability, high transmission rate along with a high equivocation rate.

Under the general case of Wyner's wiretap channel, the source's entropy is H_S and the main and wiretap channels are discrete and memoryless. Their respective transition probabilities are Q_M and Q_W,respectively. The error probability and the equivocation rate of the general case match those of the special case, however, the transmission rate does not. The transmission rate for the general case of Wyner's wiretap channel now includes the entropy of the source H_S. This results in the transmission rate for the general case being defined as

$$R = \frac{KH_s}{N} \quad \textbf{Eq. 2-6}$$

in source bits per transmitted symbol. As depicted in **Figure 2-4**, the source sends a binary message S^K through an encoder which produces a codeword X^N containing N bits. The codeword passes through the main channel where it is exposed to noise and other sources of error before being received as Y^N at the desired receiver. However, the eavesdropper receives an even greater degraded sample of Y^N through the wiretap channel resulting in Z^N being presented at the eavesdropper. It is important to consider that the wiretap channel ignores any assumptions about the computational capability of the eavesdropper and there are no actual encryption keys being exchanged between the sender and the intended receiver. The wiretap channel model relies solely on the parameters of the wireless channels themselves.

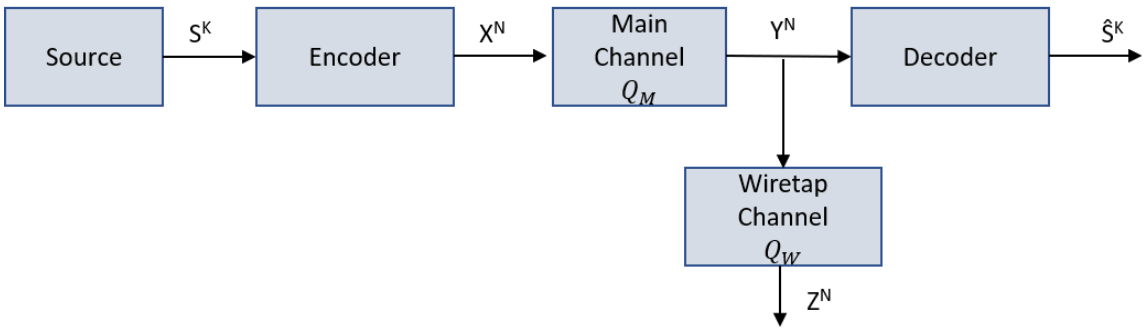

Figure 2-4: Wyner Wiretap Channel (general case) [4].

2.1.4 Wyner's Equivocation-Rate Region

In [4], Wyner presents a secrecy capacity region $\overline{R}$ depicted here in **Figure 2-5** for a pairing of transmission and equivocation rates (R, d). The rate R represents the rate that reliable communication can occur between Alice and Bob while the equivocation d is the level of confusion Eve experiences based on her observations of the communication message [5]. The region is defined as

$$\overline{R} \triangleq \{(R, d):\ 0 \leq R \leq C_M, \qquad 0 \leq d \leq H_s, \qquad Rd \leq H_s\Gamma(R)\} \qquad \textbf{Eq. 2-7}$$

The points on $\overline{R}$ where

$$R = C_M \qquad \textbf{Eq. 2-8}$$

outline where the transmission rate approaches the channel capacity for the main channel Q_M in Wyner's wiretap channel model. For points that lie along

$$d = H_s \qquad \textbf{Eq. 2-9}$$

represent a situation where the eavesdropper's equivocation approaches H_s corresponding to perfect secrecy [4]. The points along the line C_s represent the secrecy capacity of the channel pair (Q_M, Q_W) which are the main channel and the wiretap channel in Wyner's wiretap channel model. Wyner points out that a wiretap equivocation near

$$\frac{H_s \Gamma(C_M)}{C_M} \qquad \textbf{Eq. 2-10}$$

is achievable at this rate. Note that an increased equivocation requires a decreased transmission rate [4]. The point on $\overline{R}$ where the reliable transmission rate

$$R = \lim_{n\to\infty} \frac{1}{n} H(W) \qquad \textbf{Eq. 2-11}$$

is equal to the equivocation rate

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(W|Z^n) \qquad \textbf{Eq. 2-12}$$

where W is the message from Alice to Bob and Z^n contains the Eve's observations. This rate represents the highest rate that Eve gains no information at the message W. Wyner shows that when the input probability distribution is optimized, a maximum difference in mutual information is possible, represented as

$$\Gamma(R) = \sup_{p_{x\in P(R)}} I(X;Y|Z). \qquad \textbf{Eq. 2-13}$$

The point on $\Gamma(C_s)$ is the point at which the maximum transmission rate at which perfect secrecy is achieved [6].

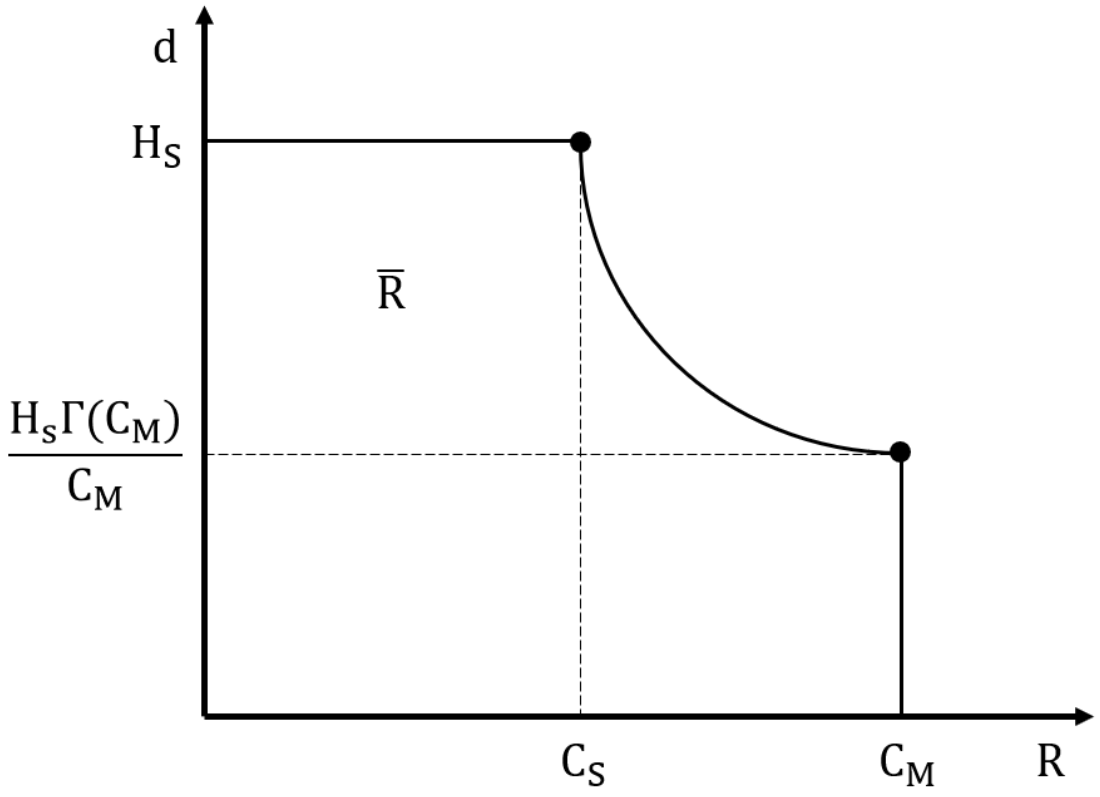

Figure 2-5: Wyner Achievable Wiretap Code Region [4].

2.1.5 Information Measurements

The measure of average information within a discrete random variable X having a probability distribution p_X is known as the entropy of X expressed as

$$H(X) = -\sum_{x \in X} p(x) \log p(x) \qquad \textbf{Eq. 2-14}$$

and is sometimes referred to as the degree of uncertainty about X [7]. Entropy is a fundamental concept of information theory and physical layer security [2].

Given two discrete random variables X and Y having a joint probability distribution p_{XY}, the joint entropy of X and Y is

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x,y) \qquad \textbf{Eq. 2-15}$$

and is representative of the degree of uncertainty regarding X and Y. Conditional entropy is the degree of uncertainty of X given Y and is defined as

$$H(X|Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(x|y) \qquad \textbf{Eq. 2-16}$$

Now that the concepts of entropy and conditional entropy have been introduced, the concept of mutual information can be presented. Mutual information represents a measure of the information which one random variable conveys about a different random variable.

For example, if Y is a sequence of observations made, the amount of information provided about a random variable X would yield an amount of information about X given Y. This is defined as

$$I(X;Y) = H(X) - H(X|Y). \qquad \textbf{Eq. 2-17}$$

As a result of symmetry, the following definition of

$$I(X;Y) = H(Y) - H(Y|X) \qquad \textbf{Eq. 2-18}$$

also exists. In addition, it is worth noting that

$$I(X;Y) = I(Y;X). \qquad \textbf{Eq. 2-19}$$

Building on this definition of mutual information, its relation to secrecy can be considered. The secrecy capacity [5] of the general wiretap channel is denoted as

$$C_s = \max_{p(u,x)} I(X;Y) - I(X;Z) \qquad \textbf{Eq. 2-20}$$

which defines the maximization of the mutual information difference between the mutual information between Alice and Bob and the mutual information between Alice and Eve. In addition, a DMC [2] capacity can be defined as

$$C = \max_{p(x)} I(X;Y). \quad \textbf{Eq. 2-21}$$

Under the weak secrecy constraint, the information transferred per-symbol must go to zero [8]. If X^n represents an encoded bit stream of length n sent by Alice and Z^n is the information observed by Eve, weak secrecy is given as

$$\lim_{n\to\infty} \frac{1}{n} I(X^n;Z^n) = 0. \quad \textbf{Eq. 2-22}$$

The strong secrecy constraint, however, requires that the entire information transferred to an eavesdropper goes to zero [8] and is defined as

$$\lim_{n\to\infty} I(X^n;Z^n) = 0. \quad \textbf{Eq. 2-23}$$

2.2 Multiple Input Multiple Output Wireless Communications

2.2.1 MIMO Benefits

Many wireless networks of today leverage MIMO multi-antenna array technology. The initial benefits gained from MIMO centered around increased data rates and increased SNR at distant receivers as a result of focusing the wireless signal in the direction of the intended receiver, i.e. beamforming.

MIMO systems can deliver significant performance improvements over traditional single antenna systems [9]. These improvements are attributed to various gains, namely array, diversity, and spatial multiplexing, as well as interference reduction.

2.2.2 Array Gain

An increase in average received SNR can be realized from array gain. Array gain involves adaptive processing utilizing multiple antennas to create a coherent combining effect [9]. The processing can be implemented by the transmitter and/or receiver. Channel state information knowledge at the transmitter or receiver is necessary for array gain.

Another factor is the total number of antennas employed at the transmitter and receiver. It is more practical to have CSI at the receiver than at the transmitter since obtaining CSIT requires a higher level of complexity in the system [10].

2.2.3 Diversity Gain

Diversity gain provides the benefit of increased resiliency against the negative effects of channel fading. Techniques used to achieve diversity gain are typically either spatial diversity or time/frequency diversity [9]. Spatial diversity is achieved using multiple antennas (i.e. multiple propagation paths), where the signal transmitted and received on each antenna can be combined to offset the fluctuations in signal power caused by fading. In the case of time/frequency diversity, additional transmission time or increased bandwidth is required since the information being sent must be sent over additional timeslots and/or frequencies.

2.2.4 Interference Resistance

Resistance to interference can be improved using MIMO as well. By processing the received signals received on each receive antenna, multi-antenna receivers can better filter out unwanted signals resulting from users of shared or reused channels [11]. However, to facilitate such selectivity, the receiver must have some level of channel knowledge for the signals it wants to preserve while minimizing all others [9].

2.2.5 Spatial Multiplexing

A multi-antenna system can also increase its information throughput compared to that of a SISO system since multiple antennas can be used to send separate bit streams across each antenna, utilizing parallel propagation paths and multiple channels. This is referred to as spatial multiplexing [12]. In this scenario, the receiver receives the multiple

data sequences and performs a merge of them allowing for an increase in spectral efficiency. For example, a MIMO system with three transmit antennas and three receive antennas would provide a three times improvement over a standard SISO system in terms of throughput.

There are four fundamental system models used when analyzing wireless communication systems, including MIMO. They are SISO, SIMO, MISO, and MIMO.

2.2.6 Single Input Single Output

The most basic antenna configuration is the SISO model as shown in **Figure 2-6**. In a SISO system, there exists a single transmit antenna and a single receive antenna. SISO provides no array gain or diversity gain since it is limited to a single propagation path.

Figure 2-6: Single Input Single Output 1 x 1 System Model.

2.2.7 Single Input Multiple Output

A SIMO system like the one depicted in **Figure 2-7**, incorporates multiple antennas at the receiver while maintaining a single antenna at the transmitter. With SIMO, the receiver must implement any multi-antenna processing techniques. To enhance the received signal strength, one option the receiver has is to utilize a voting strategy by which the signals detected by the various receive antennas are compared and the receiver can choose to process the instance with the strongest SNR. A second approach known as Maximal Ratio Combining involves the receiver combining the

signals received on each separate antenna in a manner that yields an increased overall SNR [13]. MRC is among the techniques further investigated in this thesis to better evaluate its potential for allowing reduced transmitter power while maintaining a desired SNR at the receiver.

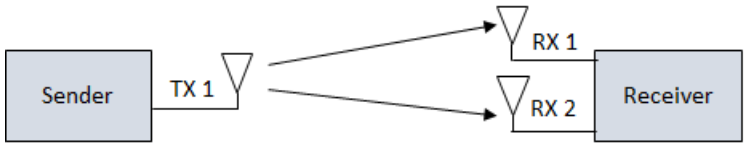

Figure 2-7: Single Input Multiple Output 1 x 2 System Model.

2.2.8 Multiple Input Single Output

Figure 2-8 presents the model for a 2 x 1 MISO system where the multiple antennas are now on the transmitter side of the system while the receiver has been reduced to using a single antenna. A common technique used in a MISO system is transmit beamforming allowing the transmitter to focus the power of the information signal in the direction of the desired receiver(s).

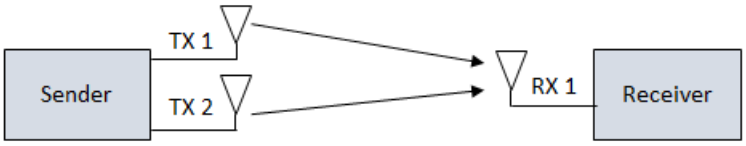

Figure 2-8: Multiple Input Single Output 2 x 1 System Model.

2.2.9 Multiple Input Multiple Output

The fourth and final model is shown in **Figure 2-9** and it is the MIMO system. The model depicted here is a 2 x 2 system where the transmitter and the receiver each have dual antennas resulting in a total of four wireless channels between them.

The MIMO model provides the highest increase in data rate compared to the previous models presented.

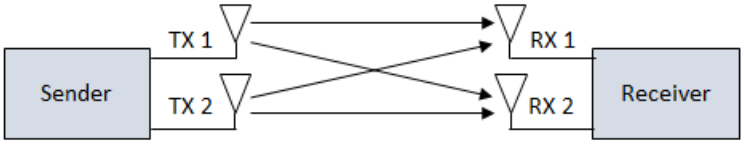

Figure 2-9: Multiple Input Multiple Output 2 x 2 System Model.

2.2.10 MIMO Channel

Considering a single-user MIMO channel with flat-fading, the channel model is defined as

$$\mathbf{y} = \mathbf{Hx} + \mathbf{n}. \qquad \textbf{Eq. 2-24}$$

Here, **y** represents the M_R x 1 received signal vector, **H** represents the M_R x M_T channel matrix containing the complex channel gains between the transmit and receive antennas, **x** represents the M_T x 1 transmitted signal vector and finally **n** represents the M_R x 1 AWGN vector [14]. It is common to assume flat-fading when analyzing wireless systems as this assumption serves to simplify the analysis.

2.2.11 Singular Value Decomposition

The channel capacity of a MIMO system can be obtained using a linear algebra analysis technique known as Singular Value Decomposition [15]. SVD provides a mechanism such that the MIMO channel matrix **H** can be decomposed into several parallel spatially-diverse SISO channels. **Figure 2-10** depicts the SVD process for a MIMO system. The total number of channels resulting from the decomposition of **H** is equal to the rank of **H.** Given a MIMO channel model

$$\mathbf{y} = \mathbf{Hx} + \mathbf{n}, \qquad \textbf{Eq. 2-25}$$

the SVD of **H** is

$$\mathbf{H} = \mathbf{U\Phi V}^{\mathrm{H}} \qquad \textbf{Eq. 2-26}$$

where **U** is the M_R x M_R unitary matrix, **V** is the M_T x M_T unitary matrix, and Φ is the M_R x M_T diagonal matrix consisting of singular values of matrix **H** in descending order [16].

$$\mathbf{\Phi} = \begin{bmatrix} \boldsymbol{\lambda_1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\lambda_2} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \ddots & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \boldsymbol{\lambda_{M-1}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{\lambda_M} \end{bmatrix} \qquad \textbf{Eq. 2-27}$$

where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{M-1} \geq \lambda_M$. Given CSIT exists, a precoding scheme can be applied to the information data stream vector **x** prior to transmission such that the transmitted symbols are

$$\mathbf{s} = \mathbf{Vx} \qquad \textbf{Eq. 2-28}$$

The resulting received signal vector **z** is comprised of a post-multiplication of **y** and $\mathbf{U}^{\mathrm{H}}$ such that

$$\mathbf{z} = \mathbf{U}^{\mathrm{H}}\mathbf{y} \qquad \textbf{Eq. 2-29}$$

and to simplify further

$$\mathbf{z} = \mathbf{U}^{\mathrm{H}}(\mathbf{Hs} + \mathbf{n}) \qquad \textbf{Eq. 2-30}$$

$$\mathbf{z} = \mathbf{U}^{\mathrm{H}}(\mathbf{H}(\mathbf{Vx}) + \mathbf{n}) \qquad \textbf{Eq. 2-31}$$

$$\mathbf{z} = \mathbf{U}^{\mathrm{H}}(\mathbf{U\Phi V}^{\mathrm{H}}(\mathbf{Vx}) + \mathbf{n}) \qquad \textbf{Eq. 2-32}$$

$$\mathbf{z} = \mathbf{U}^{\mathrm{H}}(\mathbf{U}\boldsymbol{\Phi}\mathbf{V}^{\mathrm{H}}(\mathbf{V}\mathbf{x}) + \mathbf{n}) \qquad \textbf{Eq. 2-33}$$

$$\mathbf{z} = \boldsymbol{\Phi}\mathbf{x} + \mathbf{U}^{\mathrm{H}}\mathbf{n} \qquad \textbf{Eq. 2-34}$$

$$\mathbf{z} = \boldsymbol{\Phi}\mathbf{x} + \bar{\mathbf{n}}. \qquad \textbf{Eq. 2-35}$$

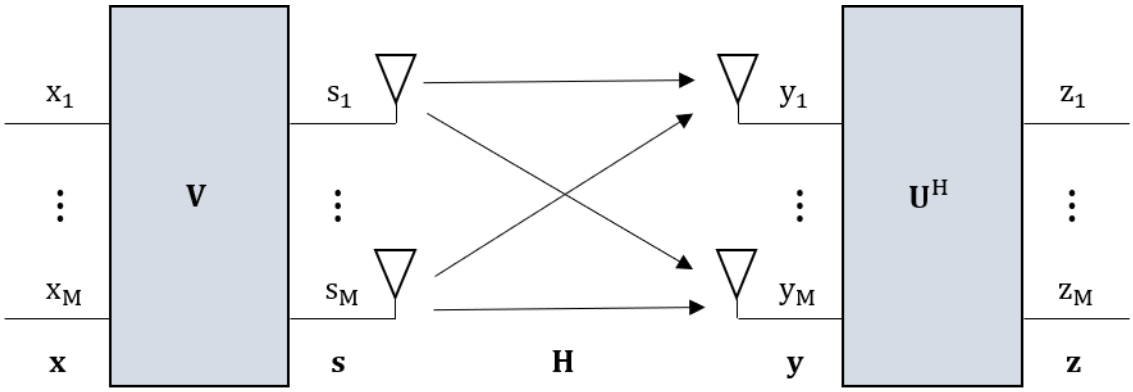

Figure 2-10: SVD Decomposition of MIMO Channel [15].

CHAPTER 3

PHYSICAL LAYER SECURITY

3.1 Physical Layer Security Overview

Physical Layer Security is an active research topic that aims to provide an increased level of security in communications systems outside of traditional computational security methods based on cryptography. PLS stands to provide the most benefit from a security perspective in the area of wireless communications due to the secrecy concerns resulting from the broadcast nature of the wireless medium. Researchers seek to better understand the degree of secrecy that can be realized through PLS by exploiting the physical properties of wireless channels. Traditionally in wireless communications, the random nature of wireless channels resulting from noise, fading, and interference were viewed as negative, degrading effects [17]. However, PLS can leverage these effects to provide a more favorable channel to an intended receiver while ensuring a degraded, less desirable channel to a potential eavesdropper.

With the arrival of Multiple Input Multiple Output technologies, the interest in PLS has been steadily increasing over the past decade or so. MIMO, which was presented in the previous chapter, provides system designers with additional channels to work with as a result of the presence of multiple transmit and receive antennas. Using these additional channels, PLS provides a means to not only focus the energy of information bearing signals in the direction of an intended receiver but can also leverage these

channels to obscure the information bearing signal from eavesdroppers. MIMO combined with PLS techniques have garnered much consideration as an improved security strategy for smaller devices. Lighter weight security implementations will be needed for next generation smaller devices, especially in IoT, where extreme power limitations prevent the use of traditional computationally complex encryption algorithms.

This chapter discusses PLS in more depth including where the physical layer fits into the larger data communication protocol architecture and presents various PLS techniques based on multi-antenna systems.

3.2 The TCP/IP Protocol Layered Architecture

Modern digital communication protocols are fundamentally based on a layered protocol architecture (or stack) known as the Open Systems Interconnect model. Under the OSI reference model, each layer provides specific functionality which serves the adjacent layers. A derivative of the OSI model is the TCP/IP protocol suite shown in **Figure 3-1**. As shown, the TCP/IP stack consists of the following five layers (from top to bottom): Application, Transport, Network, Data Link, and Physical.

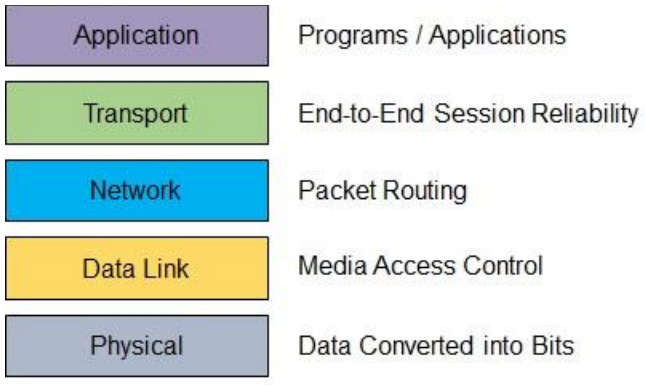

Figure 3-1: TCP/IP Communications Protocol Stack.

3.2.1 Application Layer

The Application layer is the most familiar since the various computer applications users interact with communicate at this layer, such as web browsers, email programs, and video conferencing programs. This layer serves as the “doorway” by which user applications share data over a communication network.

3.2.2 Transport Layer

The Transport layer helps to ensure reliable communication occurs. It provides connection-oriented and connectionless-oriented communications between hosts. Sessions between communicating hosts are tracked and managed at this layer ensuring incoming datagrams are delivered to the appropriate application through the layer above.

3.2.3 Network Layer

The task of routing packets of data across communication networks is the primary function of the Network layer. This layer utilizes IP addressing to determine the source and destination of data packets and forwards the packets through the network determining and utilizing the most efficient path available.

3.2.4 Data Link Layer

The layer directly beneath the Network layer is the known as the Data Link layer. At this layer, the primary concern is controlling access onto the communication medium [18] similar in manner to traffic signals at an intersection. Network congestion is managed at this layer. The network medium would experience significant packet collisions resulting in high error rates without this layer.

3.2.5 Physical Layer

The Physical layer provides an interface between the upper layer protocols and the physical communication medium such as electrical, optical, wireless, etc. The encoding and transmission of data over the medium is the main purpose of the PHY layer [18].

Figure 3-2 depicts security mechanisms which are commonly applied at the layers above the PHY layer. However, the PHY layer was not considered when the current security schemes, based on cryptographic techniques, were developed. PLS aims to address this lack of security at the PHY layer in the overall goal of achieving a complete security architecture with secrecy components present at every layer.

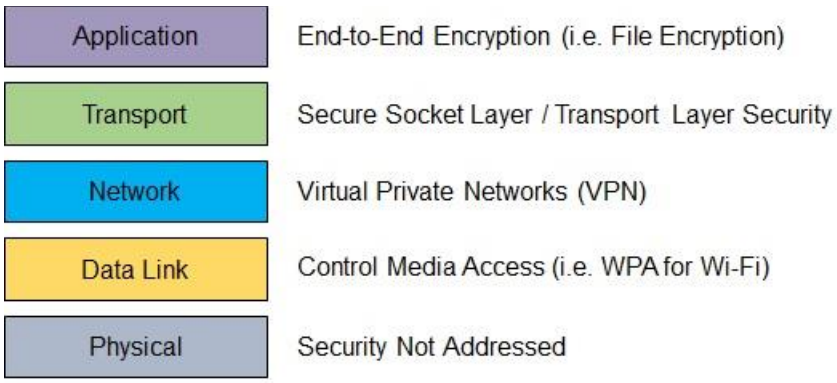

Figure 3-2: Security Implemented at Upper TCP/IP Layers.

3.3 Physical Layer Security Multi-Antenna Techniques

3.3.1 PLS Techniques Discussed

This section presents a four PLS techniques that utilize multiple antennas, two of which are further investigated in future chapters. These PLS techniques include beamforming, artificial noise, zero-forcing [19], and convex optimization.

3.3.2 Beamforming

The objective with beamforming, as it relates to PLS, is to provide the intended receiver Bob with a better SNR than that observed by the eavesdropper Eve. A more thorough discussion of beamforming is presented in the next chapter.

3.3.3 Artificial Noise

The technique of artificial noise entails the sender Alice generating AN and transmitting that noise in all directions other than in the direction of the intended receiver Bob. Alice can improve the overall effect of the AN on Eve if CSI for Eve's channel is known to Alice, which typically does not apply in the case of a passive eavesdropper. Artificial noise is covered more in depth in chapter 5.

3.3.4 Zero-Forcing

For the ZF approach, Alice transmits the information signal into the null space of Eve, requiring some level of knowledge of Eve's channel to perform the necessary precoding and to minimize Eve's capacity [20]. Zero-forcing is also known as null-space beamforming [21]. The objective when employing ZF is to reduce to signal level observed at Eve to zero such that the following condition is satisfied

$$\mathbf{h}_e\mathbf{w}^{\mathrm{H}} = 0 \qquad \textbf{Eq. 3-1}$$

where $\mathbf{h}_{\mathrm{e}}$ represents Eve's channel vector and $\mathbf{w}^{\mathrm{H}}$ represents the null-space beamforming vector [21].

3.3.5 Convex Optimization

Precoding based on CVX can be used to maximize the secrecy capacity by maximizing the capacity difference between Bob and Eve. It can be used along with ZF and AN schemes in situations where there is limited CSI [21].

CHAPTER 4

BEAMFORMING: THEORY AND SIMULATION

4.1 Beamforming for PLS

In this chapter, the PLS beamforming techniques of both transmit and receive beamforming are further considered. MATLAB simulations of MISO and SIMO systems are performed, and the results analyzed. The impact on the BER experienced by a potential eavesdropper is demonstrated through these simulations. Also demonstrated is the transmitter power reduction potential of RX beamforming.

4.2 Transmit Beamforming

The objective with beamforming, as it relates to PLS, is to ensure the intended receiver Bob has a better SNR than that observed by the eavesdropper Eve [22]. In transmit beamforming, the signal is steered towards the desired receiver by multiplying the information symbols sent across each transmit antenna by the complex conjugate of the desired receiver's channel. This results in the multiple signals being received at the desired receiver being combined in a manner that increases the receiver's SNR [23].

Figure 4-1 presents the model for the masked beamformer scheme used in the TX beamforming simulations in this thesis. Rayleigh flat-fading is assumed.

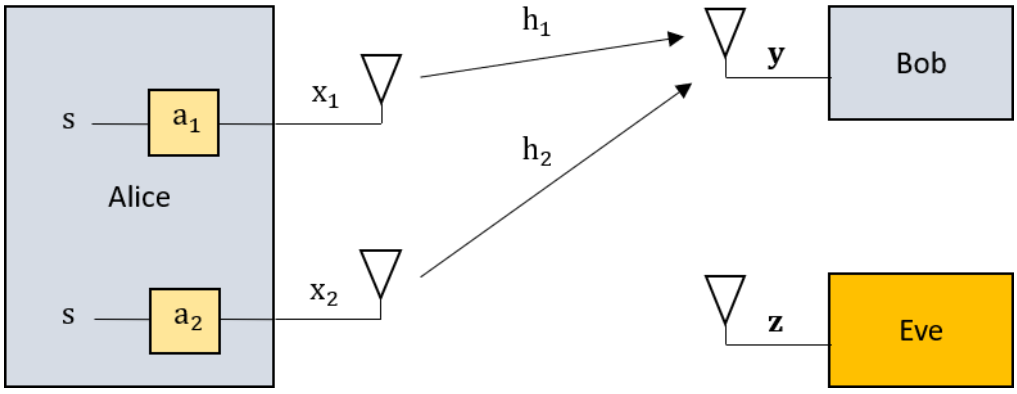

Figure 4-1: Transmit Beamformer Simulation Model.

In this TX beamforming scenario, Alice uses two transmit antennas to beamform the information bearing signal to Bob where Bob and Eve both are employing a single receive antenna [23]. Alice transmits the information signal as

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 s \\ a_2 s \end{bmatrix} \qquad \textbf{Eq. 4-1}$$

where **x** is the transmitted signal vector containing the products of the information symbols and the beamforming weights generated by Alice based on Bob's CSI transmitted across the corresponding transmit antenna in Alice's multiantenna array.

Bob's channel matrix **H** contains the complex channel coefficients h_1 and h_2 and the signal received at Bob becomes

$$y = \begin{bmatrix} h_1 & h_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n \qquad \textbf{Eq. 4-2}$$

$$y = h_1 x_1 + h_2 x_2 + n \qquad \textbf{Eq. 4-3}$$

$$y = h_1 a_1 s + h_2 a_2 s + n \qquad \textbf{Eq. 4-4}$$

$$y = \frac{h_1 h_1^* s}{|h_1|} + \frac{h_2 h_2^* s}{|h_2|} + n. \quad \textbf{Eq. 4-5}$$

Since the beamforming phase shifts are

$$a_1 = \frac{h_1^*}{|h_1|} \quad \textbf{Eq. 4-6}$$

and

$$a_2 = \frac{h_2^*}{|h_2|} \quad \textbf{Eq. 4-7}$$

respectively, Bob's received signal simplifies to

$$y = (|h_1| + |h_2|)s + n. \quad \textbf{Eq. 4-8}$$

4.3 Transmit Beamforming Simulation Results

In **Figure 4-2**, a comparison of a SISO system with a 2 x 1 MISO system using transmit beamforming is presented. This simulation uses QPSK modulation and illustrates that transmit beamforming based on Bob's CSI can yield an improved BER for Bob while Eve's BER remains no better than that of the theoretical SISO performance. The resulting SNR gap between Bob and Eve supports the concept of using transmit beamforming to provide a measurable level of secrecy between Alice and Bob compared to that between Alice and Eve. The resulting plots also suggest that as the SNR values increase, this SNR gap continues to increase, further enhancing the potential secrecy available between Alice and Bob.

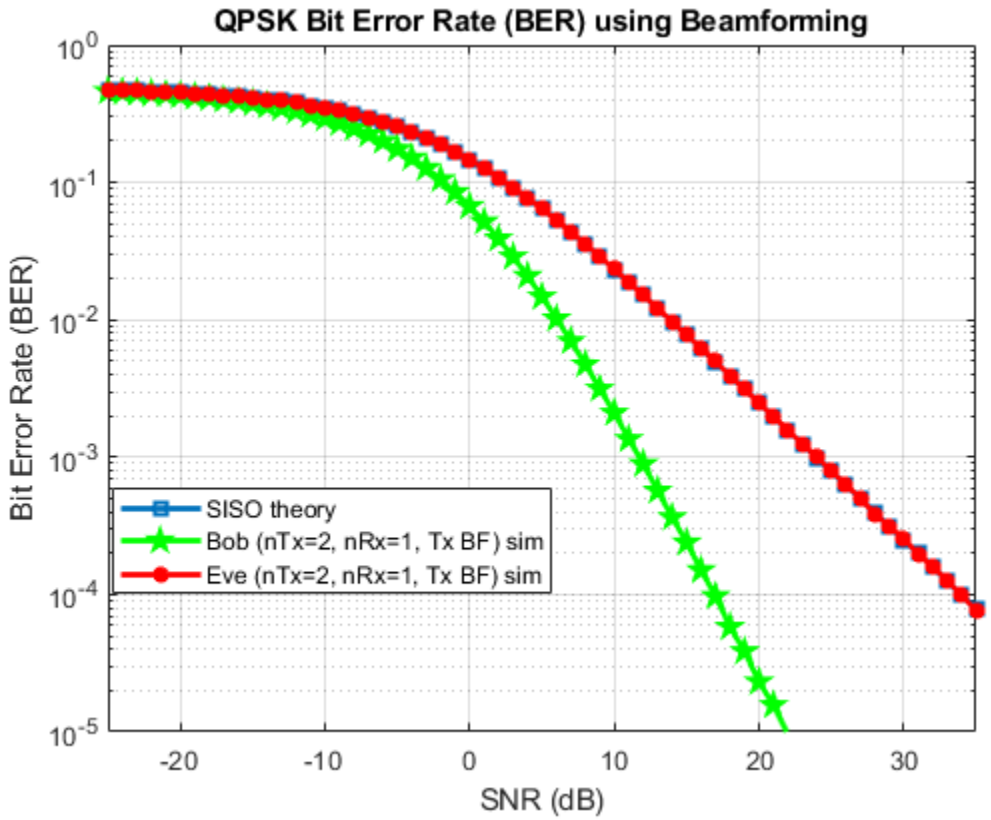

Figure 4-2: BER Simulation Plots for Bob and Eve with SISO Theory Comparison.

Figure 4-3 further illustrates this point. Here the BER results of both Bob and Eve are presented for the 2 x 1 MISO case where transmit beamforming is employed as well as when no beamforming is used. Eve's performance remains the same with and without beamforming across the entire plotted SNR range. This is expected since the transmit beamforming employed by Alice is based on Bob's CSI and, as a result, Eve reaps no benefit from the beamforming while Bob experiences a significant gain in performance from Alice's beamforming. Again, the SNR gap yields an increasing level of secrecy between Alice and Bob. Eve's BER, for example, is more than two orders of magnitude larger than that of Bob's at an SNR of 20 dB.

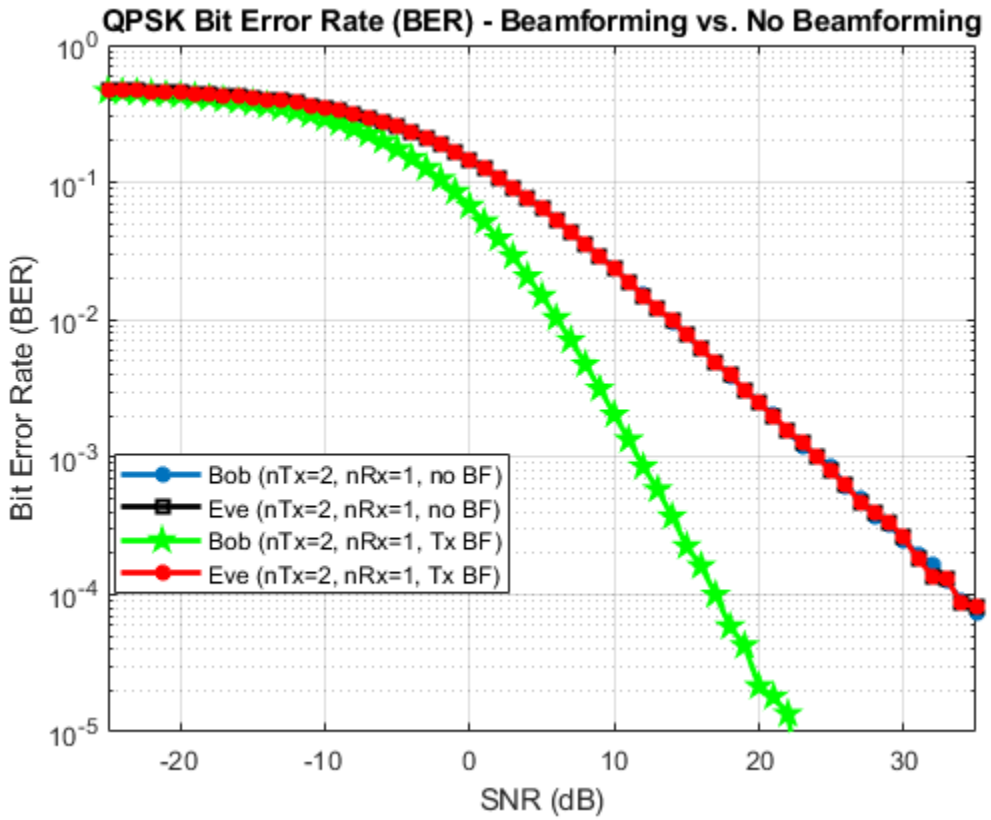

Figure 4-3: BER Simulation Plots for Bob and Eve with and without TX Beamforming.

4.4 Receive Beamforming and MRC

4.4.1 Receive Beamforming

In this section, receive beamforming (i.e. receive diversity) is presented where the beamforming processing is performed at the receiver instead of the transmitter. Received signals are combined to improve the overall SNR at the receiver. A signal processing technique known as Maximal Ratio Combining can be used when a receiver has multiple antennas [24].

Because the receiver has multiple antennas, the receiver detects the transmitted signal through multiple paths [25]. The receiver processes the quality of the signals from

each path weighting them accordingly. The multiple signals are then co-phased before being summed in phase maximizing the diversity gain [26]. The resulting combined signals are then passed to the demodulator. The signal received on the i^{th} antenna is generally defined as

$$\mathbf{y_i} = h_i x + n_i \qquad \textbf{Eq. 4-9}$$

where $\mathbf{y_i}$ is the symbol received on the i^{th} antenna, h_i represents the channel complex coefficients for the i^{th} antenna's channel, x is the original symbol transmitted, and finally the AWGN noise on the i^{th} antenna is n_i [24].

The combined signal becomes

$$\mathbf{y} = \mathbf{h}x + \mathbf{n}. \qquad \textbf{Eq. 4-10}$$

Considering the 1 x 2 MRC simulation presented in the next section, the received symbol vector becomes

$$\mathbf{y} = [y_1 \quad y_2]^T. \qquad \textbf{Eq. 4-11}$$

The channel for the two receive antennas becomes

$$\mathbf{h} = [h_1 \quad h_2]^T \qquad \textbf{Eq. 4-12}$$

with the AWGN noise vector being

$$\mathbf{n} = [n_1 \quad n_2]^T. \qquad \textbf{Eq. 4-13}$$

Following equalization, the resulting symbol is given as

$$\hat{x} = \frac{\mathbf{h}^H\mathbf{y}}{(|h_1|^2 + |h_2|^2)} = \frac{\mathbf{h}^H\mathbf{h}x}{(|h_1|^2 + |h_2|^2)} + \frac{\mathbf{h}^H\mathbf{n}}{(|h_1|^2 + |h_2|^2)} \qquad \textbf{Eq. 4-14}$$

which reduces to

$$\hat{x} = x + \frac{\mathbf{h}^{H}\mathbf{n}}{(|h_1|^2 + |h_2|^2)} \qquad \textbf{Eq. 4-15}$$

after simplifying**.**

4.4.2 Maximal Ratio Combining for Reduced Transmitter Power

With the proliferation of smaller portable IoT devices that commonly have limited power constraints, the possibility of employing RX beamforming techniques like MRC to maintain an acceptable BER at a reduced SNR is of interest.

An MRC simulation is performed to better demonstrate the potential of using MRC to provide a desired BER at a lower SNR. As in the transmit beamforming simulations, Rayleigh flat-fading is again assumed.

4.4.3 Maximal Ratio Combining Simulation Results

In **Figure 4-4**, results from a simulation incorporating MRC is presented. The BER performance for an intended receiver in a 2 x 1 MISO transmit beamforming case is compared to a case of a 1 x 2 SIMO system using MRC. The theoretical results for a 2 x 1 SIMO system are also plotted for comparison. The matching BER performance observed by the receiver from both transmit beamforming and MRC supports the theory that the transmitter could simply employ a single transmit antenna instead of multiple transmit antennas with transmit beamforming. Transmit beamforming increases the complexity of the transmitter resulting in increased processing requirements. A higher processing complexity typically means increased power consumption by the transmitter. The results from this simulation suggests that a receiver can leverage MRC to reduce the complexity at the transmitter. This approach could further increase the operational reliability of small IoT devices with limited battery capacity.

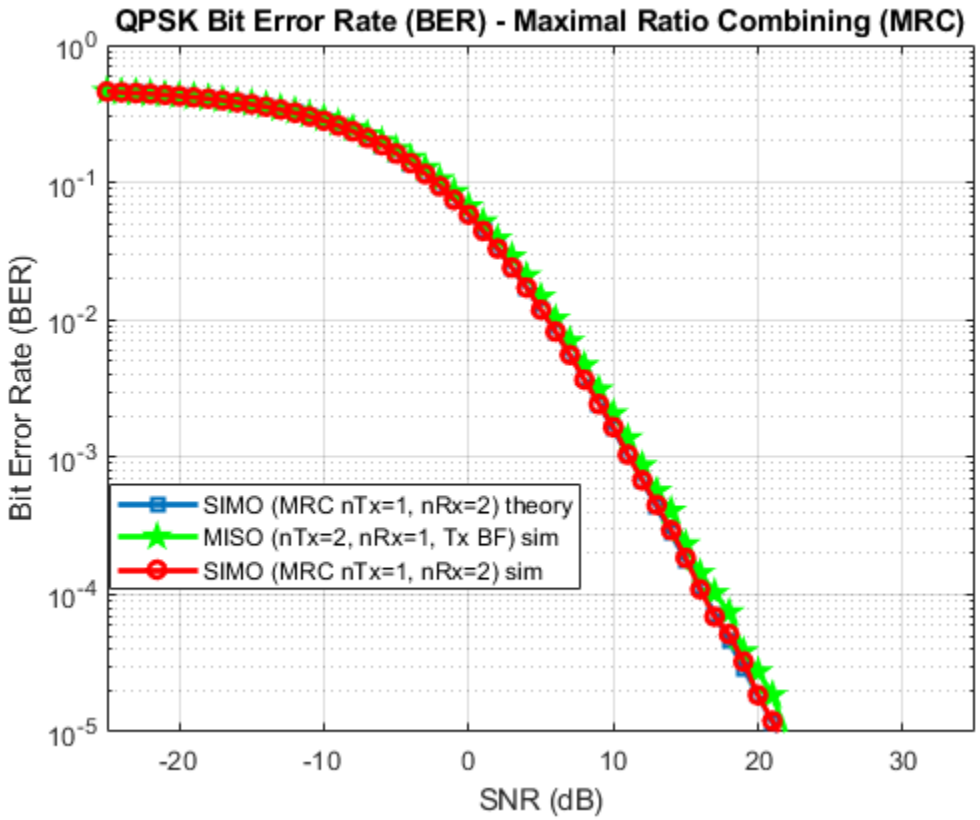

Figure 4-4: BER Simulation Plots for Maximal Ratio Combining compared to MISO TX Beamforming.

CHAPTER 5

ARTIFICIAL NOISE: THEORY AND SIMULATION

5.1 Artificial Noise for PLS

In this chapter, the PLS technique called artificial noise generation is further investigated. MATLAB simulations of a MISO system with a range of power allocations applied to AN are performed. The impact on the BER experienced by a potential eavesdropper is demonstrated through these simulations.

5.2 Artificial Noise

The technique of artificial noise entails the sender Alice generating artificial noise and transmitting that noise in all directions other than in the direction of the intended receiver Bob. Alice can improve the overall effect of the AN on Eve if channel state information for Eve's channel is known to Alice, which typically does not apply in the case of a passive eavesdropper. The desired result of generating AN is to degrade the channel of potential eavesdroppers while at the same time not impacting the quality of the channel of the intended receiver [27]. It is important to note that even in a scenario where Eve's SNR is increased, the secrecy provided will remain since the increased SNR of Eve will not only provide her with a stronger information signal but with increased artificial noise observed by her as well.

Utilizing the transmit beamforming model in Figure 4.1, a series of AN simulations performed in this thesis make use of a precoding scheme presented in [27] where the sender Alice has two transmitting antennas, while the intended receiver Bob and the eavesdropper Eve each have a single receive antenna. Both Bob's and Eve's respective received signals are derived in this section. In these simulations, the sender Alice sends the signal

$$\mathbf{x}_k = \mathbf{a}_k\mathbf{s}_k + \mathbf{w}_k \qquad \textbf{Eq. 5-1}$$

with $\mathbf{x}_k$ representing the complex Gaussian symbol vector, $\mathbf{a}_k$ is a beamforming weight, $\mathbf{s}_k$ being the information signal, and $\mathbf{w}_k$ being the complex Gaussian vector of the AN being generated by Alice. The condition defined by

$$\mathbf{H}_k^H\mathbf{w}_k = 0 \qquad \textbf{Eq. 5-2}$$

is satisfied by Alice choosing $\mathbf{w}_k$ such that it lies within the null-space of $\mathbf{H}_k^H$ which is the conjugate transpose of Bob's channel matrix $\mathbf{H}_k$.

Bob's received signal is

$$\mathbf{y}_k = \mathbf{H}_k^H\mathbf{x}_k + \mathbf{n}_k \qquad \textbf{Eq. 5-3}$$

$$\mathbf{y}_k = \mathbf{H}_k^H(\mathbf{a}_k\mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k \qquad \textbf{Eq. 5-4}$$

$$\mathbf{y}_k = \mathbf{H}_k^H\mathbf{a}_k\mathbf{s}_k + \mathbf{n}_k. \qquad \textbf{Eq. 5-5}$$

As is seen, the AN-related component has disappeared in the signal received by Bob. In comparison, the signal observed by Eve is

$$\mathbf{z}_k = \mathbf{G}_k^H\mathbf{x}_k + \mathbf{e}_k \qquad \textbf{Eq. 5-6}$$

$$\mathbf{z}_k = \mathbf{G}_k^H(\mathbf{a}_k\mathbf{s}_k + \mathbf{w}_k) + \mathbf{e}_k \qquad \textbf{Eq. 5-7}$$

$$\mathbf{z}_k = \mathbf{G}_k^H \mathbf{a}_k \mathbf{s}_k + \mathbf{G}_k^H \mathbf{w}_k + \mathbf{e}_k \quad \textbf{Eq. 5-8}$$

where the AN represented by $\mathbf{G}_k^H \mathbf{w}_k$ remains in the signal received by Eve significantly reducing the quality of Eve's channel $\mathbf{G}_k$. Bob on the other hand does not see the AN component since the AN vector $\mathbf{w}_k$ lies in his null-space, conditioning the AN to impact potential eavesdroppers including Eve in all subspaces other than Bob's.

In terms of the amount of total transmission power allocated to the generation of AN versus the information signal, the transmitted signal is given by

$$\mathbf{x}_k = \sqrt{(1 - r)}\mathbf{s}_k + \sqrt{r}\mathbf{w}_k \quad \textbf{Eq. 5-9}$$

where r is the ratio of the amplitude of the AN compared to the total amplitude of the transmitted signal. The AN simulation results are presented in the next section.

5.3 Artificial Noise Simulation Results

In **Figure 5-1**, the simulation results are given for a 2 x 1 Multiple Input Single Output system where the percentage of total transmit power allocated to AN generation is set at 20%. This figure shows that Eve's BER is considerably increased from a mere 20% of the power being used for AN compared to her BER when no AN is generated. While Eve's BER was already increasingly higher than Bob's BER for SNR regime above 0 dB as a result of the TX beamforming by Alice, the complimentary effects from the presence of AN is shown. Eve's BER, for instance, at an SNR of 20 dB has increased from approximately $10^{-2.5}$ to 10^{-1} and, in fact, appears to approach a limit of 10^{-1} for all SNR values above 10 dB. In Eve's case, higher SNR values, while increasing the observed SNR for the information-bearing signal, the SNR of the AN is also increased leaving Eve without no benefit from the higher SNR regime. Bob's BER, on the other

hand, is slightly affected due to the AN being generated based on Bob's CSI. This is not due to the AN directly but that the portion of total transmit power allocated to the information-bearing signal has decreased to 80% versus 100% when no AN is generated.

If the power allocation to AN is increased even further, as is the case in **Figure 5-2**, **Figure 5-3**, and **Figure 5-4**, the BER of Eve continues to increase reaching $10^{-0.5}$ in the instance where the AN power allocation is 80%. However, the decreasing information-bearing signal power allocation also begins to impact Bob's BER as well. This is highly visible in Figure 5.4 where Bob's BER is higher than Eve's BER when no AN is applied for SNR values below 10 dB.

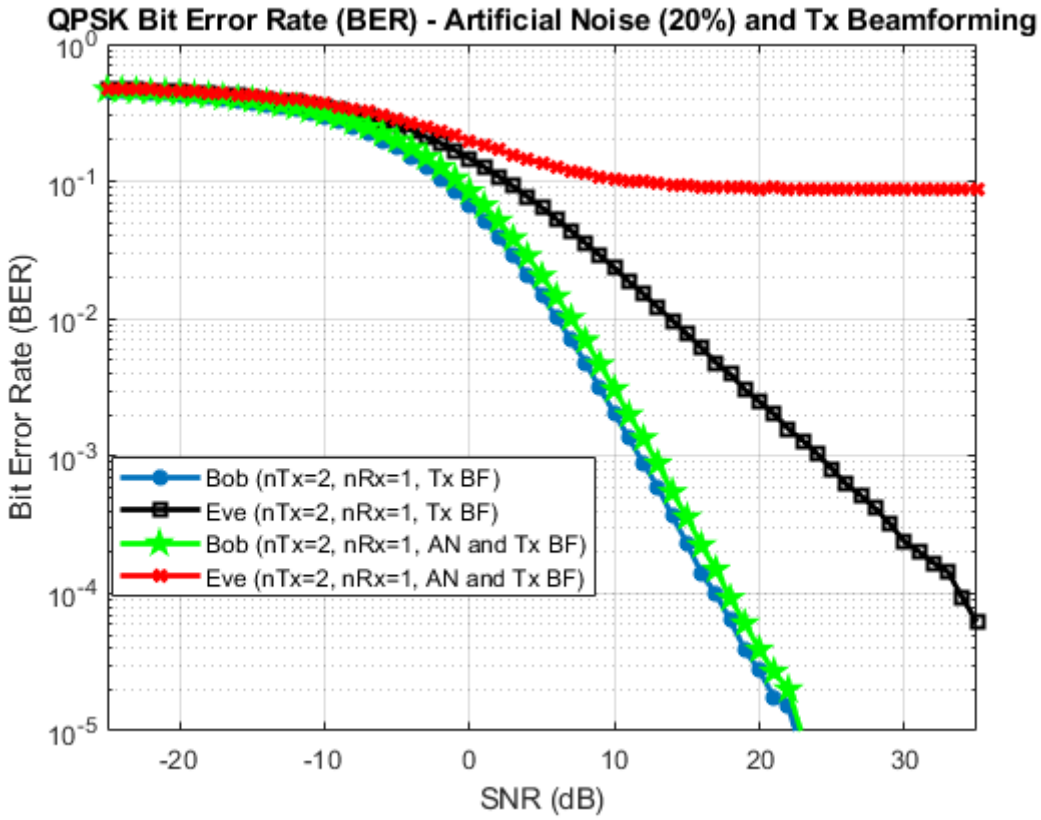

Figure 5-1: BER Simulation Plots for Bob and Eve with TX Beamforming and Artificial Noise at 20% of Total Transmit Power.

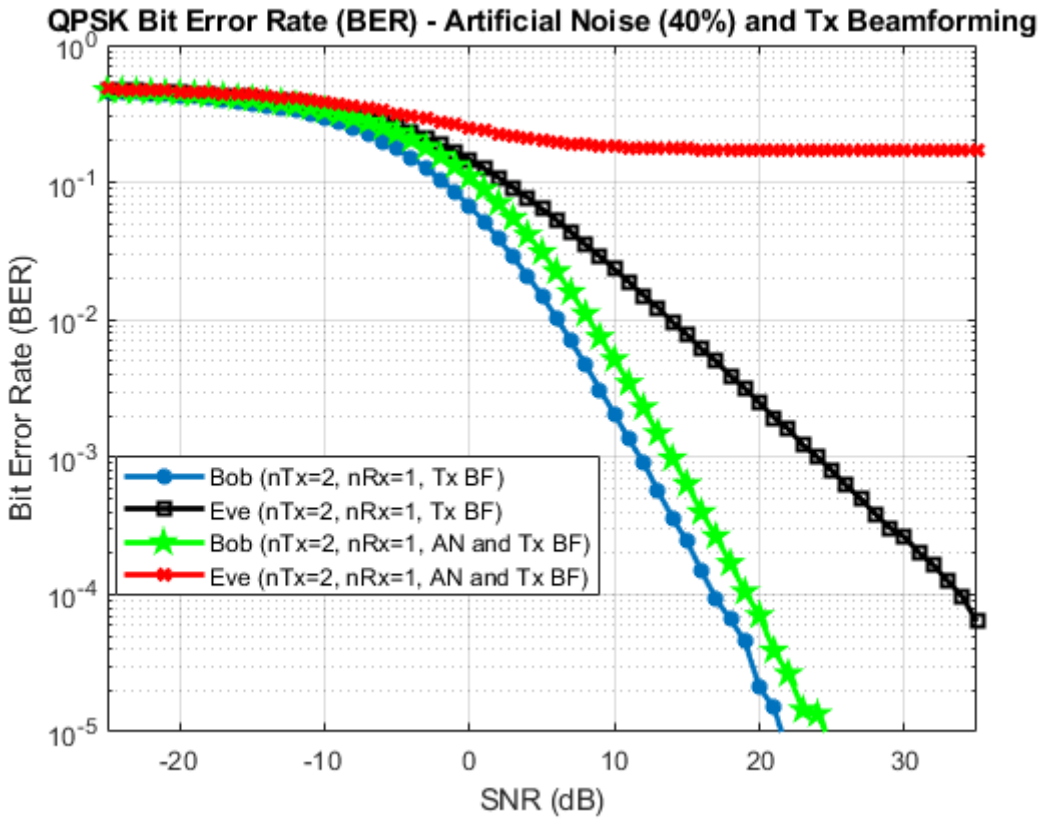

Figure 5-2: BER Simulation Plots for Bob and Eve with TX Beamforming and Artificial Noise at 40% of Total Transmit Power.

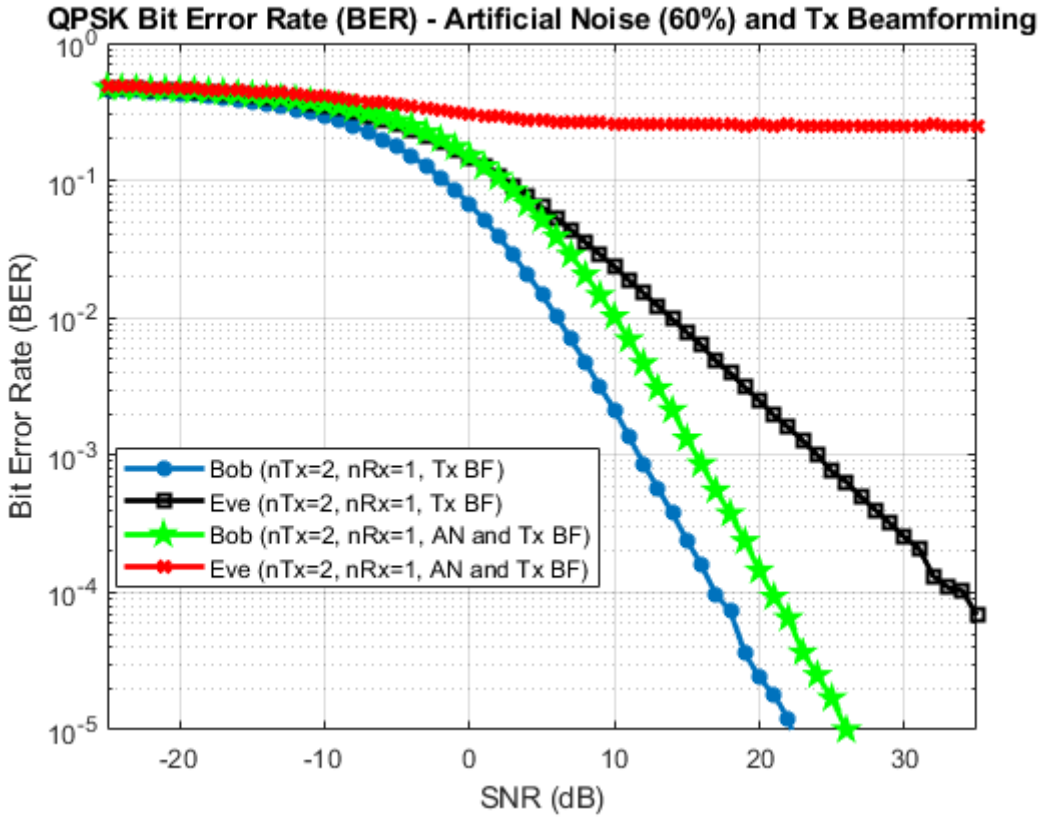

Figure 5-3: BER Simulation Plots for Bob and Eve with TX Beamforming and Artificial Noise at 60% of Total Transmit Power.

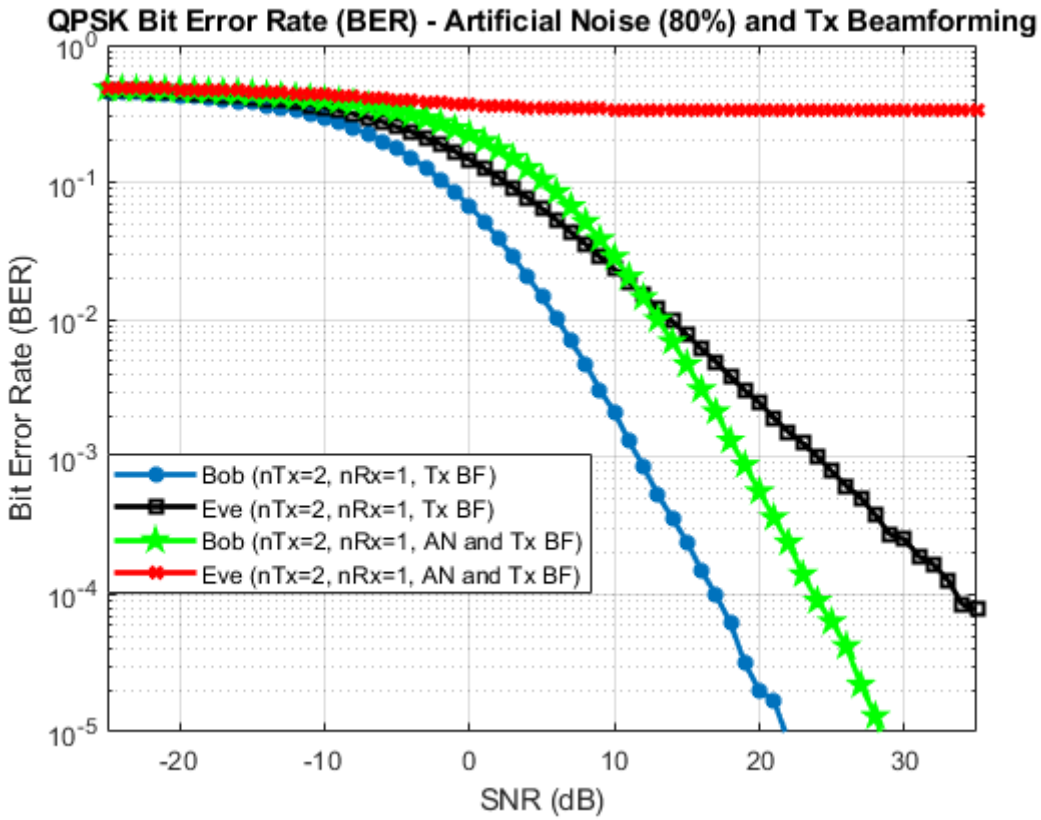

Figure 5-4: BER Simulation Plots for Bob and Eve with TX Beamforming and Artificial Noise at 80% of Total Transmit Power.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The results presented in this thesis illustrated how the use of TX BF can substantially increase the level of secrecy of information being transmitted between a transmitter and an intended receiver while increasing the difficulty of interception on the part of an eavesdropper.

The possibility of reduced transmitter power consumption using MRC at a receiver was also investigated. The simulation results observed using MATLAB suggest that MRC could be used as an alternative to transmit beamforming to reduce the processing complexity of the transmitter and in turn conserving battery power at the transmitter. Reduced battery consumption is especially important in the use of small portable battery-powered IoT devices. The number of portable IoT devices is expected to grow at an ever-increasing rate as the next-generation cellular 5G wireless networks become operational over the next several years. AN generation was investigated as well. Through the simulations performed and their presented results, this thesis demonstrated that the probability of intercept, as a result of increased BER seen by an eavesdropper, can be further decreased using AN. While the addition of AN does slightly degrade the intended receiver's performance, the impact on the eavesdropper is much greater making AN a key component of a PLS security strategy.

6.2 Future Work

For future work in the techniques of BF and AN, an implementation of these techniques in physical devices to assess their performance in an actual real world setting with increased interference could be performed. To perform such an implementation would require a pair of transceivers with MIMO arrays and the ability to modify the beamforming and artificial noise behavior, possibly using software-defined radio systems. With equipment such as SDRs, the researcher could perform actual over the air experimentation to compare MATLAB simulation results to measurements made using the SDRs.

APPENDIX A

BEAMFORMING MATLAB CODE

A.1 Transmit Beamforming Code

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% MISO No Beamforming versus Beamforming
%
% This MATLAB script provides a comparison between the
% a MISO 2 x 1 simulated system's performance and that of
% simulated Tx beamforming for a MISO 2 x 1 system containing the
% following actors:
% Alice (transmitter) has 2 Tx antennas
% Bob (intended receiver) has 1 Rx antenna
% Eve (unintended receiver i.e. eavesdropper) has 1 Rx antenna
% [6],[23]
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% Close and clear all
clear; close all; clc;

% Simulation settings
N = 10^6;    % Total symbol count
n = 2;  % Modulation order
L = 2^n;     % Modulation points
SNR_dB = -25:1:35; % SNR values (independent variable) in dB
EsNo_dB = SNR_dB + 3 * (n - 1); % Symbol Energy-to-Noise Power in dB
SNR_lin = 10.^(SNR_dB/10);  % Get the linear SNR

% Vectors to store estimation errors
bob_err = zeros(1, length(SNR_dB));
eve_err = zeros(1, length(SNR_dB));
bob_err_noBF = zeros(1, length(SNR_dB));
eve_err_noBF = zeros(1, length(SNR_dB));

% Timer to track simulation progress
tStart = tic;

% Main Simulation Loop
for idx = 1:1:length(SNR_dB)

    % Pick random channel coefficients (Alive to Bob, Alice to Eve)
    % Flat-fading assumed
    alice_bob_channel = repelem(reshape((randn(1,N) +
```

```
      randn(1,N)*1j)/sqrt(2),2,N/2),1,2);
    alice_eve_channel = repelem(reshape((randn(1,N) +
      randn(1,N)*1j)/sqrt(2),2,N/2),1,2);

% QPSK Grey-coded modulation transmitted by Alice
    x = round(rand(1,N)) + round(rand(1,N)) * 2;
    b = reshape(dec2bin(x).',1,2 * N);

    % Initialize vector to store transmitted symbol
    s = zeros(1, N);
    for u = 1:N
        if x(u) == 0
            s(u) = -1;
        elseif x(u) == 1
            s(u) = -1j;
        elseif x(u) == 2
            s(u) = 1j;
        else
            s(u) = 1;
        end
    end

    % Set transmitted symbols for with and without beamforming
    % to be the same.
    s = repelem(s,2,1)/sqrt(2);
    s_noBF = s;

    % Create Noise for Alice to Bob and Alice to Eve channels
    alice_bob_noise = 10^(-EsNo_dB(idx)/20) * (randn(1,N) +
      randn(1,N)*1j)/sqrt(2);
    alice_eve_noise = 10^(-EsNo_dB(idx)/20) * (randn(1,N) +
      randn(1,N)*1j)/sqrt(2);

    % Beamformer (Transmitter-based beamforming to Bob)
    alice_bob_channel_eff = alice_bob_channel.*exp(-1j *
      angle(alice_bob_channel));

    % Transmit signals through the channels
    bob_receive = sum(alice_bob_channel_eff.*s,1) + alice_bob_noise;
    eve_receive = sum(alice_eve_channel.*s,1) + alice_eve_noise;
    bob_receive_noBF = sum(alice_bob_channel.*s_noBF,1) +
      alice_bob_noise;
    eve_receive_noBF = sum(alice_eve_channel.*s_noBF,1) +
      alice_eve_noise;

    % Equalization to Bob's channel (BF effective channel)
    bob_s_estimate = bob_receive./sum(alice_bob_channel_eff,1);

    % Intended Receiver (Bob)(without Beamforming at all)
    bob_s_estimate_noBF = bob_receive_noBF./sum(alice_bob_channel,1);

    % Make detected symbol decisions based on measured phase
    % (Bob with BF to Bob)
    angle_bob = 180/pi * angle(bob_s_estimate);
    bob_x_estimate = zeros(1,N);
```

```
for d = 1:N
    if -45 <= angle_bob(d) && angle_bob(d) < 45
        bob_x_estimate(d) = 3;
    elseif 45 <= angle_bob(d) && angle_bob(d) < 135
        bob_x_estimate(d) = 2;
    elseif 135 <= angle_bob(d) || -135 >= angle_bob(d)
        bob_x_estimate(d) = 0;
    else
            bob_x_estimate(d) = 1;
       end
end
bob_b_estimate = reshape(dec2bin(bob_x_estimate).',1,2 * N);

% Symbol detection (Bob No BF)
angle_bob_noBF = 180/pi*angle(bob_s_estimate_noBF);
bob_x_estimate_noBF = zeros(1,N);
for d = 1:N
    if -45 <= angle_bob_noBF(d) && angle_bob_noBF(d) < 45
        bob_x_estimate_noBF(d) = 3;
    elseif 45 <= angle_bob_noBF(d) && angle_bob_noBF(d) < 135
        bob_x_estimate_noBF(d) = 2;
    elseif 135 <= angle_bob_noBF(d) || -135 >= angle_bob_noBF(d)
        bob_x_estimate_noBF(d) = 0;
    else
        bob_x_estimate_noBF(d) = 1;
    end
end
bob_b_estimate_noBF = reshape(dec2bin(bob_x_estimate_noBF).',1,2 *
  N);

% Unintended Receiver (Eve)
% Equalization to Eve's channel with BF to Bob
eve_s_estimate = eve_receive./sum(alice_eve_channel,1);

% Unintended Receiver (Eve)
% Equalization with Eve's CSI without BF
eve_s_estimate_noBF = eve_receive_noBF./sum(alice_eve_channel,1);

% Symbol detection (Eve with BF to Bob)
angle_eve = 180/pi * angle(eve_s_estimate);
eve_x_estimate = zeros(1, N);
for d = 1:N
    if -45 <= angle_eve(d) && angle_eve(d) < 45
        eve_x_estimate(d) = 3;
    elseif 45 <= angle_eve(d) && angle_eve(d) < 135
        eve_x_estimate(d) = 2;
    elseif 135 <= angle_eve(d) || -135 >= angle_eve(d)
        eve_x_estimate(d) = 0;
    else
        eve_x_estimate(d) = 1;
    end
end
eve_b_estimate = reshape(dec2bin(eve_x_estimate).',1,2 * N);

% Symbol detection (Eve no BF)
angle_eve_noBF = 180/pi * angle(eve_s_estimate_noBF);
```

```
    eve_x_estimate_noBF = zeros(1, N);
    for d = 1:N
        if -45 <= angle_eve_noBF(d) && angle_eve_noBF(d) < 45
            eve_x_estimate_noBF(d) = 3;
        elseif 45 <= angle_eve_noBF(d) && angle_eve_noBF(d) < 135
            eve_x_estimate_noBF(d) = 2;
        elseif 135 <= angle_eve_noBF(d) || -135 >= angle_eve_noBF(d)
                eve_x_estimate_noBF(d) = 0;
             else
                eve_x_estimate_noBF(d) = 1;
        end
    end
    eve_b_estimate_noBF = reshape(dec2bin(eve_x_estimate_noBF).',1,2 *
      N);

    % Count the estimation errors
    bob_err(idx) = size(find(b - bob_b_estimate),2);
    eve_err(idx) = size(find(b - eve_b_estimate),2);
    bob_err_noBF(idx) = size(find(b - bob_b_estimate_noBF),2);
    eve_err_noBF(idx) = size(find(b - eve_b_estimate_noBF),2);

    % Display elapsed time
    tElapsed = toc(tStart)
end

% Simulation results
bob_BER = bob_err/(2 * N);
eve_BER = eve_err/(2 * N);
bob_BER_noBF = bob_err_noBF/(2 * N);
eve_BER_noBF = eve_err_noBF/(2 * N);

% Plot the results
close all
figure
semilogy(SNR_dB,bob_BER_noBF,'*-','LineWidth',2); % MISO (Bob)
hold on
semilogy(SNR_dB,eve_BER_noBF,'-ks','LineWidth',2); % MISO (Eve)
semilogy(SNR_dB,bob_BER,'p-g','LineWidth',2); % MISO (Bob - BF)
semilogy(SNR_dB,eve_BER,'-r*','LineWidth',2); % MISO (Eve - BF)
axis([-25 35 10^-5 1])
grid on
title('QPSK Bit Error Rate (BER) - Beamforming vs. No Beamforming');
legend('Bob (nTx=2, nRx=1, no BF)','Eve (nTx=2, nRx=1, no BF)','Bob
(nTx=2, nRx=1, Tx BF)','Eve (nTx=2, nRx=1, Tx BF)');
xlabel('SNR (dB)');
ylabel('Bit Error Rate (BER)');
```

A.2 Maximal Ratio Combining Code

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% MISO Transmit Beamforming versus Maximal Ratio Combining
% i.e. Rx Beamforming
%
% This MATLAB script provides a comparison between the
```

```
% a MISO 2 x 1 simulated system's performance and that of
% simulated Rx Beamforming for a SIMO 1 x 2 system containing the
% following actors:
% Alice (transmitter) has 1 Tx antenna
% Bob (intended receiver) has 2 Rx antenna
% [6],[23]
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% Close and clear all
clear; close all; clc;

% Simulation parameters
N = 10^6;   % Information symbols
n = 2;  % Modulation order
L = 2^n;    % Modulation points
SNR_dB = -25:1:35; % SNR values (independent variable) in dB
EsNo_dB = SNR_dB + 3 * (n - 1); % Symbol Energy-to-Noise Power in dB
SNR_lin = 10.^(SNR_dB/10);  % Get the linear SNR
nRx = 2;    % Number of Rx antennas for MRC simulation

% Vector to store estimation errors
bob_err = zeros(1, length(SNR_dB));

% Timer to track simulation progress
tStart = tic;

% Main MISO Simulation Loop
for idx = 1:1:length(SNR_dB)

    % Pick random channel coefficients (Alive to Bob)
    % Flat-fading assumed
    alice_bob_channel = repelem(reshape((randn(1,N) +
      randn(1,N)*1j)/sqrt(2),2,N/2),1,2);

    % QPSK Grey-coded modulation transmitted by Alice
    x = round(rand(1,N)) + round(rand(1,N)) * 2;
    b = reshape(dec2bin(x).',1,2 * N);

    % Initialize vector to store transmitted symbols
    s = zeros(1,N);
    for u = 1:N
        if x(u) == 0
            s(u) = -1;
        elseif x(u) == 1
                  s(u) = -1j;
              elseif x(u) == 2
                  s(u) = 1j;
        else
            s(u) = 1;
        end
    end

    % Copy symbols vector for use in MRC simulation below
    s_mrc = s;
```

```
    % Set transmitted symbols
    s = repelem(s,2,1)/sqrt(2);

    % Create Noise for Alice to Bob channel
    alice_bob_noise = 10^(-EsNo_dB(idx)/20) * (randn(1,N) +
      randn(1,N)*1j)/sqrt(2);

    % Beamformer (Transmitter-based beamforming to Bob)
    alice_bob_channel_eff = alice_bob_channel.*exp(-
      1j*angle(alice_bob_channel));

    % Received signal
    bob_receive = sum(alice_bob_channel_eff.*s,1) + alice_bob_noise;

    % Equalization to Bob's channel (BF effective channel)
    bob_s_estimate = bob_receive./sum(alice_bob_channel_eff,1);

    % Make detected symbol decisions based on measured phase
    % (Bob with BF to Bob)
    angle_bob = 180/pi * angle(bob_s_estimate);
    bob_x_estimate = zeros(1,N);
    for d = 1:N
        if -45 <= angle_bob(d) && angle_bob(d) < 45
            bob_x_estimate(d) = 3;
        elseif 45 <= angle_bob(d) && angle_bob(d) < 135
            bob_x_estimate(d) = 2;
        elseif 135 <= angle_bob(d) || -135 >= angle_bob(d)
            bob_x_estimate(d) = 0;
        else
            bob_x_estimate(d) = 1;
        end
    end
    bob_b_estimate = reshape(dec2bin(bob_x_estimate).',1,2*N);

    % Count estimation errors
    bob_err(idx) = size(find(b - bob_b_estimate),2);

    % Display elapsed time
    tElapsed = toc(tStart)
end

% Main SIMO (MRC) Simulation Loop
for idx = 1:1:length(SNR_dB)

    % Pick random channel coefficients (Alive to Bob)
    % Flat-fading assumed
    alice_bob_channel_mrc = (randn(nRx,N) + randn(nRx,N)*1j)/sqrt(2);

    % Create Noise for Alice to Bob channel
    alice_bob_noise_mrc = 10^(-EsNo_dB(idx)/20) * (randn(nRx,N) +
      randn(nRx,N)*1j)/sqrt(2);

    % Received signal
    sd_mrc = kron(ones(nRx,1),s_mrc);
    bob_receive_mrc = alice_bob_channel_mrc.*sd_mrc +
```

```
      alice_bob_noise_mrc;

    % Equalization Maximal Ratio Combining (MRC)
    bob_s_estimate_mrc = sum(conj(alice_bob_channel_mrc).*
      bob_receive_mrc,1)./sum(alice_bob_channel_mrc.*conj(alice_bob_cha
      nnel_mrc),1);

    % Make detected symbol decisions based on measured phase
    % (Bob SIMO)
    angle_bob_mrc = 180/pi * angle(bob_s_estimate_mrc);
    bob_x_estimate_mrc = zeros(1,N);
    for d = 1:N
        if -45 <= angle_bob_mrc(d) && angle_bob_mrc(d) < 45
            bob_x_estimate_mrc(d) = 3;
        elseif 45 <= angle_bob_mrc(d) && angle_bob_mrc(d) < 135
            bob_x_estimate_mrc(d) = 2;
        elseif 135 <= angle_bob_mrc(d) || -135 >= angle_bob_mrc(d)
            bob_x_estimate_mrc(d) = 0;
        else
            bob_x_estimate_mrc(d) = 1;
        end
    end
    bob_b_estimate_mrc = reshape(dec2bin(bob_x_estimate_mrc).',1,2 *
      N);

    % Count the estimation errors
    bob_err_nRx2(idx) = size(find(b - bob_b_estimate_mrc),2);

    % Display elapsed time
    tElapsed = toc(tStart)
end

% Theoretical Results
p = 1/2 - (1 + 1./SNR_lin).^(-1/2)/2;
theory_BER_nRx2 = p.^2.*(1 + 2 * (1 - p));

% Simulation results
bob_BER = bob_err/(2 * N);
bob_BER_nRx2 = bob_err_nRx2/(2 * N);

% Plot results
close all
figure
semilogy(SNR_dB,theory_BER_nRx2,'s-','LineWidth',2); % SIMO MRC theory
hold on
semilogy(SNR_dB,bob_BER,'p-g','LineWidth',2); % MISO (Bob - BF)
semilogy(SNR_dB,bob_BER_nRx2,'o-r','LineWidth',2); % Bob SIMO MRC sim
axis([-25 35 10^-5 1])
grid on
title('QPSK Bit Error Rate (BER) - Maximal Ratio Combining (MRC)');
legend('SIMO (MRC nTx=1, nRx=2) theory','MISO (nTx=2, nRx=1, Tx BF)
sim','SIMO (MRC nTx=1, nRx=2) sim');
xlabel('SNR (dB)');
ylabel('Bit Error Rate (BER)');
```

APPENDIX B

ARTIFICIAL NOISE MATLAB CODE

B.1 Artificial Noise Code

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% MISO Tx Beamforming With Artificial Noise (20%)
%
% This MATLAB script provides a simulation of the Bit Error Rate
% (BER) response of both an intended and an unintended receiver
% using a MISO 2 x 1 Tx Beamforming system with 20% of the total
% transmitted power used to generate artificial noise.
% The actors are the following:
% Alice (transmitter) has 2 Tx antennas
% Bob (intended receiver) has 1 Rx antenna
% Eve (unintended receiver i.e. eavesdropper) has 1 Rx antenna
% [6],[23]
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% Close and clear all
clear; close all; clc;

% Simulation settings
N = 10^6;   % Total symbol count
n = 2;  % Modulation order
L = 2^n;    % Modulation points
SNR_dB = -25:1:35; % SNR values (independent variable) in dB
EsNo_dB = SNR_dB + 3 * (n - 1); % Symbol Energy-to-Noise in dB
SNR_lin = 10.^(SNR_dB/10);  % Get the linear SNR
Ran = 0.2; % Ratio of Artificial Noise to Total Power

% Initialize vectors to store estimation errors
bob_err = zeros(1, length(SNR_dB));
eve_err = zeros(1, length(SNR_dB));
bob_err_noAN = zeros(1, length(SNR_dB));
      eve_err_noAN = zeros(1, length(SNR_dB));

% Timer to track simulation progress
tStart = tic;

% Main Simulation Loop
for idx = 1:1:length(SNR_dB)

    % Pick random channel coefficients (Alive to Bob, Alice to Eve)
```

```
    % Flat-fading assumed
    alice_bob_channel = repelem(reshape((randn(1,N) +
      randn(1,N)*1j)/sqrt(2),2,N/2),1,2);
    alice_eve_channel = repelem(reshape((randn(1,N) +
      randn(1,N)*1j)/sqrt(2),2,N/2),1,2);

    % QPSK Grey-coded modulation transmitted by Alice
    x = round(rand(1,N)) + round(rand(1,N)) * 2;
    b = reshape(dec2bin(x).',1,2 * N);

    % Initialize vector to store transmitted symbols
    s = zeros(1, N);
    for u = 1:N
        if x(u) == 0
            s(u) = -1;
        elseif x(u) == 1
            s(u) = -1j;
        elseif x(u) == 2
            s(u) = 1j;
        else
            s(u) = 1;
        end
    end

    % Set transmitted symbols for with and without artificial noise
    % to be the same.
    s = repelem(s,2,1)/sqrt(2);
    s_noAN = s;

    % Create Noise for Alice to Bob and Alice to Eve channels
    alice_bob_noise = 10^(-EsNo_dB(idx)/20) * (randn(1,N) +
      randn(1,N)*1j)/sqrt(2);
    alice_eve_noise = 10^(-EsNo_dB(idx)/20) * (randn(1,N) +
      randn(1,N)*1j)/sqrt(2);

    % Beamformer (Transmitter-based beamforming to Bob)
    alice_bob_channel_eff = alice_bob_channel.*exp(-
      1j*angle(alice_bob_channel));

    % Artificial noise based on Bob's channel
    for i = 1:N
        w(:,i) = null(alice_bob_channel_eff(:,i).');
    end
    s = sqrt(1 - Ran)*s + sqrt(Ran)*w;

    % Received signals
          bob_receive = sum(alice_bob_channel_eff.*s,1) +
alice_bob_noise;
    eve_receive = sum(alice_eve_channel.*s,1) + alice_eve_noise;
    bob_receive_noAN = sum(alice_bob_channel_eff.*s_noAN,1) +
      alice_bob_noise;
    eve_receive_noAN = sum(alice_eve_channel.*s_noAN,1) +
      alice_eve_noise;

    % Equalization to Bob's channel (BF effective channel)
```

```
bob_s_estimate = bob_receive./sum(alice_bob_channel_eff,1);

% Intended Receiver (Bob)(without artificial noise)
bob_s_estimate_noAN =
  bob_receive_noAN./sum(alice_bob_channel_eff,1);

% Symbol decisions (Bob with AN)
angle_bob = 180/pi * angle(bob_s_estimate);
bob_x_estimate = zeros(1, N);
for d = 1:N
    if -45 <= angle_bob(d) && angle_bob(d) < 45
        bob_x_estimate(d) = 3;
    elseif 45 <= angle_bob(d) && angle_bob(d) < 135
        bob_x_estimate(d) = 2;
    elseif 135 <= angle_bob(d) || -135 >= angle_bob(d)
        bob_x_estimate(d) = 0;
    else
        bob_x_estimate(d) = 1;
    end
end
bob_b_estimate = reshape(dec2bin(bob_x_estimate).',1,2*N);

% Symbol decisions (Bob No AN)
angle_bob_noAN = 180/pi * angle(bob_s_estimate_noAN);
bob_x_estimate_noAN = zeros(1, N);
for d = 1:N
    if -45 <= angle_bob_noAN(d) && angle_bob_noAN(d) < 45
        bob_x_estimate_noAN(d) = 3;
    elseif 45 <= angle_bob_noAN(d) && angle_bob_noAN(d) < 135
        bob_x_estimate_noAN(d) = 2;
    elseif 135 <= angle_bob_noAN(d) || -135 >= angle_bob_noAN(d)
        bob_x_estimate_noAN(d) = 0;
    else
        bob_x_estimate_noAN(d) = 1;
    end
end
bob_b_estimate_noAN =
  reshape(dec2bin(bob_x_estimate_noAN).',1,2*N);

% Unintended Receiver (Eve)
% Equalization to Eve's channel with AN
eve_s_estimate = eve_receive./sum(alice_eve_channel,1);

% Unintended Receiver (Eve)
% Equalization with Eve's channel without AN
eve_s_estimate_noAN = eve_receive_noAN./sum(alice_eve_channel,1);

      % Symbol decisions (Eve with AN)
angle_eve = 180/pi * angle(eve_s_estimate);
eve_x_estimate = zeros(1, N);
for d = 1:N
    if -45 <= angle_eve(d) && angle_eve(d) < 45
        eve_x_estimate(d) = 3;
    elseif 45 <= angle_eve(d) && angle_eve(d) < 135
        eve_x_estimate(d) = 2;
    elseif 135 <= angle_eve(d) || -135 >= angle_eve(d)
```

```
            eve_x_estimate(d) = 0;
        else
            eve_x_estimate(d) = 1;
        end
    end
    eve_b_estimate = reshape(dec2bin(eve_x_estimate).',1,2 * N);

    % Symbol decisions (Eve no AN)
    angle_eve_noAN = 180/pi * angle(eve_s_estimate_noAN);
    eve_x_estimate_noAN = zeros(1, N);
    for d = 1:N
        if -45 <= angle_eve_noAN(d) && angle_eve_noAN(d) < 45
            eve_x_estimate_noAN(d) = 3;
        elseif 45 <= angle_eve_noAN(d) && angle_eve_noAN(d) < 135
            eve_x_estimate_noAN(d) = 2;
        elseif 135 <= angle_eve_noAN(d) || -135 >= angle_eve_noAN(d)
            eve_x_estimate_noAN(d) = 0;
        else
            eve_x_estimate_noAN(d) = 1;
        end
    end
    eve_b_estimate_noAN = reshape(dec2bin(eve_x_estimate_noAN).',1,2 *
      N);

    % Count estimation errors
    bob_err(idx) = size(find(b - bob_b_estimate),2);
    eve_err(idx) = size(find(b - eve_b_estimate),2);
    bob_err_noAN(idx) = size(find(b - bob_b_estimate_noAN),2);
    eve_err_noAN(idx) = size(find(b - eve_b_estimate_noAN),2);

    % Display elapsed time
    tElapsed = toc(tStart)
end

% Simulation results
bob_BER = bob_err/(2 * N);
eve_BER = eve_err/(2 * N);
bob_BER_noAN = bob_err_noAN/(2 * N);
eve_BER_noAN = eve_err_noAN/(2 * N);

% Plot results
close all
figure
semilogy(SNR_dB,bob_BER_noAN,'*-','LineWidth',2); % MISO (Bob)
hold on
semilogy(SNR_dB,eve_BER_noAN,'-ks','LineWidth',2); % MISO (Eve)
semilogy(SNR_dB,bob_BER,'p-g','LineWidth',2); % MISO (Bob - AN)
      semilogy(SNR_dB,eve_BER,'-rx','LineWidth',2); % MISO (Eve - AN)
axis([-25 35 10^-5 1])
grid on
title('QPSK Bit Error Rate (BER) - Artificial Noise (20%) and Tx
Beamforming');
legend('Bob (nTx=2, nRx=1, Tx BF)','Eve (nTx=2, nRx=1, Tx BF)','Bob
(nTx=2, nRx=1, AN and Tx BF)','Eve (nTx=2, nRx=1, AN and Tx BF)');
xlabel('SNR (dB)');
ylabel('Bit Error Rate (BER)');
```

BIBLIOGRAPHY

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal,* vol. 28, no. 4, pp. 656-715, Oct 1949.

[2] T. M. Cover and J. A. Thomas, Elements of Information Theory, Hoboken, NJ: John Wiley & Sons, Inc., 2006.

[3] D. J. C. MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2005.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal,* vol. 54, no. 8, pp. 1355-1387, 1975.

[5] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," *Proceedings of the IEEE,* vol. 103, no. 10, pp. 1814-1825, 2015.

[6] K. Ryland, "Software-Defined Implementation of Two Physical Layer Security Techniques," M.S. Thesis, Arlington, VA, 2017.

[7] M. Bloch and J. Barros, Physical Layer Security: From Information Theory to Security Engineering, Cambridge Universoty Press, 2011.

[8] A. Subramanian, A. T. Suresh, S. Raj, A. Thangaraj, M. Bloch and S. McLaughlin, "Strong and Weak Secrecy in Wiretap Channels," in *2010 6th International Symposium on Turbo Codes & Iterative Information Processing*.

[9] A. J. Paulraj, D. A. Gore, R. U. Nabar and H. Bolcskei, "An Overview of MIMO Communications - A Key to Gigabit Wireless," *Proceedings of the IEEE,* vol. 95, no. 2, pp. 198-218, 2004.

[10] X. Zhou, L. Song and Y. Zhang, Physical Layer Security in Wireless Communications, Boca Raton, FL: CRC Press - Taylor & Frances Group LLC, 2014.

[11] M. Jankiraman, Space-Time Codes and MIMO Systems, Norwood, MA: ArtechHouse, Inc., 2004.

[12] D. Gesbert and J. Akhtar, "Breaking the barriers of Shannon's capacity: An overview of MIMO wireless systems," *Telektronikk Telenor's Journal*, pp. 1-9, 2002.

[13] P. M. Sankar, "Maximal ratio combining in independent identically distributed n * nakagami fading channels," *IET Communications,* vol. 5, no. 3, pp. 320-326, 2011.

[14] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj and H. V. Poor, MIMO Wireless Communications, Cambridge, England: Cambridge University Press, 2007.

[15] W. A. Shehab and Z. Al-qudah, "Singular Value Decomposition: Principles and Applications in Multiple Input Multiple Output Communication System," *International Journal of Computer Networks & Communications,* vol. 9, no. 1, pp. 13-21, 2017.

[16] Y. W. Hong, W. J. Huang and C. C. Kuo, Cooperative Communications and Networking: Technologies and System Design, New York: Springer, 2010.

[17] M. Baldi and S. Tomasin, Physical and Data-Link Security Techniques for Future Communication Systems, Cham: Springer International Publishing Switzerland, 2016.

[18] O. Bonaventure, Computer Networking : Principles, Protocols and Practice, lulu.com, 2014.

[19] X. Chen and W. H. Gerstacker, "A Survey of Multiple-Antenna Techniques for Physical Layer Security," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 2, pp. 1027-1053, 2017.

[20] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. Huang and H. H. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Wireless Communications,* vol. 18, no. 2, pp. 66-74, 2011.

[21] D. Wang, B. Bai, W. Zhao and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Communications Surveys & Tutorials,* vol. doi: 10.1109/COMST.2018.2883144, 2018.

[22] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas - Part II: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory,* vol. 56, no. 11, pp. 5515-5532, 2010.

[23] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory,* vol. 56, no. 7, pp. 3088-3104, July 2010.

[24] K. Sankar, "DSPLOG Signal Processing for Communication," 28 Sept 2008. [Online]. Available: http://www.dsplog.com/2008/09/28/maximal-ratio-combining/.

[25] "What are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing," 16 6 2015. [Online]. Available: https://support.huawei.com/enterprise/en/knowledge/EK1000079062.

[26] S. Rohilla, D. K. Patidar and N. K. Soni, "Comparative Analysis of Maximum Ratio Combining and Equal Gain Combining Diversity Technique for WCDMA: A Survey," *Internation Journal of Engineering Inventions,* vol. 3, no. 1, pp. 72-77, 2013.

[27] R. Negi and S. Goel, "Secret Communication using Artificial Noise," *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005,* vol. 3, pp. 1906-1910, Sept 2005.